Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Datenschutz und Informationsfreiheit

Bericht 2014

be Berlin

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2014

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am **2. April 2014** vorgelegten Jahresbericht 2013 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2014 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2014“) veröffentlicht.

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

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4 - 10, 10787 Berlin
Telefon: (030) +138 89-0
Telefax: (030) 215 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de/

Satz: LayoutManufaktur.com

Druck: Druckerei Dienstleistungen

Inhalt

Einleitung

„Unsere Freiheit beruht auf dem, was andere nicht über unsere Existenz wissen.“
Alexander Solschenizyn[1]

Datenschutz ist weit mehr als Datensicherheit. Datenschutz soll dem einzelnen Menschen existenzielle Freiheitsräume sichern. Daran muss anderthalb Jahre nach dem Beginn der von Edward Snowden ausgelösten Veröffentlichungen über exzessive Überwachungspraktiken der Geheimdienste demokratischer Staaten erinnert werden. Einer der Schwerpunkte unserer Tätigkeit auch im vergangenen Jahr war die Frage, welche Konsequenzen aus dem anhaltenden NSA-Skandal gezogen werden müssen. Ein Teil dieser notwendigen Konsequenzen sind Maßnahmen der Datensicherheit. Die Bundesregierung hat in ihrer Digitalen Agenda 2014–2017 noch im August die Absicht erklärt, Deutschland zum „Verschlüsselungsstandort Nummer eins auf der Welt“ zu machen.[2] Nach den Terroranschlägen von Paris im Januar 2015 unterstützten Politiker erneut die Forderung, man müsse das Recht zur Verschlüsselung einschränken, um den Terror effektiv bekämpfen zu können.

In Deutschland sind Netzbetreiber bereits nach geltendem Recht dann zur Herausgabe von Schlüsseln an die Sicherheitsbehörden verpflichtet, wenn sie die netzseitige Verschlüsselung von Kommunikationsinhalten als Dienst anbieten.[3] Darüber hinausgehende Verbote z.B. von Ende-zu-Ende-Verschlüsselung sind weder sinnvoll noch technisch durchführbar. Dies hatte die Bundesregierung in ihren Eckpunkten der deutschen Kryptopolitik von 1999 erkannt und deshalb davon abgesehen, die freie Verfügbarkeit von Verschlüsselungsprodukten einschränken zu wollen. Diesen Schritt haben die Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt.[4] Jeder Versuch, die Nutzung

1 Zitat nach: Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, beschlossen am 26. Januar 2015
2 Digitale Agenda 2014-2017, S. 31
3 § 8 Abs. 3 TKÜV
4 Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. Oktober 1999: „Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung“

von Verschlüsselungstechnik weitergehend als bisher einschränken zu wollen, hätte lediglich symbolpolitischen Charakter. Die Verantwortung des Staates besteht auf Bundes- und Landesebene vielmehr darin, die Voraussetzungen für eine sichere Kommunikationsinfrastruktur zu schaffen. Dazu gehören auch die Förderung der Entwicklung von einfach nutzbarer Ende-zu-Ende-Verschlüsselung und die Verpflichtung öffentlicher Stellen, Verschlüsselungsverfahren anzubieten und zu nutzen. Ziel der Digitalen Agenda in Berlin und Deutschland ist es gerade, die Kommunikation zwischen Bürgern und Verwaltung einfacher und sicherer zu gestalten. Dies setzt Vertrauen voraus, das durch den Einbau von Hintertüren oder das Verbot effektiver Verschlüsselung zerstört wird.

Der flächendeckende Einsatz von Verschlüsselung wird von den meisten Fachleuten als entscheidendes Mittel zum Selbstschutz gegen die Ausspähung durch maßlos agierende Geheimdienste und kriminelle Hacker angesehen. Datenschutz geht aber über die Sicherung von Information weit hinaus. Der Europäische Gerichtshof hat im zurückliegenden Jahr in zwei bahnbrechenden Urteilen den Datenschutz als europäisches Grundrecht gestärkt, indem er zum einen die Richtlinie zur Vorratsdatenspeicherung als grundrechtswidrig aufgehoben[5] und zum anderen Google verpflichtet hat, bestimmte personenbezogene Ergebnisse in seiner Suchmaschine nicht mehr anzuzeigen.[6] Damit hat der Europäische Gerichtshof Befürchtungen entkräftet, der maßgeblich vom Bundesverfassungsgericht entwickelte Datenschutz könne im Zuge seiner zunehmenden Europäisierung entwertet werden. Das Urteil zur Vorratsdatenspeicherung stellt die Balance zwischen Freiheit und Sicherheit wieder her, die verloren zu gehen drohte. Auch der Europäische Gerichtshof ist ein Menschenrechtsgerichtshof. Seine Bedeutung in Fragen des Datenschutzes wird nicht zuletzt in Berlin zunehmen. So hat der Bundesgerichtshof die zuerst vom Amtsgericht Berlin-Mitte behandelte Frage, ob IP-Adressen dem Datenschutz unterliegen, dem Europäischen Gerichtshof zur Entscheidung vorgelegt.[7]

Die Informationsfreiheit nimmt in diesem Bericht einen größeren Raum ein als in den vergangenen Jahren. Dies macht deutlich, dass zum einen mehr Menschen als bisher ihr Recht auf voraussetzungslosen Zugang

5 Siehe 11.2
6 Siehe 11.3
7 BGH, Beschluss vom 28. Oktober 2014 (VI ZR 135/13)

zu Verwaltungsinformationen geltend machen. Zum anderen haben wir erstmals von Amts wegen die Umsetzung des Informationsfreiheitsgesetzes in einer Berliner Behörde überprüft.[8]

Zunehmend werden Informationsfreiheitsgesetze, bei denen der Bürger Zugang zu Verwaltungsinformationen als „Holschuld" beantragen muss, von Transparenzgesetzen abgelöst, in denen die Behörden von sich aus Informationen als „Bringschuld" veröffentlichen. So ist in der Freien und Hansestadt Hamburg im Oktober das Transparenzgesetz endgültig in Kraft getreten und in den Ländern Rheinland-Pfalz und Thüringen sind entsprechende Gesetze in Vorbereitung. In diese Richtung muss sich auch das Informationsfreiheitsrecht in Berlin entwickeln. Das unverbindliche Open Data-Portal der Bundeshauptstadt kann kein Transparenzgesetz ersetzen.

8 2.6

1 Digitale Verwaltung

1.1 E-Government

1.1.1 Allgemeiner Zugang nach dem E-Government-Gesetz des Bundes

Anfang August 2013 trat das E-Government-Gesetz des Bundes in Kraft,[9] das für bestimmte Vorschriften ein gestuftes Inkrafttreten festlegte. Seit dem 1. Juli 2014[10] ist jede Behörde verpflichtet, den Bürgerinnen und Bürgern einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen.[11] Verpflichtet sind dabei nicht nur Behörden des Bundes,[12] sondern auch Behörden Berlins und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen.[13]

Die Senatsverwaltung für Inneres und Sport hatte hierzu im Juni ein Rundschreiben[14] an alle öffentlichen Stellen des Landes Berlin versandt und im Ergebnis Folgendes erklärt: Da alle Berliner Behörden auch Bundesrecht ausführen würden, seien sie ausnahmslos dazu verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente zu eröffnen. Eine Beschränkung auf einzelne Fachbereiche sei nicht zulässig. Auch sei nicht vorgesehen, die allgemeine elektronische Zugangseröffnung nur auf Angelegenheiten nach dem Bundesrecht zu beschränken. Ferner habe jede Behörde ein zentrales Postfach als elektronische Zugangseröffnung zu deklarieren; separate Postfächer seien ausnahmsweise nur dann zulässig, wenn in einzelnen Fachbereichen mit einem besonders hohen Aufkommen zu rechnen sei.

9 Siehe JB 2013, 1.7
10 Art. 31 Abs. 2 des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften
11 § 2 Abs. 1 EGovG Bund
12 § 1 Abs. 1 EGovG Bund
13 § 1 Abs. 2 EGovG Bund
14 Rundschreiben InnSport ZS Nr. 7/2014 vom 26. Juni 2014, Geschäftszeichen ZS C 2 MC - 0656 [eSignatur / qeS RS]

Datenverarbeitende Stelle im Sinne des Berliner Datenschutzgesetzes ist jedoch jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist.[15] Mithin gelten alle Organisationseinheiten in diesem Sinne – wie etwa der behördliche Datenschutzbeauftragte, das Sozialamt oder das Gesundheitsamt – jeweils als eigene datenverarbeitende Stellen.

Die Kenntnisnahme der an eine dieser Organisationseinheiten gesendeten Emails durch eine zentrale Poststelle wäre daher – ebenso wie die Öffnung von als „vertraulich/verschlossen" gekennzeichneter Briefpost[16] – unzulässig. Vielmehr dürfen solche Emails nur von der jeweiligen Organisationseinheit selbst – etwa durch deren eigene Poststelle – entschlüsselt, auf eine gültige Signatur überprüft, zur Kenntnis genommen und weitergeleitet werden. Um eine Kenntnisnahme durch eine zentrale Poststelle sicher ausschließen zu können, ist es daher zwingend erforderlich, dass alle Organisationseinheiten jeweils über eigene Postfächer verfügen, da nur so ein – auch versehentlicher – unbefugter Zugriff sicher ausgeschlossen werden kann.

Daher ist auch die Gemeinsame Geschäftsordnung der Berliner Verwaltung in der jetzigen Form zu weit gefasst. Danach ist zwar grundsätzlich zum Empfang der allgemein an die Behörde gerichteten elektronischen Post für jede Organisationseinheit ein eigenes elektronisches Postfach einzurichten. Gleichwohl ist ausdrücklich eine Ausnahme vorgesehen, wonach aus Gründen der Zweckmäßigkeit ein elektronisches Postfach auch nur für die zentrale Postverteilungsstelle eingerichtet werden kann.[17] Zweckmäßigkeitserwägungen oder Kostengründe dürfen jedoch nicht zu einer Absenkung des Datenschutzniveaus führen. Insbesondere ist der Mehraufwand dezentraler elektronischer Poststellen ohnehin zu vernachlässigen, da mittlerweile alle Behörden und mithin auch alle Organisationseinheiten über eine ausreichende EDV-Ausstattung verfügen.

15 § 4 Abs. 3 Nr. 1 BlnDSG
16 § 25 Abs. 1 GGO I
17 § 23 Abs. 3 Satz 1 GGO I

Der Einrichtung dezentraler Postfächer steht auch nicht entgegen, dass die Bürgerinnen und Bürger mangels Kenntnis der Behördenorganisation häufig nicht wissen, welche Stelle in einer Behörde für das Anliegen zuständig ist. So werden zwar entsprechende Emails häufig nicht an die im Einzelfall zuständige Organisationseinheit, sondern an das zentrale Postfach der Behörde geschickt. Gleichwohl muss die Wahlmöglichkeit der Bürgerinnen und Bürger erhalten bleiben, sich direkt an die ihnen bekannte Organisationseinheit zu wenden, ohne den Umweg über das zentrale Postfach wählen zu müssen.

Wir teilten der Senatsverwaltung daher mit, dass der Einsatz nur eines zentralen elektronischen Postfachs unzulässig wäre und es vielmehr zwingend erforderlich ist, dass alle Organisationseinheiten im Sinne des Berliner Datenschutzgesetzes jeweils über eigene elektronische Postfächer verfügen. Die Senatsverwaltung sagte uns zu, das Rundschreiben anzupassen und auf eine Änderung der Gemeinsamen Geschäftsordnung der Berliner Verwaltung[18] hinzuwirken.

Jede Organisationseinheit in der Berliner Verwaltung, der eine eigene gesetzliche Aufgabe zugewiesen ist, muss über ein elektronisches Postfach verfügen, das Bürgerinnen und Bürger für E-Government-Dienste nutzen können.

1.1.2 Zentrales Service-Konto Berlin

Mit dem Service-Konto Berlin soll Bürgerinnen und Bürgern ein personalisierter Zugang zu vielen verschiedenen E-Government-Dienstleistungen angeboten werden. Damit wird eine sichere Identifizierung für Online-Anwendungen der Berliner Verwaltung durch Nutzung der eID-Funktion des neuen Personalausweises bereitgestellt. Mit dem Service-Konto Berlin soll nun sowohl die Funktionalität eines permanenten als auch eines temporären Bürgerkontos[19] angeboten werden.

18 GGO I

19 Zu den Unterschieden zwischen diesen beiden Formen elektronischer Verwaltungsdienstleistungen siehe JB 2013, 1.3

Die Nutzung soll zudem nicht nur für natürliche Personen, sondern auch für juristische Personen (z.B. Unternehmen) möglich sein. Bei juristischen Personen stellt sich jedoch das Problem, dass diese nicht über einen Personalausweis mit eID-Funktion verfügen, sondern hierfür der Personalausweis einer natürlichen Person herangezogen werden muss. Wir haben in diesem Zusammenhang auf die Problematik der Freiwilligkeit der Einwilligung im Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer hingewiesen und insoweit eine strikte Trennung zwischen privatem Service-Konto und Unternehmens-Service-Konto empfohlen.

Da das E-Government-Gesetz Berlin bislang noch nicht in das Parlament eingebracht wurde, fehlt es derzeit allerdings an einer gesetzlichen Grundlage für den Betrieb des Service-Kontos.[20]

Ohne gesetzliche Grundlage ist ein Betrieb des Service-Kontos Berlin nicht möglich.

1.2 Instant-Messaging-Dienste bei Pflegediensten

Aufgrund einer Eingabe prüften wir einen Pflegedienst, der seine Beschäftigten aufgefordert hatte, über WhatsApp miteinander zu kommunizieren.

Die Beschäftigten von Pflegediensten sind viel unterwegs. Neben Routinetätigkeiten haben sie vielfach mit unerwarteten Situationen zu kämpfen, bei denen es hilfreich ist, Kolleginnen und Kollegen zu unterrichten oder nach zusätzlichen Informationen über die Klienten zu fragen, mit denen sie zu tun haben. Statt Telefon und SMS bieten sich hierfür Instant-Messaging-Dienste an, die es erlauben, mit einer Nachricht ohne große Kosten eine Gruppe von Personen zu erreichen.

20 Siehe JB 2013, 1.7

Zulässig ist die Verwendung dieser Dienste jedoch nur, wenn durch die Kommunikation niemand außerhalb des Pflegedienstes etwas über die Klienten erfährt. Für die Beschäftigten des Pflegedienstes genau wie Ärzte gilt die Pflicht, über das zu schweigen, was sie über die Klienten oder Patienten erfahren. Darüber hinaus darf ein Arbeitgeber auch nicht die Nutzung von Verfahren anordnen, bei denen Angaben über seine Beschäftigten Dritten offenbart werden, soweit dies nicht zwingend für die Tätigkeit und die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

Daher darf ein Pflegedienst in der beschriebenen Konstellation nur solche Messaging-Dienste verwenden, die eine Ende-zu-Ende-Verschlüsselung bieten. Eine zunehmende Zahl von Diensten bietet diese Funktion, oft jedoch nicht für die Übermittlung einer Nachricht an eine Vielzahl von Empfängern. Die Verschlüsselung muss zuverlässig und langfristig wirksam sein. Der Arbeitgeber muss sicherstellen, dass Nachrichten nur an Empfänger gehen, die er seinem Betrieb sicher zuordnen kann. Einige Messaging-Dienste bieten eine solche Überprüfungsfunktion an, z.B. über den gegenseitigen Scan von QR-Codes von Smartphone zu Smartphone.

Schließlich gehört zu einer sicheren Übertragung auch die Sicherheit des verwendeten Geräts. Von Hause aus sind viele Smartphones nicht für den betrieblichen Gebrauch geeignet. Es ist jedoch Software verfügbar, die es ermöglicht, die Geräte einheitlich zu verwalten (das sog. Mobile-Device-Management), bestimmte, mit besonderen Risiken verbundene Funktionen zu deaktivieren und die übermittelten Daten in einem gesicherten Container abzulegen. Voraussetzung für eine wirksame Anwendung ist bei alldem, dass die Smartphones dem Arbeitgeber gehören und er die nötige Verfügungsgewalt über sie behält.

Ist die Kommunikation selbst gesichert, verbleiben die Metadaten: Dem Betreiber des Messaging-Dienstes wird bekannt, von welchem Gerät aus mit welchen anderen Geräten wann kommuniziert wird. Dies ist besonders dann problematisch, wenn der Anbieter – wie im Fall von WhatsApp – außerhalb der Europäischen Union angesiedelt ist und sich nicht an europäisches Telekommunikationsrecht hält.

Ausreichend gemindert ist dieses Risiko, wenn die Smartphones nicht auf den Namen der oder des jeweiligen Beschäftigten registriert werden, weder bei

dem Netzanbieter noch bei dem Softwarehersteller wie Google oder Apple noch bei dem Messaging-Dienst selbst, und die Geräte ausschließlich dienstlich genutzt werden. Dadurch wird gewährleistet, dass ihre betriebliche Verwendung nicht mit anderer, privater Nutzung und damit vielfach indirekt doch mit dem Namen der bzw. des Beschäftigten verknüpft werden kann.

Vorzuziehen ist es jedoch in jedem Fall, einen Anbieter einzuschalten, der sich in überprüfbarer Weise an europäisches Datenschutz- und Telekommunikationsrecht hält.

Instant-Messaging kann auch im sensitiven Bereich der Pflegedienste eingesetzt werden, bedarf jedoch vielfältiger sicherheitstechnischer Vorkehrungen und insbesondere einer zuverlässigen Ende-zu-Ende-Verschlüsselung. Die Nutzung von WhatsApp in der derzeitigen Ausgestaltung des Dienstes ist unzulässig.

1.3 Nutzung von Yahoo-E-Mail-Adressen

Acht Reviere des Grünflächenamts des Bezirksamts Marzahn-Hellersdorf von Berlin nutzen zur elektronischen Kommunikation kostenfreie Mailadressen des US-amerikanischen Anbieters Yahoo. Inhaltlich werden diese Adressen für die digitale Kommunikation mit dem Bürger genutzt, aber auch interne Angelegenheiten wie z.B. Krankmeldungen erfolgen über dieses Medium. Die E-Mail-Adressen sind auf den Internetseiten des Amts bei „berlin.de“ veröffentlicht.

Auf den ersten Blick erscheint dieser Sachverhalt unproblematisch. Viele Menschen nutzen entsprechende Dienste. Warum sollte ein Amt dies nicht können?

Im Gegensatz zu Privatpersonen handeln Ämter im öffentlichen Auftrag und unterliegen strengeren Vorschriften. Die Nutzung von US-amerikanischen E-Mail-Konten, zu dem auch die E-Mail-Konten bei Yahoo zählen, führt zu einer Übertragung personenbezogener Daten an eine Stelle außerhalb der Europäischen Union. Diese bedarf gemäß § 6 Abs. 1 BlnDSG einer

Rechtsgrundlage selbst dann, wenn sie im Rahmen einer Auftragsdatenverarbeitung erfolgen soll. Eine solche Rechtsgrundlage ist hier nicht ersichtlich. Vielmehr geht das Berliner Datenschutzgesetz grundsätzlich davon aus, dass eine Auftragsdatenverarbeitung nur innerhalb der Europäischen Union stattfindet. [21] Daher ist davon auszugehen, dass es sich in diesem Fall um eine nicht rechtmäßige Datenübermittlung handelt.

Hinzu kommt, dass die unverschlüsselte Übertragung personenbezogener Daten über das Medium E-Mail einen Bruch der Vertraulichkeit darstellt, gegen § 5 Abs. 2 Nr. 1 BlnDSG verstößt und möglicherweise sogar als Verletzung des Amtsgeheimnisses strafbar ist (§ 203 Abs. 2 StGB). Die datenverarbeitenden Stellen haben Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, dass diese Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine solche Maßnahme ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt die Verschlüsselung zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität von E-Mails, die nicht offenkundige Daten enthalten.

Berliner Behörden dürfen keine E-Mail-Dienste von Anbietern mit Sitz außerhalb der Europäischen Union nutzen. Wird E-Mail zur Übermittlung personenbezogener Daten genutzt, so sind diese grundsätzlich zu verschlüsseln.

1.4 Einsatz von Unterschriftenpads in den Bürgerämtern

Uns liegen Beschwerden von Bürgern vor, die den vermehrten Einsatz von Unterschriftenpads in den Bürgerämtern bemängeln. Insbesondere geht es dabei um die unklare Verwendung der geleisteten Unterschriften sowie deren Speicherung und mögliche Datenübertragungen. Ein Unterschriftenpad ist ein Gerät, mit dem eine eigenhändige Unterschrift elektronisch

21 § 3 Abs. 4 BlnDSG; siehe auch 2.2

erfasst wird. Es soll helfen, Medienbrüche zwischen elektronischen und papierenen Dokumenten zu vermeiden.

Unterschriftenpads werden in Bürgerämtern seit November bei Antragstellungen zu Reisepässen und Personalausweisen verwendet. Die Unterschriften werden im Personalausweis-Register sowie im Pass-Register des Fachverfahrens Einwohnerwesen gespeichert. Eine Erfassung von biometrischen Merkmalen bei der Erstellung des Schriftzuges, wie z.B. Druckintensität, erfolgt nicht. Eine verschlüsselte Übermittlung von Unterschriften findet zur Produktion der Personalausweise und Reisepässe an die Bundesdruckerei statt.

Auf die Unterschriftenerhebung via Unterschriftenpads kann in jedem der genannten Fälle während des Antrags- und Aushändigungsverfahrens verzichtet werden. In der Passverwaltungsvorschrift (PassVwV) ist festgelegt, dass ein Passantrag an der dafür auf dem Kontrollblatt vorgesehenen Stelle (Unterschriftenfeld) oder auf einem elektronischen Unterschriftenpad von der antragstellenden Person zu unterschreiben ist. Die PassVwV gibt im Übrigen auch den Rahmen für das Personalausweisverfahren vor. Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben.[22] Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er in geeigneter Weise über den Zweck der Datenerhebung aufzuklären. Die Freiwilligkeit der Nutzung eines Unterschriftenpads in den Berliner Bürgerämtern ist daher den Betroffenen in geeigneter Weise zu vermitteln. Dies ist zurzeit nicht der Fall. Wir haben die Berliner Bürgerämter aufgefordert, dafür zu sorgen, dass den Betroffenen die Möglichkeit des Verzichts der Abgabe von Unterschriften auf Unterschriftenpads ausdrücklich erklärt und z.B. über Aushänge deutlich gemacht wird. Die Unterschriften sind dann konventionell (auf Papier) zu leisten.

Im Rahmen unserer Beteiligung bei der Einführung neuer Verwaltungsverfahren weisen wir auf den rechtskonformen Einsatz moderner Kommunikationsmittel hin und empfehlen vor allem, die Nutzung für die Bürgerinnen und Bürger transparent und nachvollziehbar zu gestalten.

22 § 10 Abs. 1 Berliner Datenschutzgesetz (BlnDSG)

1.5 Kontrolle der bezirklichen Sicherheitskonzepte – Fortschrittsbericht

2013 haben wir mit einer Kontrolle der behördlichen Sicherheitskonzepte in den Bezirksämtern begonnen.

Bis Ende November 2014 übermittelten uns von den zwölf Bezirksämtern sieben als aktuell und gültig erklärte IT-Sicherheitskonzepte, ein Bezirksamt hat in Teillieferungen IT-Sicherheitskonzepte für zwei Standorte übergeben. Die Qualität der Konzepte variiert stark. Beispielhaft seien hier unvollständige bzw. fehlende Netzpläne, fehlende Modellierungen oder fehlende Basissicherheitschecks genannt. Zusammen mit teilweise unsystematischen Darstellungen führt dies dazu, dass sich aus den meisten Konzepten nicht auf den Zustand der Informationssicherheit schließen lässt. Positiv ist anzumerken, dass in einigen Konzepten die zusätzlichen Schutzwerte des Datenschutzes Authentizität, Revisionsfähigkeit und Transparenz teilweise bei der Schutzbedarfsfeststellung berücksichtigt wurden, was aber die Ausnahme darstellt.

Bei der Erstellung sollte künftig berücksichtigt werden, dass behördenspezifische IT-Sicherheitskonzepte die Grundlage der verfahrensspezifischen IT-Sicherheitskonzepte bilden. Daraus folgt, dass in beiden die Schnittstellen zueinander mit den daraus resultierenden Abhängigkeiten klar dargestellt werden müssen. Die verfahrens- und behördenspezifischen IT-Sicherheitskonzepte müssen miteinander abgestimmt werden.

Aufgrund des teilweise unbefriedigenden Zustands der Konzepte werden wir eine Handreichung veröffentlichen, die die Behörden bei der Erstellung von gut strukturierten und übersichtlichen IT-Sicherheitskonzepten unterstützen soll.

Um die Qualität der Konzepte und deren Umsetzung zu verbessern, unterstützen wir ausdrücklich die Weiterbildung der behördlichen IT-Sicherheitsbeauftragten im Rahmen von Schulungen zum IT-Sicherheitsbeauftragen gemäß der Prüfungsordnung der Bundesakademie für öffentliche Verwaltung.

Noch immer haben nicht alle Berliner Bezirke die vorgeschriebenen IT-Sicherheitskonzepte erstellt. Die vorgelegten Konzepte variieren in ihrer Qualität stark. Die Weiterbildung der behördlichen IT-Sicherheitsbeauftragten muss intensiviert werden.

1.6 Das Berliner Open Data-Portal – Fortschritt oder Stillstand?

Im Rahmen des E-Government-Projekts „ServiceStadtBerlin“ hat das Land Berlin im September 2011 als erstes deutsches Bundesland ein eigenes Open Data-Portal als Pilot- und Testprojekt gestartet.[23] Ziel des Portals ist es, durch den freien Zugang zu Datensätzen der öffentlichen Verwaltung eine stärkere Transparenz gegenüber der Öffentlichkeit zu erreichen und darüber hinaus auch die mögliche Weiternutzung der Daten durch Zivilgesellschaft, Privatwirtschaft, Lehr- und Forschungseinrichtungen, Medien und sonstige Dritte anzuregen. Beispiele für die Weiternutzung „offener Daten“ in Form neuer Anwendungen sind z.B. die Kindergarten-Suche[24] oder auch die Internetanwendung „Bürger baut Stadt“, [25] die es Bürgern erleichtern soll, sich an Bauvorhaben und Planfeststellungsverfahren zu beteiligen.

Entsprechend der im Jahr 2012 veröffentlichten Berliner Open Data-Strategie wurde das Open Data-Portal der Hauptstadt[26] schrittweise weiter ausgebaut und im Juni 2013 mit einem neuen Design in den Regelbetrieb überführt.[27] Als weiterer Schritt zur Stärkung des Portals werden seit Oktober 2013 große Teile der amtlichen Geodaten kostenfrei zur Verfügung gestellt, deren Bezug bis dahin nur gegen Gebühr möglich war.[28] Aktuell[29] stehen auf der Webseite

23 http://daten.berlin.de, siehe JB 2011, 1.2.1 (S. 27 ff.)
24 http://daten.berlin.de/anwendungen/kindergarten-suche
25 http://daten.berlin.de/anwendungen/bürger-baut-stadt
26 Siehe dazu zuletzt JB 2013, 1.8
27 http://www.berlin.de/sen/wtf/presse/archiv/20130613.1125.386031.html
28 http://www.stadtentwicklung.berlin.de/aktuell/pressebox/archiv_volltext.shtml?arch_1310/nachricht5075.html
29 Stand: 31. Dezember 2014

895 Datensätze aus 22 verschiedenen Kategorien bereit, die zur Informationsrecherche und Weiterverarbeitung (z.B. für die Entwicklung von Applikationen) von der Öffentlichkeit, Unternehmen, Forschungseinrichtungen und sonstigen Dritten kostenfrei genutzt werden können.

Langfristig ist die Spiegelung der Informationen aus dem Berliner Datenangebot in anderen Portalen in Deutschland und Europa geplant. Dies soll innerhalb der nächsten zwei bis vier Jahre erfolgen.[30] So sind bereits jetzt viele der Daten aus dem Berliner Portal auch im bundesweiten Angebot GovData.de sowie im Portal offenedaten.de zu finden.

Bislang besteht jedoch noch keine gesetzliche Verpflichtung für öffentliche Stellen, Daten zu veröffentlichen und im Open Data-Portal des Landes Berlin einzustellen. Wir haben daher bereits 2013 einen Vorschlag für eine Gesetzesänderung unterbreitet, der entsprechende Veröffentlichungspflichten in das IFG oder das E-Government-Gesetz Berlin aufnimmt.[31]

Sowohl inhaltlich als auch technisch wurde der Ausbau des Berliner Open Data-Angebots durch die Open Data-Arbeitsgruppe begleitet. In der Arbeitsgruppe waren Mitglieder verschiedener Berliner Verwaltungen, insbesondere aus den Bereichen Geodaten, Verkehr, Umwelt, Verbraucherschutz, Gesundheit und Sozialdaten sowie des Amtes für Statistik Berlin-Brandenburg vertreten. Die Landesredaktion sowie das IT-Dienstleistungszentrum Berlin (ITDZ) wirkten bei der Gestaltung des technischen Umfeldes mit. Um die Belange des Datenschutzes zu wahren, war auch ein Vertreter des Berliner Beauftragten für Datenschutz und Informationsfreiheit in der AG durchgängig tätig. Im Februar 2014 hat die Projektgruppe den Abschlussbericht fertiggestellt.[32] Die weitere Entwicklung der Open Data-Thematik im Land Berlin bleibt abzuwarten.

30 Siehe Kurzfassung der Berliner Open Data-Strategie, S. 20
31 JB 2013, 1.7
32 Abrufbar unter http://www.berlin.de/projektzukunft/fileadmin/user_upload/pdf/sonstiges/Open_Data/AG_Open-Data_Abschlussbericht_2014.pdf

Im Sinne der Informationsfreiheit ist die stetige Fortentwicklung des Berliner Open Data-Portals in den letzten Jahren zu begrüßen, da es der Zivilgesellschaft ebenso wie der Wirtschaft und freien Softwareentwicklern den Zugang zu Informationen aus den Datenbeständen der öffentlichen Hand bietet. Gleichzeitig wird dadurch die Transparenz des Handelns der öffentlichen Verwaltung erhöht und den Bürgerinnen und Bürgern mehr Teilhabe an politischen und sozialen Prozessen ermöglicht.

2 Schwerpunkte

2.1 Konsequenzen aus dem anhaltenden NSA-Skandal?

Die Enthüllungen des ehemaligen Geheimdienstmitarbeiters Edward Snowden im Sommer 2013 haben gezeigt, wie sehr der Schutz der Privatsphäre und insbesondere das Recht auf freie, unbeobachtete Kommunikation durch die maßlosen Überwachungspraktiken und den totalen Überwachungsanspruch der amerikanischen National Security Agency (NSA), aber auch anderer Geheimdienste bedroht ist.[33]

Dadurch ist auch noch einmal deutlich geworden, wie ungeschützt elektronische Kommunikation im Internet – sei es beim Abruf von Informationen von Webseiten oder beim Austausch von E-Mails – bisher abläuft. Auf diesen Umstand weisen die Datenschutzbehörden schon seit Jahren hin. Allerdings war vor dem „Summer of Snowden" 2013 weitgehend unbekannt, in welch ungeheurem Ausmaß und mit welchem finanziellen Aufwand[34] Sicherheitsbehörden auf Inhalts- und Verkehrsdaten bei der Nutzung von Telekommunikation und Internetdiensten inzwischen zugreifen.

Die jetzt vorliegenden Informationen lassen darüber hinaus auch befürchten, dass selbst Maßnahmen (z.B. Verschlüsselung und digitale Zertifikate), mit denen man bisher glaubte, besonders wichtige Anwendungen wie das Online-Banking absichern zu können, möglicherweise kompromittiert sind. So ist zu befürchten, dass US-amerikanische Sicherheitsbehörden über die dort geltenden nationalen Regelungen auch amerikanische Anbieter digitaler Zertifikate dazu zwingen, gefälschte Zertifikate auszustellen.

Die amerikanischen Sicherheitsbehörden schrecken nicht einmal vor dem Versuch zurück, bei der technischen Standardisierung Schwächen in kryptografischen Verfahren zugrunde liegenden Basiskomponenten einzubauen. Auf diese

33 Siehe JB 2013, Einleitung

34 Allein in den USA übersteigt das jährliche Budget der Sicherheitsbehörden und ihrer Vertragspartner die Summe von 50 Milliarden Dollar; siehe C. Kurz in der FAZ vom 11. Juli 2014, S. 12: „Ein paar Milliarden mehr dürften es schon sein"

Weise soll das Schutzniveau so abgesenkt werden, dass den Geheimdiensten eine Entschlüsselung der mit diesem Verfahren verschlüsselten Informationen möglich wird.

Darüber hinaus ist deutlich geworden, dass die Geheimdienste weltweit über einen anscheinend beträchtlichen Vorrat nicht dokumentierter Sicherheitslücken für die Betriebssysteme verschiedenster Geräte verfügen, diesen regelmäßig nach Kräften ergänzen und je nach Bedarf einsetzen. Inzwischen wurde bekannt, dass auch der Bundesnachrichtendienst Software-Schwachstellen aufkauft und auf diese Weise die Unsicherheit der Internet-Kommunikation noch erhöht.[35]

Die im Zusammenhang mit den Enthüllungen geführte Debatte über die gezielte Ausspähung des Mobiltelefons der Bundeskanzlerin hat nochmals ein Schlaglicht auf das mangelhafte Sicherheitsniveau der Mobilfunknetze geworfen.

Insgesamt muss man davon ausgehen, dass es eine sichere, unbeobachtete Kommunikation ohne den Einsatz besonderer Sicherungsmaßnahmen derzeit nicht gibt. Politik und Wirtschaft sind gefordert, die erforderlichen Maßnahmen zu treffen, damit ein Schutz der Privatsphäre in der elektronischen Kommunikation wieder möglich wird. Dort, wo dies nicht durch entsprechende Veränderungen der Infrastruktur erreicht werden kann, müssen den Betroffenen Instrumente zum Selbstschutz zur Verfügung gestellt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung auf die zur Gewährleistung der Menschenrechte bei der elektronischen Kommunikation notwendigen Maßnahmen hingewiesen.[36] Darin fordert die Konferenz die Prüfung und Umsetzung von zwölf Einzelmaßnahmen. Dazu zählen neben dem Einsatz sicherer Verschlüsselungsverfahren beim Transport und der Speicherung von Daten und der Bereitstellung einer einfach zu bedienenden Verschlüsselungsinfrastruktur für jedermann auch die Verschlüsselung von Verbindungen zwischen den an der Übertragung

35 Siehe den Bericht „Mut zur Lücke“ in: Der Spiegel 46/2014, S. 34 f.

36 Entschließung vom 27. März 2014 mit Anlage: Gewährleistung der Menschenrechte bei der elektronischen Kommunikation, Dokumentenband 2014, S. 9

beteiligten Netzknoten zum Schutz der Metadaten der Kommunikation in Kombination mit dem Einsatz von Ende-zu-Ende-Verschlüsselung zum Schutz der Inhaltsdaten.

Zur Sicherung der Vertraulichkeit des Abrufs von Informationen aus Internet-Angeboten müssen sämtliche Internet-Angebote sowohl öffentlicher als auch nicht-öffentlicher Stellen die Möglichkeit anbieten, Daten verschlüsselt abzurufen (Einsatz von Transport Layer Security – TLS). Dabei sollten nur Zertifikate verwendet werden, die von vertrauenswürdigen Ausstellern herausgegeben wurden.

Die Konferenz fordert darüber hinaus die Weiterentwicklung innovativer Vorkehrungen zum Schutz der Verkehrsdaten, z.B. von Methoden zur spurlosen oder zumindest metadaten-armen E-Mail-Kommunikation sowie den Ausbau und die Förderung von Angeboten zur anonymen Kommunikation.

Weiterhin fordert die Konferenz die Prüfung und Umsetzung von Angeboten für eine Kommunikation über kontrollierte Routen: Möglichst kurze und geografisch lokale Routen können die Möglichkeit insbesondere ausländischer Nachrichtendienste zum Mitlesen der Kommunikation mindern.[37] Diese Konzepte dürfen jedoch nicht verwechselt werden mit Maßnahmen zur Kontrolle des Internets oder Versuchen, Teile davon abzuschotten. Dies fordern die Datenschutzbeauftragten des Bundes und der Länder gerade nicht.

Schließlich setzt sich die Konferenz auch für eine nachhaltige Verbesserung der Vertraulichkeit in der Mobilkommunikation ein. Dazu gehören der Einsatz wirksamer Verschlüsselungsverfahren und die Einführung einer Authentifizierung von Basisstationen gegenüber den Mobilgeräten. Damit soll u. a. das Abhören der Mobilkommunikation durch den Einsatz von IMSI-Catchern erschwert werden. Solche Einrichtungen sind mittlerweile nicht nur für

37 Die Deutsche Telekom AG hat dies nach eigenen Angaben für E-Mails ihrer Privatkunden bereits umgesetzt; siehe heise online vom 20. November 2014: „Mails unter Telekom-Privatkunden bleiben in Deutschland“

Sicherheitsbehörden, sondern praktisch für jedermann zu geringen Kosten verfügbar.[38] Auch soll die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze beschränkt werden, in die sich das jeweilige Gerät einbucht, sowie den Betreiber des „Heimatnetzes" des Betroffenen. Gegenwärtig ist eine Lokalisierung von Mobilfunkgeräten global für jeden Netzbetreiber möglich, unabhängig davon, ob ein Mobilfunkgerät in seinem Netz eingebucht ist oder nicht.

Weitere Forderungen betreffen die Beschränkung des Cloud Computings[39] mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit, die Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung, die Sensibilisierung von Nutzerinnen und Nutzern moderner Technik sowie die ausreichende Finanzierung von Maßnahmen zur Informationssicherheit. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die o. g. Maßnahmen konkretisiert.[40]

Zwar haben einige Anbieter von Telekommunikationsdienstleistungen in der Zwischenzeit lobenswerte Schritte zur Verbesserung der Datensicherheit und des Schutzes der Privatsphäre bei der elektronischen Kommunikation unternommen. So hat die Deutsche Telekom AG das von ihr betriebene Mobilfunknetz so umgerüstet, dass dort unterdessen zur Verschlüsselung zwischen Mobilfunkgerät und Basisstation in den GSM-Netzen ein Verfahren zur Anwendung kommt, das im Gegensatz zu den vorher verwendeten Versionen nach gegenwärtigem Kenntnisstand nicht durch jedermann entschlüsselt werden kann. Parallel dazu haben einige Anbieter von Smartphones den Schutz der auf den Endgeräten gespeicherten (auch personenbezogenen) Daten durch standardmäßigen Einsatz von Verschlüsselungsverfahren verbessert.

38 Nach einem Bericht in der „ZEIT" sind die dafür notwendigen technischen Komponenten für nicht mehr als 1.500 € zu erwerben, die dazu notwendige Software stehe sogar kostenlos zur Verfügung; siehe „Zeit Online Mobil" vom 17. September 2014: „Achtung Handyfänger". Diese Möglichkeiten werden offenbar auch in der Praxis genutzt: Nach Presseberichten wurden kürzlich in der norwegischen Hauptstadt Oslo zahlreiche IMSI-Catcher unbekannter Herkunft in der Nähe des Parlaments, des Sitzes der Ministerpräsidentin und von einigen Ministerien entdeckt; siehe „Der Tagesspiegel" vom 15. Dezember 2014, S. 5: „Überwachungsgeräte im Regierungsviertel gefunden"

39 Siehe dazu näher 2.2

40 Siehe Fußnote 36: Anlage zur Entschließung vom 27. März 2014, Dokumentenband 2014, S. 9

Einige Anbieter von E-Mail-Diensten haben eine verschlüsselte Übertragung von Nachrichten ihrer Kunden zwischen den Servern der beteiligten Unternehmen vereinbart. Auch werden z.B. für Kurzmitteilungsdienste zunehmend Apps angeboten, die eine wirksame Verschlüsselung der übertragenen Nachrichteninhalte erlauben. Zwar bietet aufgrund der vielfältigen möglichen Angriffsmethoden keine dieser Maßnahmen einen vollständigen Schutz. Kombiniert können sie Verletzungen der Privatsphäre im Vergleich zu der vorherigen Situation aber zumindest erschweren.

Diese Initiativen der Betreiber von Kommunikationsnetzen und -diensten allein reichen jedoch bei Weitem nicht aus. Zur Umsetzung der o. g. Forderungen ist es vor allem auch erforderlich, dass die Bundesregierung die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vornimmt. Hier ist bisher wenig geschehen. Ob der Versuch des Bundesministeriums des Innern erfolgreich sein kann, bei der Vergabe von IT-Dienstleistungsaufträgen von den Vertragspartnern Eigenerklärungen zu verlangen, die den Informationsfluss an ausländische Sicherheitsbehörden verhindern sollen („No-Spy-Erlass"), ist zweifelhaft, zumal die Kontrolle der Einhaltung solcher Erklärungen schwierig sein dürfte. Zumindest trägt der „No-Spy-Erlass" dazu bei, dass die Problematik des Zugriffs ausländischer Sicherheitsbehörden erstmals auch bei der öffentlichen Auftragsvergabe adressiert wird.

Insgesamt bleiben die Bundesregierung und der Gesetzgeber aber aufgerufen, ihre Verantwortung für die Gewährleistung der Menschenrechte bei der elektronischen Kommunikation stärker wahrzunehmen, als dies bisher der Fall ist. Insbesondere muss auch die Kontrolle der Nachrichtendienste in Deutschland effektiver gestaltet werden.[41]

Einzelne Hersteller von Produkten und Anbieter von Dienstleistungen haben lobenswerte Schritte zur Verbesserung des Schutzes der Privatsphäre ihrer Nutzer unternommen. Die bisher getroffenen Maßnahmen reichen jedoch bei Weitem nicht aus. Insbesondere ist die Bundesregierung im Hinblick auf die notwendigen Überprüfungen und Änderungen des Rechtsrahmens bisher weitgehend untätig geblieben.

41 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014: Effektive Kontrolle von Nachrichtendiensten herstellen!, Dokumentenband 2014, S. 22

2.2 Entwicklungen beim Cloud Computing – das Beispiel Office 365

Cloud Computing[42] hat in den letzten Jahren stetig zugenommen.[43] Immer mehr Unternehmen wollen Daten ihrer Kunden oder Beschäftigten in eine Cloud auslagern. Die Aussicht, IT-Kosten zu reduzieren sowie immer und jederzeit auf Daten zuzugreifen, macht diese Produkte sowohl für große und mittelständische Unternehmen als auch für Start Ups attraktiv. Immer öfter nehmen Unternehmen daher unsere Beratung zur Zulässigkeit von Office 365, ein Produkt des US-Konzerns Microsoft, in Anspruch. Aber auch Schulen oder Freizeiteinrichtungen wenden sich an uns, da ihnen die kostenlose Nutzung von Office 365 angeboten wurde und sie einen großen Vorteil in der Nutzung sehen. Um eine Hilfestellung für den Einsatz von Cloud-Diensten im Allgemeinen zu bieten, haben die Arbeitskreise Technik und Medien sowie die Arbeitsgruppe Internationaler Datenverkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierfür die Orientierungshilfe Cloud Computing grundlegend überarbeitet.[44]

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen von Cloud-Services sind alle datenschutzrechtlichen Bestimmungen einzuhalten. Besondere Anforderungen gelten vor allem dann, wenn die Daten in Länder außerhalb des Europäischen Wirtschaftsraums transferiert werden. Die Auswahl des Serverstandortes spielt dabei eine erhebliche Rolle, da dieser u. a. das anzunehmende Datenschutzniveau bestimmt und sich daraus rechtliche Vorgaben ableiten. Darüber hinaus ist von Bedeutung, ob das Produkt Office 365 von nicht-öffentlichen oder öffentlichen Stellen eingesetzt wird.

Nutzung von Office 365 durch Unternehmen

Sofern sich der Serverstandort in den USA befindet, muss die Datenübermittlung zunächst nach dem Bundesdatenschutzgesetz zulässig sein. Das Unternehmen muss für die Datenübermittlung an Microsoft, etwa im Rahmen der

42 Cloud Computing ist die Bereitstellung von Computerressourcen wie Rechenleistung und Speicherplatz als Dienstleistung, die über das Internet erbracht werden.

43 Siehe bereits eingehend JB 2011, 2.1

44 Abrufbar unter http://datenschutz-berlin.de/public/search: Orientierungshilfe Cloud Computing (Stand Oktober 2014)

E-Mail-Anwendung, eine gesetzliche Grundlage oder die Einwilligung der Kunden bzw. Beschäftigten nachweisen, da die Privilegierung der Auftragsdatenverarbeitung bei Empfängern in Drittländern nicht gilt.[45]

Eine Einwilligung ist nur wirksam, wenn sie freiwillig erfolgt.[46] Insbesondere bei Arbeitsverhältnissen ist aufgrund des angenommenen Ungleichgewichts zwischen Beschäftigten und Unternehmen eine solche Freiwilligkeit selten anzunehmen. Aber auch der Transfer von Kundendaten in die Cloud auf der Basis einer Einwilligung erscheint für Unternehmen wenig praktikabel. Für Neukundinnen und -kunden müsste diese von vornherein transparent in den Vertrag aufgenommen werden. Bei Altkundinnen und -kunden stellt sich das Problem, dass kaum alle einwilligen werden und dann folglich die Kundendaten getrennt werden müssten.

Der Transfer kann aber zulässig sein, soweit es zur Wahrung berechtigter Interessen erforderlich ist, dass die Daten in die Cloud von Microsoft übermittelt werden und schutzwürdige Interessen des Betroffenen nicht überwiegen.[47] Dementsprechend muss das berechtigte wirtschaftliche Interesse des Datenübermittlers mit dem Interesse der Betroffenen an einem angemessenen Datenschutzniveau für ihre personenbezogenen Daten abgewogen werden.

Sofern keine sensitiven Daten[48] in die Cloud gegeben werden sollen, wird die Interessenabwägung je nach Einzelfall zu Gunsten oder zulasten des Datenübermittlers ausgehen. Hierfür sind Abwägungskriterien zu entwickeln, wie z.B. die Festsetzung einer Vertragsstrafe, die der Cloud-Anbieter bei Rechtsverstößen zahlen müsste, oder die Schaffung größtmöglicher Transparenz für die Betroffenen.

Problematisch ist die Nutzung von Office 365 aber dann, wenn sensitive Daten übermittelt werden. Es kann nie ausgeschlossen werden, dass Beschäftigte ihre Krankmeldung per E-Mail verschicken oder Kundinnen und Kunden sensitive Informationen an das Unternehmen weiterleiten. Dann wird eine Abwägung der Interessen dazu führen, dass ein Datentransfer in die Cloud nicht zulässig ist.

45 Siehe § 3 Abs. 8 Satz 2 BDSG
46 § 4a BDSG
47 § 28 Abs. 1 Satz 1 Nr. 2 BDSG
48 § 3 Abs. 9 BDSG

Hinzu kommt allerdings, dass bei einer Datenübermittlung in einen Drittstaat wie die USA beim Datenempfänger ein angemessenes Datenschutzniveau herrschen muss.[49] Die Unternehmen als Kunden von Microsoft können dabei einen sog. EU-Standardvertrag vereinbaren, der von der Europäischen Kommission als angemessene Garantien hinsichtlich des Schutzes der Betroffenen anerkannt ist.

Microsoft hat seinen Standardvertrag durch die Art. 29-Datenschutzgruppe prüfen lassen. Diese hat festgestellt, dass die Vertragstexte den EU-Standardvertragsklauseln für die Auftragsdatenverarbeitung entsprechen.[50] Allerdings stellte die Art. 29-Gruppe auch klar, dass es der jeweiligen Aufsichtsbehörde vorbehalten bleibt, die technisch-organisatorischen Maßnahmen zu überprüfen. Eine abschließende technische Prüfung des Produktes Office 365 steht noch aus, sodass gegenwärtig keine Aussage über die technisch-organisatorische Sicherheit getroffen werden kann. Im Arbeitskreis Technik der Datenschutzkonferenz hat das Bayerische Landesamt für Datenschutzaufsicht angeboten, einen externen Sachverständigen mit der Prüfung des Produktes zu beauftragen.

Unabhängig vom Standort des Servers stellt sich aber das Problem der Zuverlässigkeit von Microsoft als Auftragnehmer der Cloud-Dienstleistung. Nach deutschem Datenschutzrecht handelt der Auftragnehmer ausschließlich nach Weisung des Kunden als Auftraggeber.[51] Die amerikanischen Sicherheitsgesetze können amerikanische Unternehmen wie Microsoft aber zwingen, die Daten an amerikanische Behörden zu übermitteln und diese zu verpflichten, dem Kunden die erzwungene Herausgabe nicht mitzuteilen.[52] Es ist daher zweifelhaft, ob man US-amerikanische Auftragnehmer überhaupt als geeignet ansehen kann.[53]

Sofern sich der Serverstandort, wie Microsoft einem Teil der europäischen Kunden zusagt, in Dublin oder Amsterdam befindet, erscheint eine Übermittlung zunächst weniger problematisch. Allerdings wurde uns in einem Gespräch mit Microsoft erläutert, dass es zum Zwecke einer Wartung zu Zugriffen aus

49 §§ 4b, 4c BDSG
50 Beschluss 2010/87/EU der Kommission vom 5. Februar 2010
51 § 11 Abs. 3 Satz 1 BDSG
52 Sog. Gagging Order (Maulkorberlass); siehe JB 2013, 2.2
53 Siehe § 11 Abs. 2 Satz 1 BDSG

Drittstaaten (wie Indien, USA) kommen kann. Zudem hat ein US-Gericht im April entschieden, dass Microsoft die Inhalte von E-Mail-Accounts selbst dann an US-Behörden aushändigen muss, wen diese außerhalb der USA (z.B. in Europa) gespeichert sind. Microsoft hat gegen dieses Urteil Rechtsmittel eingelegt. Eine abschließende Entscheidung hierüber steht noch aus.

Nutzung von Office 365 durch öffentliche Stellen

Neben in Berlin ansässigen Unternehmen erhalten wir auch Anfragen von öffentlichen Stellen. Insbesondere ist die Frage der zulässigen Nutzung für Schulen und sonstige Bildungseinrichtungen von Bedeutung, da Microsoft ihnen das Produkt kostenfrei zur Verfügung stellt.

Die Weitergabe von Daten an Microsoft als Auftragnehmer erfordert auch bei öffentlichen Stellen als Datenübermittler eine rechtfertigende Vorschrift oder eine Einwilligung, wenn sich der Serverstandort in den USA befindet.[54] Hier stellen sich die gleichen praktischen Probleme bei der Einwilligung wie bei der Nutzung durch nicht-öffentliche Stellen, sodass nur eine Rechtsgrundlage im Berliner Datenschutzgesetz in Betracht käme. Eine solche fehlt jedoch.

Bemerkenswert ist, dass nach dem Berliner Datenschutzgesetz keine Datenweitergabe an Drittstaaten im Rahmen der Auftragsverarbeitung vorgesehen ist. Während im Berliner Datenschutzgesetz eine Wartung außerhalb der Europäischen Union erwogen wird,[55] fehlt ein entsprechender Hinweis bei der Auftragsdatenverarbeitung.[56] Hieraus ist abzuleiten, dass eine Weitergabe an Stellen in Drittstaaten im Rahmen der Auftragsdatenverarbeitung für öffentliche Stellen in Berlin nicht zulässig ist. Wegen der Vorbildwirkung der öffentlichen Stellen für eine datenschutzkonforme Nutzung von Dienstleistungen ist dies auch begrüßenswert.

Sofern eine vertragliche Zusicherung vorliegt, dass die Daten ausschließlich in Irland lagern, bedarf es zwar für den Datentransfer keiner rechtfertigenden Vorschrift im Sinne des Berliner Datenschutzgesetzes. Allerdings kann auch Microsoft nicht ausschließen, dass es zu Zugriffen aus den USA zu

54 § 4 Abs. 3 Nr. 3 BlnDSG
55 Siehe § 3 a Abs. 2 Satz 2 Nr. 10 BlnDSG
56 Siehe § 3 BlnDSG und oben 1.3

Wartungszwecken kommt. Daneben stellt sich auch hier das allgemeine Problem der Geeignetheit von Microsoft als Auftragnehmer. Es ist bisher nicht auszuschließen, dass US-Unternehmen zur Herausgabe der Inhalte der Cloud durch amerikanische Behörden verpflichtet werden.

Die Nutzung von Office 365 wirft zahlreiche noch ungeklärte Fragen auf. Im Ergebnis ist es schwer, das Produkt auf „sichere datenschutzrechtliche Füße" zu stellen. Es ist deshalb besonders zu begrüßen, dass einige Unternehmen nach unserer Beratung auf die Nutzung von Office 365 verzichtet haben.

2.3 Gemeinsame Terrorabwehrzentren

Nach dem 11. September 2001 wurden unterschiedliche behördenübergreifende Kooperationsplattformen installiert, die das Ziel verfolgen, eine engere Zusammenarbeit der Sicherheitsbehörden in verschiedenen Bereichen zu gewährleisten. Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) in Berlin-Treptow befasst sich inhaltlich mit der Bekämpfung des islamistischen Terrorismus, das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ) in Köln mit den Bereichen Rechts- und Linksextremismus/-terrorismus, Ausländerextremismus/-terrorismus sowie Spionage einschließlich der Weiterverbreitung von atomwaffenfähigem Material. In beiden Zentren sind alle Landesverfassungsschutzämter und -kriminalämter, das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Militärische Abschirmdienst, die Bundespolizei, der Generalbundesanwalt, das Zollkriminalamt und das Bundesamt für Migration und Flüchtlinge vertreten. Im GETZ ist zusätzlich noch das Bundesamt für Wirtschaft und Ausfuhrkontrolle beteiligt. Zu den Sitzungen werden anlass- und themenbezogen auch Vertreter von Europol eingeladen.

Sowohl im GTAZ als auch im GETZ gibt es Auswertungs- und Analysezentren der nachrichtendienstlichen Behörden (NIAS) und der polizeilichen Behörden (PIAS), in denen sich die entsprechenden Behörden von Bund und Ländern regelmäßig jeweils innerhalb ihres Verbundes austauschen. Darüber hinaus kommen die Behörden von Polizei und Verfassungsschutz aus Bund und

Ländern sowie von den anderen beteiligten Behörden verbundsübergreifend in verschiedenen Arbeitsgruppen zu Sitzungen zusammen, um sich über Sachverhalte zu informieren.

Die Einrichtung des GTAZ und des GETZ beruht nicht auf gesetzlichen Organisationsregelungen oder öffentlich-rechtlichen Vereinbarungen. Die Innenministerkonferenz bzw. das Bundesinnenministerium gingen bei der Einrichtung der gemeinsamen Zentren davon aus, dass aufgrund der mangelnden Außenwirkung und Rechtspersönlichkeit dieser Einrichtungen keine neuen Behörden geschaffen wurden. Die gemeinsamen Zentren sollen sich für ihren Informationsaustausch allein auf die bestehenden Datenübermittlungsvorschriften aus den jeweiligen Fachgesetzen der agierenden Behörden stützen. Auf die Schaffung einer eigenständigen rechtlichen Grundlage bei der Einrichtung dieser Plattformen wurde daher verzichtet.

Die noch nicht abgeschlossene Überprüfung von Datenerhebungs- und -übermittlungsvorgängen der Berliner Verfassungsschutzbehörde und des Polizeipräsidenten im GTAZ und GETZ gestaltet sich für uns schon deshalb nicht einfach, weil die Protokolle teilweise keine standardisierte Form aufweisen. In mehreren Fällen war für uns nicht ersichtlich, welche Behördenvertreter an den Sitzungen teilgenommen haben. Datenerhebungen und -übermittlungen durch Berliner Behörden sowie deren Rechtmäßigkeit können so nicht oder nur schwer nachvollzogen werden. In einigen Fällen war bei den protokollierten Sachverhalten unklar, ob und welche personenbezogenen Daten in den jeweiligen Arbeitsgruppensitzungen zwischen den Akteuren tatsächlich ausgetauscht wurden, obwohl die protokollierten Sachverhaltsschilderungen einen personenbezogenen Datenaustausch nahelegten.

Je nachdem, welche Arbeitsgruppe im GTAZ beziehungsweise GETZ betroffen ist, werden die Protokolle an das Bundesamt für Verfassungsschutz, die jeweiligen Landesverfassungsschutzbehörden, die Landeskriminalämter, den Bundesnachrichtendienst, den Generalbundesanwalt, die Bundespolizei, das Zollkriminalamt, den Militärischen Abschirmdienst, das Bundesamt für Migration und Flüchtlinge sowie gegebenenfalls an Europol versandt. Teilweise bleibt fraglich, ob Vertreter dieser Behörden an den jeweils protokollierten Sitzungen teilgenommen haben und eine Übersendung aller Informationen in den jeweiligen Protokollen notwendig ist.

Jedenfalls bei den Berliner Behörden werden die Protokolle zu Zwecken der Datenschutzkontrolle bis zu zwei Jahre gespeichert, unabhängig davon, ob sie tatsächlich für die konkrete Arbeit der Behörde benötigt werden. Obwohl die Daten im gesperrten Zustand aufbewahrt werden und einem Zweckentfremdungsverbot unterliegen, ist diese Verfahrensweise aufgrund des Missbrauchspotenzials und des informationellen Trennungsgebotes[57] kritisch zu bewerten.

Unsere Prüfung, ob der Informationsaustausch der Berliner Behörden mit anderen nachrichtendienstlichen oder polizeilichen Behörden des Bundes und der Länder im GTAZ und GETZ die Grenzen des informationellen Trennungsprinzips überschreitet, dauert an.

Während den Polizei- und Sicherheitsbehörden die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung obliegt, für die regelmäßig Anhaltspunkte für eine Straftat oder einen Gefahrenverdacht vorliegen müssen, beobachten und berichten Nachrichtendienste über fundamentale Gefährdungen, die das Gemeinwesen als Ganzes destabilisieren können. Auf diesen wesentlichen Unterschied sind die verschiedenen Handlungsweisen dieser Behörden – nämlich offen bei den Polizeibehörden und verdeckt bei den Nachrichtendiensten – und die Ausgestaltung insbesondere der Datenerhebungs- und Verarbeitungsbefugnisse – nämlich enger und präziser wegen der damit verbundenen Zwangsmaßnahmen bei den Polizeibehörden bzw. ohne detailscharfe Ausgestaltung der einzusetzenden Mittel oder Tätigkeitsfelder bei den Nachrichtendiensten – zurückzuführen.[58] Nur bei herausragenden öffentlichen Interessen ist daher ein Informationsaustausch zwischen Nachrichtendiensten und Polizei zulässig.

Im GTAZ und GETZ erfolgt eine Berichterstattung zu den angesprochenen Sachverhalten häufig ohne eine vorherige konkrete Anfrage der teilnehmenden Behörden. Damit können sich die anderen Behörden gewissermaßen „angebotene“ personenbezogene Daten herausgreifen, wenn sie sie für die Aufgabenerfüllung benötigen. Für ein solches „Feilbieten“ sind die

57 BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 123
58 BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 116 ff.

Datenschutzvorschriften in den jeweiligen fachspezifischen Gesetzen jedoch nicht konzipiert worden. Es bestehen gravierende verfassungsrechtliche Zweifel, ob ein solches Vorgehen ohne hinreichend bestimmte gesetzliche Regelung rechtmäßig ist, da es zu einer erheblichen Intensivierung des Informationsaustauschs bei gleichzeitiger Erosion des Trennungsprinzips führt.

Die jetzigen Datenübermittlungsvorschriften stellen zudem durch ihre Formulierung nicht in jedem Fall sicher, dass ein Datenaustausch nur bei herausragenden öffentlichen Interessen zwischen Polizei und Nachrichtendiensten stattfindet. Eine solche Beschränkung ergibt sich nach der Rechtsprechung des Bundesverfassungsgerichts aus dem informationellen Trennungsprinzip. Dagegen kann beispielsweise bei einer weiten Auslegung der Fachgesetze auch eine Übermittlungspflicht bestehen, wenn lediglich Delikte der Allgemeinkriminalität (z. B. Diebstahl oder Sachbeschädigung) betroffen sind, selbst wenn sie nur einen sehr entfernten Zusammenhang mit den Staatsschutzdelikten aufweisen.[59] Eine Beschränkung der Übermittlung von Daten lediglich bei Vorliegen von erheblichen Straftaten ist durch den Wortlaut des Gesetzes nicht vorgesehen. Inwieweit vor diesem Hintergrund die Berliner Behörden solche personenbezogenen Daten in verfassungsrechtlich problematischer Weise übermittelt bzw. im GTAZ bzw. GETZ erhoben haben, ist anhand der uns vorliegenden Protokolle im Rahmen von Einzelfallprüfungen noch näher aufzuklären.

Unabhängig davon haben wir nach den Vorgaben des Bundesverfassungsgerichts in regelmäßigen Abständen die Antiterror-Datei zu überprüfen.

Der Informationsaustausch im GTAZ und GETZ ist datenschutzrechtlich nicht unproblematisch. Wir werden die Zusammenarbeit der Berliner Behörden mit diesen Zentren genauer überprüfen.

59 § 20 Abs. 1 Satz 1 und 2 BVerfSchG und Art. 73 Nr. 10 Buchstabe b und c GG; ebenso § 21 Abs. 1 Satz 1 BVerfSchG i. V. m. § 21 VSG Bln

2.4 Schutz von Mandatsgeheimnissen in Ermittlungsverfahren gegen Abgeordnete

Rechtsanwälte und Notare sind als berufliche Geheimnisträger zur Verschwiegenheit verpflichtet.[60] Die Schweigepflicht dient dem Schutz der Privatsphäre des Mandanten oder von sonstigen Betroffenen und umfasst alle Tatsachen, die den Verpflichteten in ihrer beruflichen Eigenschaft anvertraut oder auf andere Weise bekannt gemacht wurden. Zusätzliche Fragen stellen sich, wenn gegen Abgeordnete ermittelt wird, die zugleich Träger von Berufsgeheimnissen sind.

Im Juni fand aufgrund eines richterlichen Beschlusses in einem strafrechtlichen Ermittlungsverfahren gegen den früheren Senator für Justiz und Verbraucherschutz und heutigen Abgeordneten Michael Braun, der zugleich als Rechtsanwalt und Notar tätig ist, eine Durchsuchung seiner Kanzleiräume statt. Hierbei beschlagnahmten die Ermittlungsbehörden Mandatsunterlagen. Über das Ermittlungsverfahren wurde ausführlich in den Medien berichtet. Herr Braun wandte sich zur datenschutzrechtlichen Bewertung der Angelegenheit an uns.

Vorrangig stellte sich die Frage nach Umfang und Grenzen der Verschwiegenheitspflicht eines beruflichen Geheimnisträgers, der sich öffentlich zu den gegen ihn erhobenen Vorwürfen zur Wehr setzen möchte.

Ungeachtet des hohen Stellenwertes der Vertraulichkeit stehen der Schweigepflicht in einigen Fällen gewichtige Interessen gegenüber, die eine Offenbarung von Geheimnissen zulassen. Solche Offenbarungsrechte sind zwar nicht ausdrücklich im Gesetz geregelt, lassen sich jedoch aus dem Gedanken des rechtfertigenden Notstands[61] sowie dem Recht auf Wahrung eigener berechtigter Interessen[62] in Ausnahmefällen herleiten und sind durch Gerichte für bestimmte Fallgruppen, etwa zur gerichtlichen Geltendmachung von Honoraransprüchen,

60 Siehe insbesondere § 203 Strafgesetzbuch (StGB)
61 § 34 StGB
62 § 193 StGB

zur Abwehr von Regressansprüchen sowie zur eigenen Verteidigung in berufs- und strafrechtlichen Verfahren, anerkannt worden.

In Anlehnung an diese Rechtsprechung kann ein Rechtsanwalt bzw. Notar bei ungerechtfertigten öffentlichen Angriffen gegen ihn in Ausnahmefällen zur Offenbarung von Mandatsgeheimnissen auch gegenüber der Öffentlichkeit berechtigt sein, wenn die drohenden Nachteile für ihn sehr schwer wiegen, er keine anderen Möglichkeiten hat, diesen Nachteilen zu begegnen, und die Mandatsgeheimnisse im Vergleich hierzu von untergeordneter Bedeutung sind.

Notare haben darüber hinaus bei Zweifeln über die Reichweite der Verschwiegenheitspflicht die Möglichkeit, eine Entscheidung der Aufsichtsbehörde herbeizuführen, die sie von sämtlichen straf-, dienst- und zivilrechtlichen Konsequenzen freistellen kann.[63]

Eine weitere Frage betraf die praktische Durchführung von Durchsuchungen und Beschlagnahmen in Rechtsanwaltskanzleien bzw. bei Berufsgeheimnisträgern.

Der Leitende Oberstaatsanwalt und der Polizeipräsident teilten uns mit, dass es keine gesonderte Geschäftsanweisung hierzu gebe. Der Leitende Oberstaatsanwalt hielt insoweit die gesetzlichen Regelungen[64] sowie die dazugehörigen Ausführungsvorschriften[65] für ausreichend konkret. Der Polizeipräsident erklärte, es befinde sich derzeit eine allgemeine Geschäftsanweisung über die Durchsuchung, Beschlagnahme und Sicherstellung sowie die Behandlung von Asservaten in Überarbeitung. Darin werde auf die entsprechenden gesetzlichen Regelungen, u. a. auch auf das strafprozessuale Beschlagnahmeverbot[66] hingewiesen.

Darüber hinaus empfiehlt es sich, konkrete Regelungen zu technisch-organisatorischen Maßnahmen zu treffen, die bei der Durchführung einer Durchsuchung und/oder Beschlagnahme zu beachten sind und hierbei den

63 § 18 Abs. 3 Bundesnotarordnung
64 § 95 Abs. 2 Satz 2 und § 97 Strafprozessordnung (StPO)
65 § 73a der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV)
66 § 97 StPO

Besonderheiten der Stellung von Berufs- bzw. Amtsgeheimnisträgern Rechnung tragen. Denkbar wären etwa spezielle Verschluss- oder Dokumentationsvorgaben.

Soweit eine Durchsuchungsmaßnahme in den Räumen einer Bürogemeinschaft von Rechtsanwälten stattfindet, ist zudem besonders darauf zu achten, dass keine Unterlagen von Geheimnisträgern beschlagnahmt werden, gegen die sich die Ermittlungsmaßnahme nicht richtet. Insoweit sind auch die Mitglieder einer solchen Bürogemeinschaft selbst zum Schutz der einzelnen Mandatsverhältnisse in der Pflicht, Akten mit Mandatsangaben jeweils anwaltsbezogen getrennt in verschlossenen Schränken aufzubewahren, zu denen nur Befugte Zugang haben, und getrennte Terminkalender zu führen. Gleiches gilt für ärztliche Praxisgemeinschaften.[67]

Im Zusammenhang mit der Durchführung eines Ermittlungsverfahrens gegen einen Abgeordneten, der gleichzeitig Berufsgeheimnisträger ist, stellt sich auch die Frage nach der Reichweite der Datenübermittlungsbefugnisse der Ermittlungsbehörden an das Abgeordnetenhaus.

Aufgrund der in der Geschäftsordnung des Abgeordnetenhauses (GO Abghs) niedergelegten allgemeinen Genehmigung des Abgeordnetenhauses zur Durchführung von Ermittlungsverfahren wegen Straftaten gegen eines seiner Mitglieder ist – abgesehen von den hier nicht zutreffenden Ausnahmen[68] – die Staatsanwaltschaft zunächst nur verpflichtet, vor Einleitung des Ermittlungsverfahrens dem Präsidenten des Abgeordnetenhauses unmittelbar Mitteilung hierüber zu machen.[69] Darüber hinausgehende Informationen zum Gegenstand des Ermittlungsverfahrens darf die Staatsanwaltschaft daher zu diesem Zeitpunkt noch nicht ungefragt übermitteln. Hierzu wäre sie lediglich auf Anfrage des Präsidenten des Abgeordnetenhauses berechtigt, jedoch nur in dem Umfang, der dem Präsidenten die Prüfung ermöglicht, ob ein Ausnahmetatbestand erfüllt ist, der nicht der allgemeinen Genehmigung des Abgeordnetenhauses unterliegt.

67 Siehe dazu 5.4
68 Siehe Nr. 1 Satz 1, 3 Anlage 5 GO Abghs
69 Nr. 1 Satz 2 Anlage 5 GO Abghs

Da die allgemeine Genehmigung des Abgeordnetenhauses zur Durchführung von Ermittlungsverfahren wegen Straftaten gegen Abgeordnete grundsätzlich nicht den Vollzug einer angeordneten Durchsuchung oder Beschlagnahme umfasst,[70] ist die Staatsanwaltschaft jedoch vor der Vollstreckung des Durchsuchungsbeschlusses verpflichtet, eine Genehmigung des Abgeordnetenhauses zu beantragen und in diesem Zusammenhang berechtigt, nähere Informationen zum Ermittlungsverfahren an den Präsidenten des Abgeordnetenhauses zu übermitteln. Eine solche Genehmigung wurde nicht eingeholt.[71] Der Senator für Justiz und Verbraucherschutz erklärte hierzu gegenüber dem Abgeordnetenhaus, dass aufgrund dieses Vorfalls zwischenzeitlich Abläufe in der Staatsanwaltschaft, die Aufklärung der Staatsanwälte sowie entsprechende Arbeitsunterlagen verbessert worden seien, sodass sich ein Übersehen der Immunität in einer Einzelfrage nicht wiederholen könne.[72] Wir werden die Umsetzung dieser neuen Vorgaben überprüfen.

Der Antrag für eine solche Genehmigung (und damit auf Aufhebung der Immunität des Abgeordneten) ist mit einer Sachdarstellung und einer Erläuterung der Rechtslage zu verbinden.[73] Die Beschreibung der zur Last gelegten Tat soll die Tatsachen enthalten, in denen die gesetzlichen Merkmale der Straftat gesehen werden, sowie Zeit und Ort ihrer Begehung angeben; die Strafvorschriften sind zu bezeichnen, die als verletzt in Betracht kommen.

Die Staatsanwaltschaft darf jedoch nur Informationen übermitteln, die für das Abgeordnetenhaus erforderlich sind, um über den Antrag auf Aufhebung der Immunität zu entscheiden. Hierfür muss die Staatsanwaltschaft insbesondere einzelfallbezogen prüfen, welche personenbezogenen Informationen dem Parlament zur Beurteilung der Angelegenheit mitzuteilen sind. In Zweifelsfällen empfiehlt sich eine restriktive Handhabung bei der Datenübermittlung, da das Parlament jederzeit die Möglichkeit hat, für seine Entscheidung über den Antrag weitere Daten von der Staatsanwaltschaft anzufordern, soweit es deren Erforderlichkeit für seine Entscheidung begründen kann.

70 Siehe Nr. 2d, Nr. 1 Satz 3 Anlage 5 GO Abghs

71 Siehe u. a. die Erklärung des Präsidenten zur Durchsuchung der Büroräume des Abgeordneten Michael Braun im Abgeordnetenhaus, Plenarprotokoll 17/50, S. 5071 f.

72 Siehe Inhaltsprotokoll des Ausschusses für Verfassungs- und Rechtsangelegenheiten, Verbraucherschutz, Geschäftsordnung 17/45, S. 2 ff.

73 Nr. 192 Abs. 2 RiStBV

Bei der Bewertung der Erforderlichkeit einer Datenübermittlung sollte in Fällen wie dem vorliegenden zudem in besonderem Maße berücksichtigt werden, dass bestimmte personenbezogene Daten im Rahmen eines der Schweigepflicht unterliegenden Mandatsverhältnisses erhoben und verarbeitet wurden und daher besonders vertraulich zu behandeln sind.

Anhand des Ermittlungsverfahrens gegen den Abgeordneten Michael Braun wird exemplarisch deutlich, welche Vielzahl von Besonderheiten bei der Durchführung von Ermittlungsverfahren zu beachten sind, die berufliche Geheimnisträger betreffen.

2.5 Online-Lernplattformen

Unsere Wissensgesellschaft ist von einer fortschreitenden Digitalisierung, Ausdifferenzierung und Vernetzung der Informations- und Kommunikationsstrukturen geprägt. Der sichere Umgang mit elektronischen Medien gehört inzwischen zu den zentralen Kulturtechniken. Vor diesem Hintergrund erlangt die Entwicklung von Fähigkeiten, medial vermittelte Informationen auszuwählen, zu verstehen, zu nutzen und zu kommunizieren, kontinuierlich an Bedeutung.

Nach neuen Erkenntnissen trifft die weitverbreitete Auffassung, Kinder und Jugendliche würden allein durch ihr Aufwachsen in einer von neuen Technologien geprägten Gesellschaft automatisch zu kompetenten Nutzern digitaler Medien, nicht zu[74]. Die Förderung entsprechender Schlüsselkompetenzen bei Kindern und Jugendlichen wird daher zunehmend als Teil des schulischen Bildungsauftrages gesehen. Von den Potenzialen der Identitäts- und Persönlichkeitsbildung, der gesellschaftlichen und kulturellen Teilhabe und Mitgestaltung des sozialen Lebens ausgehend, ist die Vermittlung von Medienkompetenz unter Einbeziehung der Persönlichkeitsrechte der Anwender als eine zentrale Anforderung an Schulen anzusehen.

74 International Computer and Information Literacy Study – ICILS 2013 auf einen Blick, S. 5

Die Ergebnisse der aktuellen JIM-Studie 2014 zeigen auf, dass der Schulalltag diesen Anforderungen noch nicht gerecht wird. [75] Während die 12- bis 19-jährigen Schüler – nach eigenen Angaben – zu Hause im Durchschnitt 51 Minuten pro Tag am Computer oder im Internet etwas für die Schule tun,[76] geben zwei Drittel der Schüler an, dass digitale Medien oder Lernprogramme im Unterricht (z.B. zur Online-Recherche, zum Verfassen von Texten, Präsentationen) kaum bzw. überhaupt nicht zum Einsatz kommen.[77]

Die Kultus- und Bildungsverwaltungen fördern deshalb unter der Bezeichnung „eLearning" oder „eEducation" zunehmend Projekte, die sich mit der Einführung von „virtuellen Klassenzimmern" befassen. Zum Einsatz kommen hier sog. „Learning Management Systems (LMS)". Diese sollen – unter Einsatz moderner Informations- und Kommunikationstechnologien – das Lernen zu jeder Zeit, an jedem Ort, auf unterschiedlichste Weise, allein oder im kommunikativen Austausch ermöglichen und dabei auch die Rolle der Lernenden und Lehrenden neu definieren.

Bei den LMS oder auch „Online-Lernplattformen" handelt es sich um auf Servern betriebene komplexe Softwaresysteme. Sie unterstützen den Lehr- und Unterrichtsbetrieb, ergänzen den Klassenraumunterricht und stellen webbasierte Lernangebote und Werkzeuge für Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen zur Verfügung. Zur Entlastung des Lehrbetriebes können auf den Plattformen zum Teil auch Aufgaben der Schulverwaltung – z.B. elektronisches Klassenbuch, Fehlzeitenmanagement, Stundenplanänderungen und Vertretungsregelungen – erledigt werden.

Die Lehrkräfte, Schülerinnen und Schüler melden sich mit einem personalisierten Benutzerkonto auf der Online-Lernplattform an. Ihr Nutzungsverhalten wird in der Regel gespeichert. Festgehalten wird z.B., welcher Nutzer zu welcher Zeit auf welche Seite zugegriffen hat. Soweit die Lernplattform zur Aufgabenbearbeitung und Lernkontrolle im Unterricht eingesetzt wird, werden auch Leistungsdaten der Schülerinnen und Schüler erfasst. Bereichsspezifische

75 Seit 1998 führt der Medienpädagogische Forschungsverbund Südwest gemeinsam mit dem Südwestrundfunk die JIM-Studie (Jugend, Information, (Multi-)Media) als Langzeituntersuchung durch.

76 JIM-Studie 2014, 9.3, S. 30

77 JIM-Studie 2014, 9.3, S. 32

Regelungen für die Erhebung, Speicherung und weitere Verarbeitung dieser personenbezogenen Daten existieren nicht. Es gelten die allgemeinen datenschutzrechtlichen Bestimmungen des Berliner Schulgesetzes und des Berliner Datenschutzgesetzes.

Danach dürfen Schulen nur die personenbezogenen Daten der Schülerinnen und Schüler verarbeiten, die zur Erfüllung der ihnen zugewiesenen schulbezogenen Aufgaben erforderlich sind.[78] Viele Online-Plattformen registrieren jedoch erheblich mehr Nutzerdaten als für die schulische Aufgabenwahrnehmung erforderlich sind. So wird z.B. in der Regel erfasst, wann, wie oft und zu welchen Zeiten eine Schülerin oder ein Schüler auf der Online-Plattform an bestimmten Aufgaben gearbeitet hat. Diese Daten dürfen von den Lehrkräften nicht eingesehen werden. Die Verfahren sind entsprechend anzupassen.

Die für den Einsatz der Online-Lernplattform datenschutzrechtlich verantwortliche Stelle[79] ist die jeweilige Schule. Als „Herrin der Daten" hat sie über Art, Umfang und Verwendung der Datenverarbeitung maßgeblich zu bestimmen. Insofern unterscheiden sich Online-Lernplattformen positiv von Internet-Communities wie „Google+" oder „Facebook", die in keiner Weise der Kontrolle der Schule unterliegen. Die Schule hat festzulegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt und welche Daten lediglich optional erhoben werden. Als Stammdaten sind in der Regel erforderlich: Name und Anschrift der Schule, Daten zur Anlage von Benutzerkonten, Angaben zur Vergabe von Rollen und Berechtigungen und eine Email-Adresse für die Zusendung von Benachrichtigungen. Weitere Daten kann der Benutzer im Nutzerprofil auf freiwilliger Basis selbst eingeben. Die sog. Logdaten, die auf dem Server abgelegt werden, dürfen nur für die Überwachung der Funktionsfähigkeit und Sicherheit der Systeme und zur Aufklärung einer rechtswidrigen Nutzung der Lernplattform verwendet werden. Entsprechendes sollte in einer verbindlichen Nutzerordnung konkret festgelegt werden. Die Schülerinnen, Schüler und deren Eltern sind in angemessener Weise über den Einsatz einer Lernplattform zu informieren. Sofern die Nutzung bestimmter Module nur mit Einwilligung erfolgt, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht hinzuweisen.

78 § 64 Abs. 1 SchulG
79 Siehe § 4 Abs. 3 Nr. 1 BlnDSG

Der Einsatz von Online-Lernplattformen ist zudem nur unter bestimmten technischen und organisatorischen Rahmenbedingungen zulässig. Die Nutzung der Online-Plattform erfordert einen passwortgeschützten Zugriff. Für die Nutzer bzw. Anwender sind differenzierte Rollenkonzepte (z.B. Administrator, Kursverwalter, Lehrkraft) zu entwickeln und einzurichten. Entsprechend dem Rollenkonzept sind den Teilnehmern differenzierte Zugriffsrechte zuzuweisen. Es sind verbindliche Vorgaben für eine Protokollierung von Datenzugriffen, den Datenexport, die Datenlöschung und die Schnittstellen zu bzw. Trennung von anderen Systemen zu treffen. Insbesondere muss auch auf Online-Lernplattformen die eventuelle Verarbeitung von Schulverwaltungsdaten (z.B. Personaldaten der Lehrkräfte) einerseits und von Daten über Unterrichtsinhalte andererseits getrennt bleiben.

Digitale Medien und Lernmaterialien sowie der Einsatz mobiler Endgeräte im Unterricht eröffnen vielversprechende neue didaktische und pädagogische Möglichkeiten der Wissensvermittlung. Sie bergen jedoch auch erhebliche Risiken bei der Verarbeitung von Schülerdaten. Im Sinne einer datenschutzgerechten Gestaltung der Verfahren sind den Schulen daher verbindliche Vorgaben für den Einsatz von Online-Lernplattformen zu machen.

2.6 Informationszugang bei der Bauaufsicht – eine erste Prüfung von Amts wegen

Die Piratenfraktion im Abgeordnetenhaus erfragt beim Senat seit einiger Zeit im Rahmen von jährlichen Kleinen Anfragen den Umgang der öffentlichen Stellen des Landes Berlin mit dem IFG. In der Antwort auf die zuletzt gestellte Kleine Anfrage[80] hieß es, dass die Häufung von Anträgen in den Bezirken auf Auskünfte des jeweiligen Bau- und Wohnungsaufsichtsamtes sowie des Umwelt- und Naturschutzamtes zurückgehen würde. Die Anzahl der bei den Bezirken gestellten Anträge nach dem IFG reichte jedoch von 49 beim Bezirksamt Tempelhof-Schöneberg über 521 beim Bezirksamt Charlottenburg-Wilmersdorf bis hin zu 2726 beim Bezirksamt Pankow. Angesichts dieser unterschiedlichen Fallzahlen lag die Vermutung nahe, dass die Bezirke für Akteneinsichten bei den

80 „Das Informationsfreiheitsgesetz in der Praxis – Bilanz 2013“, Drs. 17/13046

Bau- und Wohnungsaufsichtsämtern sowie den Umwelt- und Naturschutzämtern unterschiedliche Maßstäbe zugrunde legen.

Wir nahmen die Antwort auf die Kleine Anfrage daher zum Anlass, uns bei den Bezirksämtern zu erkundigen, in wie vielen Fällen und auf welcher jeweiligen Rechtsgrundlage im Jahr 2013 Akteneinsicht in das Bauaktenarchiv, das Baulastenverzeichnis sowie in die Akten des Umwelt- und Naturschutzamtes gewährt wurde. Die Antworten der Bezirksämter zeigten, dass wir bei den Bauaufsichtsämtern an der richtigen Stelle angesetzt hatten:

Mehrere Bezirksämter übersandten zwar Antwortschreiben, beantworteten aber unsere Fragen hinsichtlich der Bauaufsichtsämter inhaltlich entweder gar nicht oder teilten nur bloße Fallzahlen mit, ohne die jeweils zugrunde gelegte Rechtsgrundlage zu benennen.

Hinsichtlich des **Bauaktenarchivs** wurden uns verschiedenste Rechtsgrundlagen genannt. So erkannten zwar einige Bezirke, dass sich die Akteneinsicht durch Nichtbeteiligte nach dem IFG sowie die Akteneinsicht durch Beteiligte nach dem Verwaltungsverfahrensgesetz Berlin[81] richtet. Daneben wurden jedoch auch das Verwaltungsverfahrensgesetz des Bundes[82] und die Bauordnung Berlin[83] als alleinige Rechtsgrundlage aufgeführt. Dabei wurde übersehen, dass für die Bauaufsichtsämter nicht das Verwaltungsverfahrensgesetz des Bundes, sondern das Verwaltungsverfahrensgesetz des Landes Berlin einschlägig ist,[84] und die Bauordnung Berlin überhaupt keine Rechtsgrundlage für die Akteneinsicht in Bauakten enthält.

Hinsichtlich des **Baulastenverzeichnisses** waren die Antworten noch erstaunlicher. So benannten uns nur zwei Bezirke das hierfür allein einschlägige IFG.[85] Daneben wurde auch hier mehrmals das Verwaltungsverfahrensgesetz des Bundes sowie die Bauordnung Berlin genannt. Mehrere Bezirke teilten ferner mit, dass entsprechende Akteneinsichten nicht gezählt würden bzw. überhaupt nicht Gegenstand der Kleinen Anfrage gewesen seien.

81 § 4a Abs. 1 IFG
82 § 29 VwVfG Bund
83 § 59 Abs. 3 BauO Bln
84 § 1 Abs. 1 i. V. m. § 4a Abs. 1 VwVfG Bln
85 Zu den Einzelheiten siehe JB 2013, 18.3.3

Da unsere Befürchtungen sogar noch übertroffen wurden, entschlossen wir uns, den Umgang mit Akteneinsichten in Bauakten sowie ins Baulastenverzeichnis vor Ort zu überprüfen.

Dabei handelte es sich um die erste Prüfung von Amts wegen, die wir nach dem Informationsfreiheitsgesetz vornahmen. Hierzu wählten wir das Bezirksamt Charlottenburg-Wilmersdorf aus, das in der Antwort die zutreffenden Rechtsgrundlagen für die Akteneinsicht in das Bauaktenarchiv und das Baulastenverzeichnis genannt und auch sonst die Rechtslage zutreffend dargestellt hatte. Jedoch ergab sich bei der Prüfung vor Ort, dass das Bezirksamt in der Antwort zwar die geltende Rechtslage zutreffend wiedergegeben hatte, diese jedoch in der bezirklichen Praxis nicht zugrunde gelegt wurde.

Zunächst wurde uns von den zwei insgesamt vorhandenen Vorgängen zu Akteneinsichten nach dem IFG nur ein Vorgang vorgelegt, da sich der weitere Vorgang in der Widerspruchsstelle befand. Nachdem in diesem Vorgang offensichtlich zunächst Unklarheit darüber bestand, ob Akteneinsicht in laufende Vorgänge überhaupt nach dem IFG gewährt werden könne, wurden dem Antragsteller verschiedene Termine unterbreitet, ohne dass dieser auf eine mögliche Gebührenfolge hingewiesen wurde. Nach erfolgter Akteneinsicht wurde auf Grundlage des Ausdrucks des Elektronischen Bau- und Genehmigungsverfahrens eine Gebühr von 10,02 € festgesetzt, die wie folgt begründet wurde: Der Umfang im Sinne von Aufwand sei gering und mit 40 % anzusetzen, die Schwierigkeit durchschnittlich und ebenfalls mit 40 % anzusetzen, der wirtschaftliche Nutzen durchschnittlich und mit 10 % anzusetzen sowie die Bedeutung für den Beteiligten und die wirtschaftlichen Verhältnisse des Antragstellers jeweils durchschnittlich und mit 5 % anzusetzen. Der eigentliche Gebührenbescheid enthielt zwar einen Hinweis auf die richtige Tarifstelle,[86] erschöpfte sich in der Begründung jedoch auf die Nennung der Rechtsgrundlage.

Aus den vier vorgelegten Anträgen auf Akteneinsicht in bzw. Aktenauskunft aus dem Baulastenverzeichnis ergab sich, dass in drei Fällen für eine Negativ-Bescheinigung eine Gebühr von 17 € nach der Baugebührenordnung[87] sowie in einem Fall für die Übersendung einer Kopie des Baulastenblatts eine Gebühr

86 Tarifstelle 1004 b) Nr. 1 des Gebührenverzeichnisses zur VGebO
87 Tarifstelle 9.3 der BauGebO

von 29 € nach der Baugebührenordnung[88] erhoben wurde. In den vorgelegten Bauakten selbst waren keine beantragten bzw. gewährten Akteneinsichten nach dem IFG, dem UIG oder dem Verwaltungsverfahrensgesetz Berlin erfasst bzw. dokumentiert. Schließlich befanden sich im Bauaktenarchiv Gebührenaushänge von zwei externen Kopierdienstleistern, in der beispielsweise für die Anfertigung von Fotokopien im Format A3 schwarz-weiß Gebühren von 0,30 € je Fotokopie ausgewiesen wurden.

Als Ergebnis mussten wir daher festhalten, dass der Umgang des Bezirksamts mit Informationszugangsbegehren hinsichtlich der Bauakten und dem Baulastenverzeichnis in weiten Teilen nicht der geltenden Rechtslage entspricht:

Rechtsgrundlage für die Akteneinsicht in **Bauakten** ist für Verfahrensbeteiligte das Verwaltungsverfahrensgesetz Berlin, für Nichtbeteiligte das IFG, wobei im zuletzt genannten Fall Betroffene vorab anzuhören sind. Weder nach dem Verwaltungsverfahrensgesetz Berlin noch nach dem IFG kommt es auf ein wie auch immer geartetes Interesse des Antragstellers an der Akteneinsicht an, sodass die Akteneinsicht keinesfalls verweigert werden darf, weil kein berechtigtes Interesse des Antragstellers erkennbar ist. Akteneinsichten von Verfahrensbeteiligten sind gebührenfrei,[89] für Akteneinsichten von Nichtbeteiligten sind Gebühren nach der Verwaltungsgebührenordnung Berlin zu erheben.[90] Dabei ist zu beachten, dass nur der tatsächlich entstandene Verwaltungsaufwand zugrunde gelegt werden darf und die wirtschaftlichen Verhältnisse des Antragstellers allenfalls zu dessen Gunsten berücksichtigt werden dürfen.[91] Auch muss die Gebührenhöhe nachvollziehbar begründet werden. Zudem richten sich die Gebühren für die Anfertigung von Fotokopien allein nach der Verwaltungsgebührenordnung.[92] Soweit hierfür externe Kopierdienstleister eingeschaltet werden, dürfen die Gebühren keinesfalls höher ausfallen.[93] Ferner muss die öffentliche Stelle für den Einsatz von externen Kopierdienstleistern

88 Tarifstelle 9.2 der BauGebO
89 Siehe Anmerkung zur Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO
90 § 16 IFG i. V. m. Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO
91 § 5 VGebO; zu den Einzelheiten siehe JB 2013, 18.4 (S. 197 f.)
92 Tarifstellen 1004 d) und 1001 c) des Gebührenverzeichnisses zur VGebO
93 Nach Tarifstelle 1004 d) des Gebührenverzeichnisses zur VGebO werden für Fotokopien bis zum Format A3 schwarz-weiß nur 0,15 € erhoben.

entsprechende Auftragsdatenverarbeitungsverträge abschließen, die den Anforderungen des Berliner Datenschutzgesetzes[94] genügen.

Wir hatten die Bauämter der Bezirke im Mai – schon vor der Prüfung in Charlottenburg-Wilmersdorf – durch ein Rundschreiben[95] auf diese Rechtslage hingewiesen. Das Bezirksamt Charlottenburg-Wilmersdorf hält dieses Rundschreiben jedoch nicht für praktikabel, weil die Anhörung Betroffener und evtl. erforderliche Schwärzungen vor der Akteneinsicht durch Nichtbeteiligte zu viel Aufwand erfordere und personell nicht zu leisten sei.

Rechtsgrundlage für die Akteneinsicht in bzw. Aktenauskunft aus dem **Baulastenverzeichnis** ist bereits seit 2005 allein das IFG, weswegen einerseits jeder Mensch einen entsprechenden Antrag stellen kann[96] (und nicht nur ein berechtigter Personenkreis) und andererseits die hierfür anfallenden Gebühren nur nach der Verwaltungsgebührenordnung zu erheben sind (und nicht nach der Baugebührenordnung).[97] Zum einen dürfen daher für die Negativ-Bescheinigung, dass keine Baulast eingetragen ist, keine Gebühren erhoben werden.[98] Zum anderen sind die Gebühren nur am entstandenen Verwaltungsaufwand sowie an den jeweils erforderlichen Kopien o. Ä. zu bemessen und dürfen daher nicht pauschal mit 29 € je Grundstück festgesetzt werden.[99] Daher ist bei Heranziehung der zutreffenden Rechtsgrundlage keinesfalls mit einer Erhöhung der Gebühren für Baulastenauskünfte zu rechnen, sondern vielmehr mit einer ganz erheblichen Senkung.

Schließlich ist es unerheblich, ob der Antragsteller seinen Antrag auf eine bestimmte Rechtsgrundlage stützt, da die öffentliche Stelle ohnehin alle in Betracht kommenden Rechtsgrundlagen zu prüfen und die für den Antragsteller – sowohl im Hinblick auf den Umfang als auch die mögliche Gebührenfolge – günstigste auszuwählen hat, etwa die gebührenfreie Akteneinsicht in Umweltinformationen vor Ort nach dem UIG.[100]

94 § 3 BlnDSG
95 Rundschreiben vom 21. Mai 2014, Geschäftszeichen 50.651.17
96 § 3 Abs. 1 Satz 1 IFG
97 Zu den Einzelheiten siehe JB 2013, 18.3.3
98 Zu den Einzelheiten siehe 14.3.1
99 Zu den Einzelheiten siehe JB 2013, 18.3.3
100 § 18a Abs. 1 und Abs. 4 Satz 2 Nr. 1 IFG i. V. m. § 2 Abs. 3 UIG

Keinesfalls darf die öffentliche Stelle die Anwendbarkeit des IFG mit dem Argument verneinen, dass hierdurch ein erhöhter Zeitaufwand entstehe, der personell nicht zu leisten sei. Zum einen gehört zur ordnungsgemäßen Aufgabenerfüllung der öffentlichen Stelle auch die Bearbeitung von Informationszugangsbegehren nach dem IFG, wobei der hierfür entstehende Verwaltungsaufwand durch die zu erhebenden Gebühren ausgeglichen wird. Zum anderen dürfen die schutzwürdigen Belange Betroffener an der Geheimhaltung ihrer personenbezogenen Daten nicht dadurch unterlaufen werden, dass diese aus reinen Zweckmäßigkeitserwägungen nicht angehört bzw. nicht beteiligt werden.

Das Ergebnis unserer Prüfung, die Erfahrungen im Rahmen unserer Schlichtungstätigkeit sowie die Antworten auf die Kleinen Anfragen „Das Informationsfreiheitsgesetz in der Praxis“ zeigen, dass der Umgang mit dem IFG – auch 15 Jahre nach dessen Inkrafttreten – weiterhin uneinheitlich und teilweise stark verbesserungswürdig ist.

3 Inneres und Justiz

3.1 ASOG-Novelle – verfassungsrechtlich bedenklich

Das Abgeordnetenhaus berät derzeit über ein Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes.[101,102] Dies soll die anlassbezogene automatische Kennzeichenfahndung durch die Polizei sowie eine Datenübermittlung von der Polizei an Nachrichtendienste zur Aufklärung oder Bekämpfung des internationalen Terrorismus und des gewaltbezogenen Rechtsextremismus ermöglichen.

Bereits im Vorfeld des Gesetzgebungsverfahrens haben wir gegenüber der Senatsverwaltung für Justiz und Verbraucherschutz zum Referentenentwurf Stellung genommen. Unsere Empfehlungen wurden jedoch größtenteils nicht berücksichtigt, weshalb wir sie bei der parlamentarischen Beratung bekräftigt haben.

Zunächst ist es notwendig, den Einsatz der automatischen Kennzeichenfahndung hinsichtlich ihrer Eignung, Notwendigkeit und Auswirkungen zu evaluieren, weil sie wegen ihrer großen Streubreite, der Betroffenheit vieler Unbeteiligter und der verdeckten Durchführung einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Die im Gesetzesentwurf vorgesehene jährliche Berichtspflicht des Senats[103] kann eine solche Evaluierung nicht ersetzen. Sie dient zwar der parlamentarischen Kontrolle der Maßnahme, stellt jedoch keine umfassende wissenschaftliche Begleitung der Einführung der automatischen Kennzeichenfahndung und hierbei insbesondere keine unabhängige Überprüfung der tatsächlichen Eignung der Maßnahme für die vorgesehenen Zwecke und deren Auswirkungen dar.

Nicht geklärt ist bislang zudem die verfassungsrechtliche Zulässigkeit der automatischen Kennzeichenfahndung. Gegen entsprechende Regelungen in den Polizeigesetzen der Länder Baden-Württemberg, Bayern und Hessen wurden

101 ASOG
102 Drs. 17/1795
103 § 24c Abs. 3 ASOG-E

beim Bundesverfassungsgericht Verfassungsbeschwerden erhoben, deren Ergebnis abzuwarten bleibt.

Weiterhin kritisieren wir die vorgesehene Regelung zur Datenübermittlung zwischen der Berliner Polizei und den Nachrichtendiensten.[104] Aufgrund des informationellen Trennungsprinzips[105] dürfen Daten insoweit grundsätzlich nicht ausgetauscht werden. Ausnahmsweise kommt zur operativen Aufgabenwahrnehmung ein Austausch in Betracht, wenn dies herausragenden öffentlichen Interessen dient und hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen bestehen und auch die Eingriffsschwellen für die Erlangung der Daten nicht unterlaufen werden.[106]

Nach der geplanten Vorschrift zur Datenübermittlung zwischen Polizei und Nachrichtendiensten ist zudem derzeit nicht ausgeschlossen, dass Datenübermittlungen zu Kontaktpersonen stattfinden, die von einem Terrorismusbezug der Hauptperson nichts wissen.[107] Das Bundesverfassungsgericht hat in seiner Entscheidung zum Antiterrordateigesetz jedoch ausgeführt, dass Daten zu Kontaktpersonen überhaupt nur von Interesse sein können, wenn sie Aufschluss über die als terrorismusnah geltende Hauptperson vermitteln können.[108] Insofern ist die vorgesehene Regelung derzeit zu weit gefasst und sollte anhand der Vorgaben des Bundesverfassungsgerichts konkretisiert werden.

Die geplanten gesetzlichen Erweiterungen der polizeilichen Befugnisse zur Verarbeitung personenbezogener Daten unterliegen in der derzeitigen Form verfassungsrechtlichen Bedenken und sollten daher vor Beschlussfassung entsprechend den vorgenannten Empfehlungen überarbeitet werden.

104 § 44 Abs. 4 Satz 2 ASOG-E
105 Siehe 2.3
106 Urteil des BVerfG zum Antiterrordateigesetz (ATDG) vom 24. April 2013, 1 BvR 1215/07, Rn. 123
107 Die Formulierung „bedienen will“ in § 25 Abs. 2 Satz 1 Nr. 2 ASOG umfasst auch ein undoloses Werkzeug.
108 BVerfG a.a.O., Rn. 165

3.2 Novelle zum Bundesmeldegesetz

Im Jahr 2015 werden die Landesmeldegesetze durch das Bundesmeldegesetz (BMG) abgelöst, das im Gesetzgebungsverfahren erheblicher datenschutzrechtlicher Kritik ausgesetzt war, [109] die in Teilen Berücksichtigung fand. Nunmehr sah die Bundesregierung weiteren Überarbeitungsbedarf bei der Einführung des neuen Melderechts und legte noch vor dem geplanten Inkrafttreten des Bundesmeldegesetzes einen Gesetzentwurf zu dessen Novellierung[110] vor.

Im Rahmen einer öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages hatte der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Möglichkeit, sich zum Gesetzentwurf zu äußern. Positiv zu bewerten war die im Gesetzentwurf vorgesehene Erweiterung des Rechts auf Selbstauskunft der betroffenen Person über automatisierte Meldeauskünfte mittels Datenträgern sowie die Verbesserung der datenschutzrechtlichen Kontrollmöglichkeit durch die Erstreckung der Protokollierungspflicht auf alle Arten der automatisierten Melderegisterauskunft.

Hingegen war die Anregung des Bundesrates zu kritisieren, sämtliche im neuen § 42 BMG genannten personenbezogenen Daten von Mitgliedern öffentlich-rechtlicher Religionsgesellschaften sowie von deren Familienangehörigen für einen Datenabgleich zu einem bundesweit einheitlichen Stichtag automatisiert an die Religionsgesellschaften zu übermitteln. Dies wird mit der Erleichterung der Einführung von im staatlichen Meldewesen bereits genutzten technischen Standards bei den Religionsgesellschaften begründet.

Es widerspricht den Grundsätzen der Datensparsamkeit und der Erforderlichkeit, lediglich aus Nützlichkeitserwägungen pauschal personenbezogene Daten zu übermitteln, die bei der datenempfangenden Stelle bereits vorhanden sind. Der Berliner Beauftragte hat daher empfohlen zu prüfen, ob eine technische Übertragung der bereits bei den Religionsgesellschaften gespeicherten Daten in die geplanten neuen Standards innerhalb der verantwortlichen Stelle vollzogen

109 JB 2012, 4.1
110 BT-Drs. 18/1284

werden kann. Die Aktualität der Mitgliederdaten bliebe aufgrund der bereits bestehenden regelmäßigen Übermittlungsbefugnisse davon unberührt.

Hingegen waren die Bedenken des Bundesrats hinsichtlich einer Übermittlung von Daten von Personen, die bei einer Religionsgesellschaft beschäftigt sind, an die Arbeitgeber zu teilen. Durch eine solche Datenübermittlung kann es zu einer erheblichen Beeinträchtigung der Interessen der Betroffenen kommen, weil diese unter Umständen mit arbeitsrechtlichen Konsequenzen aufgrund der Benachrichtigung ihres Arbeitgebers über die Führung einer Lebenspartnerschaft oder eine Scheidung bzw. Wiederheirat rechnen müssen. Das gilt selbst dann, wenn man den Religionsgesellschaften als Tendenzbetrieben insofern ein Fragerecht gegenüber Bewerbern einräumt oder Beschäftigte im kirchlichen Bereich entsprechenden dienst- oder arbeitsrechtlichen Mitteilungspflichten unterliegen. Das Melderecht sollte es den Betroffenen überlassen, ob und wann sie ihrem kirchlichen Arbeitgeber Informationen zu ihrem Familienstand zukommen lassen und ob sie ggf. auf steuerrechtliche Vergünstigungen verzichten wollen, um dem Risiko arbeitsrechtlicher Sanktionen zu entgehen.

Der Bundestag übernahm bei der Verabschiedung der Novelle zum BMG den Vorschlag des Bundesrates zu einem einmaligen Meldedatenabgleich, bestimmte jedoch gleichzeitig, dass Daten von Meldebehörden an öffentlich-rechtliche Religionsgesellschaften nicht zu arbeitsrechtlichen Zwecken übermittelt werden dürfen. Die Kirchen haben zugesagt, dass sie die Daten nicht zu solchen Zwecken verwenden werden.

Nach dem Adressdatenabgleich sämtlicher gemeldeter volljähriger Personen im Rahmen der Neuordnung der Rundfunkfinanzierung wird nun ein weiteres Mal aus Zweckmäßigkeitsgründen ein sehr umfangreicher Meldedatenabgleich durchgeführt, der alle Mitglieder einer öffentlich-rechtlichen Religionsgesellschaft sowie deren Familienangehörige betrifft. Diese Entwicklung ist kritisch zu beobachten.

3.3 Stadtweite Veranstaltungsdatenbank

Im Frühjahr beschäftigte sich der Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit im Abgeordnetenhaus nach Medienberichten mit der polizeilichen Datei „Stadtweite Veranstaltungsdatenbank (VDB)". In diesem Zusammenhang wurden wir um Bewertung der Dateiführung und der Auskunftspraxis der Polizei gegenüber Betroffenen gebeten. Wir haben daraufhin eine Überprüfung der Datei bei der Polizei durchgeführt.

In der VDB werden Daten zu Veranstaltungen gespeichert, die die Polizei nach ihrer Bewertung zur Erfüllung ihrer Aufgaben benötigt. Neben Mitteilungen eines etwaigen Veranstaltungsanmelders zu Thema, Art und Ort einer Veranstaltung beinhaltet die Datei u. a. auch polizeiliche Verlaufsberichte, die z.B. Informationen zur Teilnehmerzahl, zu Vorkommnissen während der Veranstaltung und zu polizeilichen Auflagen enthalten.

Derzeit werden personenbezogene Daten drei Jahre in der VDB gespeichert. Die Dauer wird insbesondere mit der hohen Praxisrelevanz der Datenbank für die polizeiliche Einschätzung und Vorbereitung von Veranstaltungen begründet. Personenbezogene Daten dürfen jedoch nur solange gespeichert werden, wie dies für die Polizeiarbeit tatsächlich erforderlich ist.[111] Denkbar wären vorliegend etwa sehr viel kürzere Fristen für die Speicherung personenbezogener Daten, die aufgrund der Thematik der Veranstaltungen nur einmalig relevant sind. Möglicherweise finden bestimmte Veranstaltungen auch so häufig statt, dass es ausreichend ist, das Verhalten des jeweiligen Anmelders bzw. der Teilnehmer innerhalb der letzten ein bis zwei Jahre zu kennen, um den Veranstaltungsverlauf polizeilich richtig einschätzen zu können. Vorstellbar wäre auch eine Differenzierung der Speicherdauer nach Anmelder- und Teilnehmerdaten.

Wir haben der Polizei geraten, eine Evaluation der Nutzungshäufigkeit der in der VDB gespeicherten personenbezogenen Daten durchzuführen und hiernach ein detailliertes Löschkonzept zu erstellen.

Ein weiteres Thema der Prüfung war die Art und Weise der Erteilung von Auskünften aus der VDB an die betroffenen Anmelder von Veranstaltungen. Die

111 § 42 Abs. 1 ASOG

Polizei beschränkt die Auskunft zur Zeit in der Regel auf die vom Anmelder selbst zu seiner Person übermittelten Daten und begründet dies damit, dass die weiteren Daten zur Veranstaltung und nicht zur Person des Anmelders gespeichert würden. Das ist unzulässig.

Die Polizei muss einem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten erteilen, ohne dass hierbei nach dem Zweck der Speicherung oder der Herkunft der Daten unterschieden werden darf.[112] Ausschlaggebend ist, dass ein tatsächlicher Bezug zwischen Information und Person besteht.[113] Sämtliche Daten einer Veranstaltung, die in der VDB gespeichert sind, stehen in einer spezifischen Beziehung zum Anmelder und sind daher Angaben über seine sachlichen Verhältnisse. Hierbei spielt es keine Rolle, ob die Daten von der Polizei auch unter diesem Gesichtspunkt betrachtet werden.

Nur soweit eine Abwägung im Einzelfall ergibt, dass die schutzwürdigen Belange der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen, besteht keine Verpflichtung zur Auskunftserteilung aus der VDB.[114]

Die Führung einer polizeilichen Datenbank über Veranstaltungen ist nicht per se unrechtmäßig. Sie ist jedoch nur dann erlaubt, wenn die gesetzlichen Vorgaben zu Art, Umfang und Dauer der Datenverarbeitung sowie zur Gewährung der Betroffenenrechte strikt eingehalten werden.

3.4 Wohnheim für Asylsuchende: Überwachung auf Schritt und Tritt?

Nachdem wir auf Unzulänglichkeiten bei der Datenverarbeitung in einem Neuköllner Wohnheim für Asylsuchende aufmerksam gemacht wurden, haben wir eine Prüfung vor Ort durchgeführt.

112 § 50 Abs. 1 Satz 1 ASOG
113 Siehe auch § 4 Abs. 1 Satz 1 Berliner Datenschutzgesetz (BlnDSG)
114 § 50 Abs. 2 ASOG

Wir haben festgestellt, dass die Heimausweise der Bewohnerinnen und Bewohner bei jedem Verlassen bzw. Betreten des Geländes vom Sicherheitsdienst des Heimes gescannt werden. Die durch das Ein- und Auschecken entstehenden Bewegungsdaten sowie die Information, ob die Bewohnerin oder der Bewohner an einem bestimmten Tag überhaupt im Haus war oder nicht, werden gespeichert. Diese Information benötigt die private Betreiberin für die Abrechnung gegenüber dem Land Berlin. Die Abrechnung erfolgt pro Tag und pro Bewohnerin bzw. Bewohner. Zum Zeitpunkt der Prüfung war allerdings zehn Jahre lang nachvollziehbar und durch die Heimleitung einsehbar, an welchem Tag und zu welcher Uhrzeit welche Bewohnerin und welcher Bewohner das Wohnheim verlassen haben und wann sie wieder zurückgekehrt sind.

Eine derart umfassende Datenerfassung und -speicherung ist für die erwähnten Abrechnungszwecke nicht notwendig und daher unzulässig. Für die taggenaue Abrechnung ist es vertretbar, wenn die Bewegungsdaten zunächst erfasst, aber noch am selben Tag dahingehend überprüft werden, welche Bewohnerinnen und Bewohner anwesend sind und welche nicht. Lediglich dieser Umstand der An- oder Abwesenheit am jeweiligen Tag kann dann als Nachweis für die abgerechneten Leistungen so lange gespeichert werden, bis die Rechnung vom Land Berlin bezahlt worden ist. Die genauen Bewegungsdaten sind hingegen täglich zu löschen.

Zudem wurden von allen Besucherinnen und Besuchern des Wohnheims Vor- und Zuname, Datum, Uhrzeit und Zielzimmernummer erfragt, gespeichert und nur unregelmäßig gelöscht. Die Erhebung und Speicherung von Besucherdaten ist im Rahmen der zulässigen Ausübung des der Betreiberin zustehenden Hausrechts zu beurteilen. Hierbei müssen sowohl der Anspruch der Asylsuchenden, Besuch zu empfangen, als auch der störungsfreie Betrieb des Wohnheims miteinander in Einklang gebracht werden. Die Betreiberin des Wohnheims hat ein berechtigtes Interesse daran zu wissen, wer das Heimgelände betritt und wieder verlässt. Es ist ein insbesondere aus Sicherheitsgründen, aber auch in finanzieller Hinsicht nachvollziehbares Bedürfnis der Betreiberin zu wissen, wie viele Externe sich auf dem Heimgelände aufhalten. Hierfür dürfen die Namen der Besucherinnen und Besucher und die Zielzimmernummern erfragt werden. Sobald der Besuch das Wohnheim verlässt, sind die Daten allerdings zu löschen.

Darüber hinaus hat die Prüfung ergeben, dass sich in den Fluren der Gebäude und vereinzelt im Hofbereich auf dem Gelände insgesamt 33 Videokameras befinden. Wohnräume und Gemeinschaftsräume werden nicht überwacht. Die in der Vergangenheit im Wohnheim festgestellten Sachbeschädigungen, Überfälle und Diebstähle rechtfertigen die Videoüberwachung in den Fluren der Gebäude und im Hofbereich auf dem Gelände. Da seit der Installation der Videoüberwachung die Vorfälle jedoch deutlich zurückgegangen sind und eine zeitlich unbegrenzte, dauerhafte Überwachung ohne konkrete Zwecke nicht zulässig ist, haben wir der Betreiberin empfohlen, die Situation in den Erfassungsbereichen der Kameras weiterhin genau zu beobachten und die Vorfälle zu dokumentieren bzw. bei der Polizei anzuzeigen. Sofern über einen Zeitraum von etwa einem Jahr keine Vorfälle mehr festgestellt werden, wäre der ursprüngliche Überwachungszweck nicht mehr vorhanden und die Kameras müssten abgeschaltet werden.

Wir haben der Betreiberin aufgegeben, sämtliche festgestellten Mängel zeitnah zu beheben. Die Umsetzung dieser Vorgaben werden wir kontrollieren.

Die Betreiberin des Wohnheims darf zu allen Bewohnerinnen und Bewohnern den Umstand der An- und Abwesenheit als Nachweis für die abgerechneten Leistungen solange speichern, bis die Rechnung vom Land Berlin bezahlt worden ist. Die von den Besucherinnen und Besuchern erfragten Daten sind zu löschen, sobald der Besuch das Wohnheim verlässt. Ergibt die Beobachtung der Situation in den Erfassungsbereichen der Videokameras, dass der ursprüngliche Überwachungszweck nicht mehr vorhanden ist, müssen die Kameras abgeschaltet werden.

3.5 Der Polizeiarbeitsplatz in der BVG-Sicherheitsleitstelle

Im Rahmen eines Maßnahmenpakets für mehr Sicherheit im Öffentlichen Personennahverkehr (ÖPNV) einigten sich der Senat, die Berliner Verkehrsbetriebe (BVG) und die Polizei darauf, einen ständigen Polizeiarbeitsplatz in der Sicherheitsleitstelle der BVG einzurichten. Seit Dezember

2011 wird dieser Arbeitsplatz 24 Stunden im Dreischichtbetrieb mit einem Polizeibeamten besetzt.

Mittlerweile ist eine Vereinbarung zwischen der BVG und der Polizei geschlossen worden, die die Nutzung der Videoüberwachungsanlagen der BVG für polizeiliche Zwecke regelt. Danach kann der Polizeibeamte von seinem Arbeitsplatz aus im Rahmen der polizeilichen Aufgabenerfüllung eine anlassabhängige und eine anlassunabhängige Videoüberwachung durchführen.

Die Kamerabilder sämtlicher U-Bahnhöfe werden in der BVG – früher Sicherheitsleitstelle – auf einer großen Videowand in einem rollierenden Verfahren abgebildet. Nach Kenntnisnahme einer aktuellen Straftat auf einem U-Bahnhof erhält der Polizeibeamte vom BVG-Personal umgehend eine anlassabhängige Freischaltung der Live-Videosequenz des betreffenden U-Bahnhofs. Bis zur Beendigung der polizeilichen Maßnahmen am Einsatzort können diese Live-Videobilder zur Unterstützung der Einsatzkräfte eingesehen werden. Unmittelbar danach wird die Videoübertragung für den Polizeibeamten beendet. Eine Speicherung der eingesehenen Sequenz durch die Polizei erfolgt nicht. Die Frei- und Abschaltung der Videosequenz auf dem Monitor am Polizeiarbeitsplatz erfolgt ausschließlich durch das BVG-Personal. Ein weiterer Grund für eine anlassabhängige Nutzung der Videoüberwachungsanlagen der BVG durch die Polizei ist die Koordinierung und Steuerung der polizeilichen Einsatzkräfte bei Sondereinsätzen und Großlagen, z.B. Demonstrationen. Je nach Einsatzanlass erfolgt die Nutzung zu präventiven oder repressiven Zwecken gemäß den Vorschriften des Allgemeinen Sicherheits- und Ordnungsgesetzes,[115] des Versammlungsgesetzes[116] oder der Strafprozessordnung.[117]

Bei der anlassunabhängigen Videoüberwachung hat der Polizeibeamte uneingeschränkten Zugriff auf die Live-Bilder ausgewählter U-Bahnhöfe, die als kriminalitätsbelastete Schwerpunktbahnhöfe gelten und in das Kriminalitätslagebild der Polizei aufgenommen wurden.[118] Auf diese Weise kann die Polizei verdächtiges Verhalten potenzieller Straftäter frühzeitig erkennen und

115 § 24 ASOG
116 § 12 a VersammlG
117 § 100 h StPO
118 Gegenwärtig sind dies die U-Bahnhöfe Alexanderplatz, Kottbusser Tor und Zoologischer Garten.

umgehend Einsatzkräfte zu dem betroffenen U-Bahnhof entsenden. Das Kriminalitätslagebild wird auf der Grundlage von Kriminalitätsstatistiken regelmäßig aktualisiert und entsprechenden Kriminalitätsentwicklungen angepasst. Die anlassunabhängige Videoüberwachung durch die Polizei darf ausschließlich an den im Kriminalitätslagebild aufgeführten U-Bahnhöfen durchgeführt werden. Eine Datenspeicherung durch die Polizei erfolgt dabei ebenfalls nicht.

Wir begrüßen, dass zwischen der BVG und der Polizei eine Vereinbarung getroffen wurde, die die restriktive Nutzung der Videoüberwachungsanlagen der BVG für polizeiliche Zwecke vorschreibt.

3.6 Videoüberwachung in den öffentlichen Einrichtungen des Landes Berlin

Die stetige Ausweitung der Videoüberwachung haben wir in der Vergangenheit regelmäßig thematisiert. Schwerpunkt unserer Berichterstattung war häufig die datenschutzrechtliche Überprüfung der Videoüberwachung, die von verantwortlichen Stellen aus dem nicht-öffentlichen Bereich durchgeführt wird (z.B. Gewerbetreibende, Hausverwaltungen, Privatpersonen). Die bislang unzureichende Kenntnis darüber, in welchem Umfang Videoüberwachungsanlagen in den öffentlichen Einrichtungen des Landes Berlin zum Einsatz kommen, hat uns veranlasst, diesbezüglich eine Umfrage zu starten. Ausgenommen war die Videoüberwachung an öffentlichen Schulen, die wir bereits 2012 dargestellt hatten.[119]

Um verlässliche Informationen darüber zu gewinnen, in welchem Ausmaß, zu welchem Zweck und unter welchen technisch-organisatorischen Rahmenbedingungen die verantwortlichen öffentlichen Stellen Videoüberwachungsanlagen betreiben, haben wir einen Fragebogen entwickelt. Die behördlichen Datenschutzbeauftragten haben diesen Fragebogen an die in ihren Zuständigkeitsbereichen liegenden öffentlichen Stellen weitergereicht.

119 JB 2012, 12.2.7

Die Rückmeldungen machten deutlich, dass Videokameras von der Berliner Verwaltung im Allgemeinen sehr zurückhaltend und auf wenige Schwerpunktbereiche reduziert eingesetzt werden. Die Anzahl der Kameras ist dabei immer abhängig von der Gebäudegröße. Viele Kameras dienen lediglich als „verlängertes Auge", d.h. die verfügen über keine Aufzeichnungs- oder Speicherfunktion. Diese Live-Beobachtung wird vorzugsweise in Eingangsbereichen öffentlicher Gebäude (der Rathäuser) betrieben. Sie dient dem Pförtnerpersonal lediglich als Unterstützung zur Beobachtung schlecht einsehbarer Bereiche (z.B. Toreinfahrten, Hintereingänge, Innenhöfe).

Positiv ist die Tatsache, dass in einigen Fällen Videokameras mit Speicherfunktion nur außerhalb der regulären Öffnungszeiten Bilddaten aufzeichnen. Sie dienen dem Zweck, Vandalismus, Einbrüche oder Einbruchsversuche zu dokumentieren und die Strafverfolgung zu unterstützen. In der Regel werden Aufzeichnungen innerhalb von Gebäuden während der Öffnungszeiten überwiegend im Bereich von Kassenautomaten und Vorräumen angefertigt.

Bei unserer Auswertung der Rückmeldungen sind nur wenige Fälle aufgefallen, bei denen die verantwortlichen Stellen eine unverhältnismäßig große Anzahl von Videokameras installiert haben, die Bilddaten mehrere Wochen ohne hinreichenden Grund speichern oder Bereiche beobachten, in denen sich Personen über einen längeren Zeitraum aufhalten (z.B. Wartebereiche).

Wir begrüßen den zurückhaltenden Einsatz von Videoüberwachung in den öffentlichen Einrichtungen des Landes Berlin. Die wenigen Fälle, bei denen uns die Videoüberwachung unverhältnismäßig, nicht erforderlich oder ungeeignet erschien, werden wir eingehend prüfen.

3.7 Begrenztes Löschungsmoratorium beim Verfassungsschutz

Aufgrund der anhaltenden Aufklärung der NSU- und NSA-Komplexe durch Gerichte und Untersuchungsausschüsse bat der Berliner Verfassungsschutz um die Zustimmung für die weitere Speicherung von personenbezogenen Daten, die möglicherweise hierzu einen Bezug aufweisen könnten.

Der NSA-Bundestagsuntersuchungsausschuss hat den Berliner Verfassungsschutz nicht um die Übermittlung von Daten gebeten. Der Informationsaustausch mit ausländischen Diensten findet außerdem nur über das Bundesamt für Verfassungsschutz statt. Ein Erkenntnisgewinn war somit nicht zu erwarten, während gleichzeitig zu löschende personenbezogene Daten weiter entgegen der Rechtslage aufgehoben werden sollten.[120] Hierzu haben wir keine Zustimmung erteilt.

Anders stellte sich jedoch die Sachlage im NSU-Komplex dar: Es ist nicht gänzlich ausgeschlossen, dass im Strafverfahren gegen Beate Zschäpe die Gerichte möglicherweise auf Informationen des Berliner Verfassungsschutzes zurückgreifen müssen. Um eine rückhaltlose Aufklärung der den Rechtsstaat tief erschütternden NSU-Gewaltverbrechen zu ermöglichen, würden wir eine fortdauernde Speicherung nicht beanstanden, wenn das Parlament ein begrenztes Löschmoratorium beschließen würde. Allerdings wäre die Verabschiedung eines Einzelfallgesetzes vorzugswürdig.

Das Parlament sollte entscheiden, ob personenbezogene Daten auch dann noch für einen begrenzten Zeitraum zur Aufklärung der NSU-Gewaltverbrechen vom Verfassungsschutz gespeichert bleiben dürfen, wenn dieser die Daten nicht mehr für die Erfüllung eigener Aufgaben benötigt.

3.8 Elektronisches Doping beim Schach

Der Deutsche Schachbund e.V. hat den Spielern der 2. Bundesliga in diesem Jahr eine Vereinbarung zur Unterzeichnung vorgelegt, mit der sich diese der Sanktionierung von Verstößen, insbesondere im Falle der Verwendung unzulässiger technischer Hilfsmittel, unterwerfen sollten. Von den Spielern wurde eine Erklärung verlangt, mit der sie sich auch ohne Anfangsverdacht mit der Überprüfung ihrer elektronischen Geräte einverstanden erklären. Diese Erklärung haben wir überprüft.

120 § 14 Abs. 2 Gesetz über den Verfassungsschutz in Berlin

Zum Hintergrund ist festzustellen, dass der Schachsport zunehmend damit konfrontiert ist, dass mittels moderner Kommunikationsmittel, wie z.B. Smartphones, Schachpartien durch die Verwendung computergestützter Schachprogramme manipuliert werden. Der Deutsche Schachbund e. V. hat die entsprechende Spielervereinbarung entwickelt, um dieses sog. E-Doping unterbinden zu können, ein für uns nachvollziehbares und legitimes Anliegen. Allerdings stellte sich bei der Prüfung der Spielervereinbarung heraus, dass sie nicht den datenschutzrechtlichen Anforderungen an Einwilligungen genügt, insbesondere zu unbestimmt war. Bei der Überprüfung technischer Geräte auf das Vorhandensein unzulässiger Hilfsmittel wird zwangsläufig eine Vielzahl personenbezogener Daten zur Kenntnis genommen. Wir haben darauf hingewiesen, dass es einer präzisen Festlegung bedarf, welche Personen auf welche konkreten Inhalte zugreifen dürfen und wie mit den gewonnenen Informationen umzugehen ist. Da sich die unzulässige Verwendung von Schachprogrammen bzw. Apps im Nachhinein technisch nicht immer nachvollziehen lässt, haben wir dem Deutschen Schachbund e. V. empfohlen, ein generelles Verbot des Beisichführens technischer Geräte während eines Turniers zu prüfen. Er hat uns signalisiert, unseren Vorschlag umzusetzen.

Wir gehen davon aus, dass sich auf diese Weise komplizierte datenschutzrechtliche Fragen im Zusammenhang mit der Kenntnisnahme personenbezogener Daten bei der Überprüfung technischer Geräte von vornherein vermeiden lassen. Dem wichtigen Anliegen, E-Doping im Schach zu verhindern, kann so angemessen Rechnung getragen werden.

3.9 Fahndung bei Facebook

Aus der Praxis

Die Polizei hat in diesem Jahr begonnen, eine Facebook-Fanpage als Plattform für Öffentlichkeitsfahndung im Rahmen der Strafverfolgung zu nutzen. Hierfür veröffentlicht sie bei Facebook anonymisierte Fahndungshinweise, die in personenbezogener Form sodann von einer polizeieigenen Seite abgerufen werden können. Die Polizei erhofft sich hiervon einen größeren Erfolg bei der Aufklärung von Straftaten. Gleichzeitig greift sie damit jedoch in nicht unerheblicher Weise in das Recht auf informationelle Selbstbestimmung der Betroffenen ein.

Im Internet veröffentlichte Fahndungsdaten sind weltweit recherchierbar und aufgrund der möglichen Weiterverwendung durch eine unüberschaubare Vielzahl von Personen praktisch kaum noch zu löschen. In sozialen Netzwerken wie Facebook besteht zudem die Gefahr, dass über die zurzeit regelmäßig nicht abschaltbare Kommentarfunktion Mutmaßungen und Beleidigungen erfolgen, die nicht nur für die direkt Betroffenen einer Öffentlichkeitsfahndung wie Tatverdächtige oder Zeugen, sondern auch für völlig unbeteiligte Personen zum Teil massive Folgen haben können. Die Polizei versucht, dieses Risiko durch eine redaktionelle Betreuung ihrer Fanpage bei Facebook zu begrenzen.

Ein weiteres Problem der Nutzung sozialer Netzwerke zur Öffentlichkeitsfahndung besteht darin, dass derzeit bei den großen Diensteanbietern wie Facebook die Einhaltung der Vorgaben des Telemediengesetzes (TMG) zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung[121] und des Rechts auf anonyme und pseudonyme Nutzung,[122] nicht gewährleistet ist, weil sich zumindest Facebook als US-Unternehmen nicht an das TMG gebunden fühlt.[123] Die Polizei ist in diesem Zusammenhang bestrebt, die Kommunikation mit den Nutzern möglichst außerhalb der sozialen Netzwerke zu führen, und speichert zudem die auf Facebook eingestellten Inhalte der Fanpage ausschließlich auf eigenen Servern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Kritikpunkte an der Öffentlichkeitsfahndung in sozialen Netzwerken in einer Entschließung zusammengefasst.[124] Für den Fall, dass Strafverfolgungsbehörden dennoch die Durchführung solcher Maßnahmen erlaubt werden soll, fordert die Konferenz neben entsprechenden technisch-organisatorischen Vorkehrungen die Konkretisierung der Vorgaben der Strafprozessordnung[125] sowie deren Umsetzungsvorschriften in diesem Bereich unter Beachtung der besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken. Insbesondere ist der Verhältnismäßigkeitsgrundsatz strikt zu beachten.

121 § 13 Abs. 4 Nr. 6, § 15 Abs. 3 TMG
122 § 13 Abs. 6 TMG
123 Mit dieser Frage ist gegenwärtig das Bundesverwaltungsgericht befasst.
124 Entschließung vom 27./28. März 2014: Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!, Dokumentenband 2014, S. 16
125 § 131 Abs. 3, § 131a Abs. 3, §131b Strafprozessordnung (StPO)

Zurzeit berät die Justizministerkonferenz über eine Änderung strafprozessualer Umsetzungsvorschriften zur Öffentlichkeitsfahndung.[126] Wir haben hierzu gegenüber der Senatsverwaltung für Justiz und Verbraucherschutz Stellung genommen und unsere Kritik am Einsatz solcher Maßnahmen bekräftigt.

Es ist anzuerkennen, dass die Polizei bemüht ist, die Nutzung sozialer Netzwerke für ihre Arbeit möglichst datenschutzfreundlich zu gestalten. Jedoch bestehen weiterhin sowohl auf praktischer als auch auf verfahrensrechtlicher Ebene grundsätzliche Bedenken gegen eine Öffentlichkeitsfahndung in sozialen Netzwerken.

3.10 Informationsrechte der Gefangenen

2013 prüften wir die praktische Umsetzung des sehr ambitionierten Justizvollzugsdatenschutzgesetzes[127] und mussten Mängel bei der vorgeschriebenen Unterrichtung der Gefangenen über bestehende Offenbarungspflichten und -befugnisse der Berufsgeheimnisträger feststellen.[128] Nunmehr gibt es Positives über die Beachtung der Rechte der von der Datenverarbeitung der JVA betroffenen Gefangenen zu berichten.

Wir haben den Justizvollzugsanstalten empfohlen, die Gefangenen bereits bei der Aufnahme über deren Informationsrechte, die die Einsichtsrechte in deren Gefangenenpersonalakte umfassen, zu unterrichten. Angesichts der Neuregelung der Informationsrechte der Gefangenen, die der Gesetzgeber verfassungsrechtlich als geboten ansah,[129] hielten wir es zur Ermöglichung der Wahrnehmung dieser Rechte für sinnvoll, die Gefangenen hierüber entsprechend aufzuklären.[130] Gesetzlich vorgesehen ist eine solche umfassende Unterrichtung der Gefangenen bislang nicht.

126 Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV)
127 JB 2011, 2.2.3
128 JB 2013, 5.2
129 Drs. 16/3705, S. 55
130 Siehe auch § 5 Abs. 2 des Gesetzes über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (StVollzG)

Unserer Empfehlung wurde gefolgt. Zukünftig werden die Gefangenen im Formular des Aufnahmeprotokolls ausdrücklich auf ihre Informationsrechte hingewiesen, und der entsprechende Gesetzestext wird ausgehändigt. Für eine schnelle Umsetzung unseres Vorschlags sorgte der von der Senatsverwaltung für Justiz und Verbraucherschutz neu eingesetzte Datenschutzkoordinator für den Berliner Justizvollzug und die Sozialen Dienste der Justiz.

Es ist lobenswert, dass die Justizvollzugsanstalten die Gefangenen über die gesetzlichen Bestimmungen hinaus in der Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung unterstützen.

4 Jugend und Soziales

4.1 Videoaufnahmen in Kitas

Aus der Praxis

Aus der Tagespresse haben wir erfahren, dass in einigen Kindertageseinrichtungen das Verhalten der Kinder und ihrer Erzieherinnen und Erzieher im Kitaalltag bereits seit geraumer Zeit mit Videokameras gefilmt und dabei umfangreiches Material ausgewertet wird. Die Aufnahmen erfolgen im Rahmen eines vom Bundesministerium für Familie, Senioren, Frauen und Jugend geförderten und vom Deutschen Jugendinstitut durchgeführten bundesweiten Projektes zur Sprachförderung.

Die Einverständniserklärungen der Eltern und der pädagogischen Fachkräfte, die das Deutsche Jugendinstitut für alle teilnehmenden Einrichtungen erstellt hat, genügen den datenschutzrechtlichen Anforderungen nicht. Die Dokumentation des Handelns von Kindern und pädagogischen Kräften mittels Videoaufnahmen berührt deren Persönlichkeitsrechte in besonderem Maße. Die verwendeten Erklärungen sind zu unbestimmt. Insbesondere ist es für die Eltern nicht überschaubar, welchen Stellen das entstandene Material zur Verfügung gestellt werden soll. Ob sich die Zusicherung, das für Schulungszwecke und Vorträge verwendete Material werde nicht im Internet veröffentlicht, tatsächlich einhalten lässt, ist fraglich. Auch bestehen Zweifel, dass in der praktischen Umsetzung immer gewährleistet werden kann, dass nur diejenigen Kinder gefilmt werden, für die eine Einwilligung erteilt worden ist.

Besonders problematisch ist die Einholung von Einwilligungserklärungen von den pädagogischen Fachkräften. Die engen Anforderungen des Bundesdatenschutzgesetzes[131] für die Datenverarbeitung im Beschäftigungsverhältnis sind nicht erfüllt. Angesichts des Abhängigkeitsverhältnisses von Beschäftigten zu ihrem Arbeitgeber können Einwilligungen grundsätzlich nicht freiwillig und daher nicht wirksam sein.

Wir haben die beteiligten Kindertageseinrichtungen aufgefordert, die Filmaufnahmen einzustellen und das Material zu löschen. Die Senatsverwaltung

131 § 32 Bundesdatenschutzgesetz (BDSG)

für Bildung, Jugend und Wissenschaft, die als Kitaaufsicht ebenfalls zuvor nicht in den Prozess eingebunden worden war, haben wir entsprechend informiert und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beteiligt. Da an dem vom Bundesministerium geförderten Projekt bundesweit zahlreiche Kindertageseinrichtungen beteiligt sind, hat dieses ebenfalls eine rechtliche Prüfung veranlasst. Bis zum Abschluss der Prüfung haben wir uns mit einer Sperrung der bereits vorhandenen Aufnahmen einverstanden erklärt.

Wir haben gegenüber den Beteiligten deutlich gemacht, dass eine frühzeitige Beteiligung der Datenschutzbeauftragten des Bundes und der Länder bereits bei der Planung entsprechender Projekte notwendig ist, um die datenschutzrechtlichen Möglichkeiten und Grenzen von vornherein zu definieren.

4.2 Weitergabe von Einkommensdaten bei Unterhaltsbeistandschaft

Immer wieder erreichen uns Eingaben, mit denen sich meist unterhaltsverpflichtete Väter darüber beschweren, dass die Jugendämter bei der Berechnung des Unterhalts für gemeinsame minderjährige Kinder Einkommensdaten an die Kindesmutter weitergeben.

Macht das Jugendamt im Rahmen der sog. Unterhaltsbeistandschaft, meist auf Antrag der Kindesmutter, die Rechte des Kindes gegenüber dem unterhaltsverpflichteten Kindesvater geltend, nimmt es eine andere Rolle ein als bei der Gewährung von Hilfen zur Erziehung. Das Jugendamt überträgt die Aufgaben des Beistandes einzelnen seiner Beamten oder Angestellten.[132] Der Beistand macht für das minderjährige Kind den gegenüber dem Unterhaltsverpflichteten bestehenden zivilrechtlichen Auskunftsanspruch[133] geltend. Der unterhaltsverpflichtete Elternteil ist verpflichtet, über Einkünfte und Vermögen Auskunft zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltsverpflichtung erforderlich ist. Diese Pflicht gilt gegenüber dem

132 § 55 Sozialgesetzbuch – Achtes Buch (SGB VIII)
133 § 1605 Bürgerliches Gesetzbuch (BGB)

minderjährigen Kind bzw. der Kindesmutter als gesetzlicher Vertreterin. Indem das Jugendamt diese Ansprüche geltend macht, wird es ebenfalls als gesetzlicher Vertreter des Kindes tätig. Dieser besonderen Rolle des Jugendamtes tragen auch die datenschutzrechtlichen Regelungen Rechnung. Der Beistand darf Sozialdaten erheben und verwenden, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Da der Beistand und die Kindesmutter gleichberechtigt nebeneinander stehen, ist es notwendig, dass auch die Kindesmutter über den Stand der Beitreibung des Unterhaltes informiert ist. Konkret bedeutet dies, dass es zur Durchsetzung der Unterhaltsansprüche notwendig ist, dass die unterhaltsrechtlich relevanten Daten auch dem antragstellenden Elternteil zugänglich gemacht werden. Nur so ist eine Vertretung im Interesse des Kindes möglich.

Zu beachten ist auch, dass dem Jugendamt lediglich eine Pflicht zur kursorischen Prüfung obliegt, sodass nicht erwartet werden kann, dass das Jugendamt vor der Übersendung Schwärzungen von Einzelangaben vornimmt. Die Unterhaltsverpflichteten sollten bereits beim Einreichen der Unterlagen darauf achten, lediglich die unterhaltsrelevanten Unterlagen vorzulegen bzw. Schwärzungen vorzunehmen. Wir gehen davon aus, dass sich Probleme in der Praxis dann vermeiden lassen.

Die Weitergabe unterhaltsrelevanter Informationen an die Kindesmutter ist zulässig.

4.3 Jugendberufsagentur – fürsorgliche Beratung statt „fürsorglicher Belagerung“

Um jungen Menschen den Einstieg in das Berufsleben zu erleichtern, soll in Berlin ähnlich wie in der Freien und Hansestadt Hamburg eine Jugendberufsagentur (JBA) eingerichtet werden. Die Agentur für Arbeit, die Jobcenter, die Jugendämter und die Berufsschulen sollen dabei ihre Leistungen „kundenfreundlich unter einem Dach“ anbieten. Für den Aufbauprozess der JBA wurde am 12. Juni 2014 das Projekt „Jugendberufsagentur in Berlin umsetzen!“ gestartet. Wir haben das Projekt intensiv begleitet, insbesondere haben wir in der Arbeitsgruppe „Datenschutz und Datensicherheit“ maßgeblich mitgewirkt.

Die hohe Jugendarbeitslosigkeit in Berlin soll gesenkt werden, indem jungen Menschen der Übergang von der Schule in den Beruf erleichtert wird. In dieser Phase stehen den jungen Menschen viele verschiedene Institutionen zur Verfügung, nämlich die Agentur für Arbeit, die Jobcenter, die Jugendämter und die Berufsschulen. Zukünftig sollen diese Institutionen ihre Leistungen „kundenfreundlich unter einem Dach" anbieten. Die JBA Berlin wird aber keine eigene Rechtspersönlichkeit besitzen. Das heißt:

1. Jede Institution bleibt jeweils für sich eigenständig bestehen.
2. Jede Institution ist für Personal-, Sach- und Finanzmittel selbst verantwortlich.
3. Jede Institution hat eine eigene Rechtsbeziehung zu den Jugendlichen.

Die JBA Berlin ist also keine neue Organisation, sondern ein reines Arbeitsbündnis der beteiligten Institutionen.

Das Projekt „Jugendberufsagentur" wird von der Senatsverwaltung für Bildung, Jugend und Wissenschaft geleitet. Wichtigstes Projektziel ist es, eine Kooperationsvereinbarung für die Bündnisbeteiligten zu formulieren. Diese regelt die Zusammenarbeit und damit auch die Datenverarbeitungsprozesse. Dabei sind insbesondere folgende Aspekte zu beachten:

- Alle Schülerinnen und Schüler der allgemein- und berufsbildenden Schulen sollen berufsorientierende Leistungen der Agentur für Arbeit in Anspruch nehmen und ab Klassenstufe 9 an einem Berufsberatungsgespräch teilnehmen.[134] Eine Verpflichtung dazu besteht allerdings nicht.
- Damit die Agentur für Arbeit Kontakt zu den Jugendlichen aufnehmen kann, ist vorher eine Einwilligungserklärung der Jugendlichen bzw. ihrer Erziehungsberechtigten erforderlich. Mit dieser Einwilligungserklärung stimmen sie zu, dass die Schule die erforderlichen Daten an die Agentur für Arbeit übermittelt, damit diese sie beraten, vermitteln und fördern kann.
- Für die Aufgabenerfüllung der einzelnen Institution kann es notwendig sein, dass die Daten der Jugendlichen ausgetauscht werden müssen. Die Daten

134 Siehe hierzu § 33 SGB III (Berufsorientierung) und § 34 SGB III (Berufsberatung)

dürfen nur dann ausgetauscht werden, wenn das Sozialgesetzbuch[135] dies erlaubt oder eine Einwilligungserklärung eingeholt wird.

- Zu Schülerinnen und Schülern, die nach der Beratung weiterhin ohne eine Anschlussoption bleiben, wird seitens der Agentur für Arbeit nur dann nochmals Kontakt aufgenommen, wenn diese hierzu eine Einwilligung gegeben haben.
- Für die Schulorganisation, die Schulentwicklungsplanung sowie die Kontrolle und Durchsetzung der Schul- und Berufsschulpflicht soll eine automatisierte Schülerdatei[136] geschaffen werden. Diese darf nur für die gesetzlich vorgesehenen Zwecke und nicht für Aufgaben im Zusammenhang mit der JBA Berlin genutzt werden.

Der Erste Bürgermeister der Freien und Hansestadt Hamburg soll im Zusammenhang mit der dortigen Jugendberufsagentur – möglicherweise scherzhaft – von einer angestrebten „fürsorglichen Belagerung“[137] der Jugendlichen gesprochen haben. Auch wenn es mitunter für die beteiligten Stellen schwierig ist, den Jugendlichen die gesetzlich vorgeschriebenen Angebote zur Berufsberatung und Orientierung nahezubringen, müssen sie dabei stets die Selbstbestimmung der jungen Menschen respektieren. Statt „fürsorglicher Belagerung“ sollten fürsorgliche Beratung und Begleitung das Ziel sein.

Die Agentur für Arbeit, die Jobcenter, die Jugendämter und die Berufsschulen wollen ihre Leistungen in einem Arbeitsbündnis „kundenfreundlich unter einem Dach“ anbieten. Datenflüsse zwischen den Bündnisbeteiligten der JBA dürfen nur erfolgen, wenn dies gesetzlich geregelt ist oder Einwilligungserklärungen vorliegen.

135 § 69 SGB X, §§ 64,65 SGB VIII
136 § 64 a SchulG; dazu siehe JB 2010, 9.2.1
137 Vgl. den gleichnamigen Roman von Heinrich Böll aus dem Jahr 1979

4.4 Übermittlung von Sozialdaten an die Polizei bei Verdacht des Abrechnungsbetrugs

Für die Leistungsgewährung nach dem Sozialgesetzbuch Zwölftes Buch (SGB XII) nutzen die Sozialämter die IT-Fachsoftware OPEN/PROSOZ. Die Senatsverwaltung für Gesundheit und Soziales hat auf die in OPEN/PROSOZ gespeicherten Sozialdaten zugegriffen und die Sozialdaten mehrerer hundert Sozialleistungsempfänger an das Landeskriminalamt weitergegeben. Bei diesen Sozialdaten handelte es sich um das konkrete Sozialamt, das Aktenzeichen und das Geburtsdatum des jeweiligen Hilfeempfängers. Hintergrund war ein vom Landeskriminalamt geführtes Ermittlungsverfahren wegen Abrechnungsbetrugs durch zwei Pflegedienste. Zu den Geschädigten der verdächtigten Pflegedienste gehören auch Sozialleistungsempfänger bzw. die die Kosten tragenden Sozialämter. Um an die betroffenen Sozialämter herantreten und die Ermittlungen dort fortsetzen zu können, hatte das Landeskriminalamt sich mit einem Auskunftsersuchen an die Senatsverwaltung für Gesundheit und Soziales gewandt.

Der Zugriff auf die in OPEN/PROSOZ gespeicherten Daten durch die Senatsverwaltung für Gesundheit und Soziales und die anschließende Datenübermittlung an das Landeskriminalamt waren unzulässig.

Sowohl bei den in OPEN/PROSOZ gespeicherten als auch bei den an das Landeskriminalamt weitergegebenen Daten handelt es sich um Sozialdaten. Das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden.[138]

Anders als die Senatsverwaltung meint, sind die betroffenen Leistungsempfänger anhand der an das Landeskriminalamt übermittelten Datensätze bestimmbar. Mithilfe der weitergegebenen Angaben zum betroffenen Sozialamt, zum Aktenzeichen und Geburtsdatum des jeweiligen Leistungsempfängers ist dessen

138 § 67 Abs. 1 Satz 1 SGB X

Identität ohne unverhältnismäßigen Aufwand feststellbar. Ferner kann, wie der zugrunde liegende Fall zeigt, auch die Senatsverwaltung für Gesundheit und Soziales selbst den Personenbezug durch einen (wenn auch unzulässigen) Zugriff auf die in OPEN/PROSOZ gespeicherten Daten herstellen.

Die Senatsverwaltung hat in Kenntnis der eigenen Unzuständigkeit auf die Daten zugegriffen und dadurch den ihr zugewiesenen Aufgabenbereich bewusst überschritten. Auch bei der anschließenden Datenübermittlung war der Senatsverwaltung bekannt, dass das Landeskriminalamt das jeweilige Auskunftsersuchen an die dafür originär zuständigen Sozialleistungsbehörden, also an die bezirklichen Sozialämter, hätte richten müssen.

Die Vorgehensweise der Senatsverwaltung für Gesundheit und Soziales wurde beanstandet.[139] Zudem haben wir der Senatsverwaltung für zukünftige Anfragen des Landeskriminalamtes einen Lösungsweg aufgezeigt und vorgeschlagen, Auftragsdatenverarbeitungsverträge mit den Sozialämtern abzuschließen. Die Sozialämter müssten die Senatsverwaltung für Gesundheit und Soziales damit beauftragen, OPEN/PROSOZ-Daten danach zu filtern, ob es in dem jeweiligen Sozialamt Sozialleistungsempfänger gibt, die von dem unter Betrugsverdacht stehenden Pflegedienst betreut werden. Bei einer erfolgreichen Recherche würde die Senatsverwaltung den Sozialämtern dann lediglich die Aktenzeichen der von dem Pflegedienst betreuten Sozialleistungsempfänger mitteilen.

Die Senatsverwaltung hat unsere Empfehlungen umgesetzt.

Benötigt das Landeskriminalamt zur Erfüllung seiner Aufgaben Sozialdaten, sind grundsätzlich nur die originär zuständigen Sozialleistungsbehörden zur Auskunftserteilung befugt. Die Senatsverwaltung für Gesundheit und Soziales darf nur dann auf die in OPEN/PROSOZ gespeicherten Sozialdaten zugreifen und Auszüge daraus an das Landeskriminalamt übermitteln, wenn sie vorher von den Sozialämtern damit beauftragt worden ist.

139 § 26 Abs. 1 BlnDSG

5 Gesundheitswesen

5.1 Änderung des PsychKG

Nachdem wir bereits 2010 zu einem ersten Entwurf der Neufassung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) Stellung genommen hatten, übersandte uns die Senatsverwaltung für Gesundheit und Soziales im Juli 2014 nach nunmehr vier Jahren einen überarbeiteten Gesetzesentwurf.

Auch bei diesem Entwurf bestanden hinsichtlich einiger Regelungen weiterhin datenschutzrechtliche Bedenken. So war u. a. vorgesehen, dass durch die Regelung der Befugnisse der Beschäftigten des Sozialpsychiatrischen Dienstes unzulässig in das Grundrecht auf Unverletzlichkeit der Wohnung hätte eingegriffen werden können. Zudem sollte eine Regelung zur Anfertigung von erkennungsdienstlichen Unterlagen der untergebrachten Personen geschaffen werden, die nicht zwischen den verschiedenen Unterbringungsvarianten differenzierte. Auch weitere Vorschriften zur Weitergabe von Daten an Dritte, zur optischen und akustischen Überwachung der ein- und ausgehenden Kommunikation sowie zur Dauer der Speicherung von Daten begegneten datenschutzrechtlichen Bedenken.

In der Zwischenzeit hat uns die Senatsverwaltung einen nochmals überarbeiteten Gesetzesentwurf übersandt, bei dem erfreulicherweise die von uns vorgeschlagenen Änderungen überwiegend berücksichtigt wurden.

Wir begrüßen, dass der Prozess zur umfangreichen Neufassung des PsychKG nunmehr voranschreitet. Wir werden den Gesetzgebungsprozess auch weiterhin konstruktiv begleiten. Der Gesetzgeber sollte Regelungen schaffen, bei denen das Recht auf informationelle Selbstbestimmung der Patientinnen und Patienten hinreichend gewahrt wird.

5.2 Umsetzung des Krebsfrüherkennungs- und -registergesetzes

Das am 9. April 2013 in Kraft getretene Krebsfrüherkennungs- und -registergesetz verpflichtet die Länder, klinische Krebsregister einzurichten. Dabei bleiben die für die Einrichtung und den Betrieb der klinischen Krebsregister notwendigen Bestimmungen einschließlich datenschutzrechtlicher Regelungen dem jeweiligen Landesrecht vorbehalten.

In der Zwischenzeit hat das Land Berlin die Entscheidung getroffen, zusammen mit dem Land Brandenburg ein gemeinsames klinisches Krebsregister einzurichten. Dazu ist unter Leitung der Senatsverwaltung für Gesundheit und Soziales eine Arbeitsgruppe eingerichtet worden, an der Krankenkassen, die Kassenärztliche Vereinigung, die Krankenhausgesellschaft und die Ärztekammer beteiligt sind. Vertreterinnen und Vertreter des Landes Brandenburg, der Ärztekammer Brandenburg und des Tumorzentrums Berlin e. V. werden hinzugezogen.

Wir haben den Senator für Gesundheit darauf aufmerksam gemacht, dass folgende Aspekte bei der Umsetzung besondere Aufmerksamkeit verdienen:

Den Betroffenen muss ein wirksames Widerspruchsrecht gegen die Speicherung ihrer Daten im Register gewährt werden. Die Erfahrungen beispielsweise mit dem bundesweiten Kinderkrebsregister zeigen, dass die Berücksichtigung des Selbstbestimmungsrechtes der Betroffenen den nötigen Grad der Vollständigkeit der Erfassung nicht gefährdet.

Den Registern ist eine Vielzahl von Aufgaben zugewiesen, die eine abgestufte Datengrundlage benötigen. Dem sollte mit einer Gliederung in einen versorgungsnahen Bereich und in einen klinischen Registerbereich entsprochen werden, wie sie von einer Reihe von Ländern auf der Basis bestehender Strukturen geplant ist. Wie im epidemiologischen, so genügen auch im klinischen Registerbereich pseudonymisierte Daten zur Aufgabenerfüllung.

Daten über Krebskranke, die mit ihrem Namen versehen sind, sollten nur bei Einrichtungen gespeichert werden, die an der Krebsbehandlung beteiligt sind.

Diese Daten werden zur Förderung der direkt patientenbezogenen Zusammenarbeit bei der Krebsbehandlung gespeichert und den behandelnden Leistungserbringern zur Verfügung gestellt. Sie sind am besten dort aufgehoben, wo sie vorwiegend zur Anwendung kommen werden, nämlich bei den leistungsfähigen Berliner Tumorzentren, die bereits jetzt klinische Krebsregister betreiben.

Bei der Bereitstellung von Daten der Krebsregistrierung für behandelnde Ärzte muss der besonderen Schutzwürdigkeit der erfassten Angaben Rechnung getragen werden. Sie geben ein umfassendes Bild über die Gesundheit der betroffenen krebskranken Personen. Dies geht bis dahin, dass erkennbar wird, mit welcher Lebenserwartung die Betroffenen zu rechnen haben.

Die Sicherheitsanforderungen sind folglich außerordentlich hoch. Überdies muss eine zuverlässige Überprüfung erfolgen, dass eine Person, die diese Daten abruft, tatsächlich die bzw. den Betroffenen behandelt und die Daten benötigt.

Eine Hilfestellung gibt hier ein Katalog von Anforderungen an die Übermittlung von Krebsregisterdaten, der von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf unsere Initiative hin beschlossen wurde.[140]

Wir haben die Senatsverwaltung aufgefordert, uns in die weitere Erarbeitung des Konzeptes für die klinische Krebsregistrierung frühzeitig einzubeziehen. Wir werden den geplanten Gesetzgebungsprozess weiterhin begleiten und auf eine sichere Übermittlung und Bereitstellung von Daten über Krebserkrankte hinwirken.

140 Entschließung vom 14. November 2014 mit Anlage: Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern, Dokumentenband 2014, S. 29

5.3 Neufassung der Orientierungshilfe Krankenhausinformationssysteme

Im März verabschiedete die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die zweite Fassung der unter unserer Federführung erarbeiteten Orientierungshilfe (OH) Krankenhausinformationssysteme (KIS).

Darin erläutern die Datenschutzbeauftragten das auf die Datenverarbeitung im Krankenhaus anwendbare Recht und geben praktische Hinweise, wie die Krankenhäuser den gesetzlichen Anforderungen und Erwartungen bei dem Betrieb von KIS entsprechen können.

Die erste Fassung hatte eine lebhafte Diskussion sowohl auf Seiten der Betreiber als auch der Hersteller von KIS hervorgerufen.[141] Die Datenschutzbeauftragten haben die vielfältigen Kommentare mit Interesse aufgenommen. Sie beschlossen, eine neue Fassung der Orientierungshilfe zu erstellen, welche die in der ersten Fassung zusammengefassten Anforderungen in teilweise neuer Formulierung beibehält und sie um die neu gewonnenen Erkenntnisse erweitert. Die zuständige Arbeitsgruppe trat in einen intensiven Austausch mit der Deutschen Krankenhausgesellschaft ein, um zusätzliche Gesichtspunkte bei der Fortschreibung des Textes berücksichtigen zu können.

Die jetzt vorliegende zweite Fassung stellt einige der rechtlichen Anforderungen klar, berücksichtigt stärker die Breite der landesrechtlichen Regelungen zum Datenschutz im Krankenhaus, betont die Freiräume, die sich den Krankenhäusern bei der Ausgestaltung ihrer Krankenhaus-IT bieten, und verdeutlicht die Verknüpfung zwischen rechtlichen und technischen Anforderungen. Darüber hinaus enthält sie neue Hinweise zur Gestaltung der Zusammenarbeit zwischen Krankenhäusern und Medizinischen Versorgungszentren in gleicher Trägerschaft.

141 JB 2011, 7.2.1

Die OH KIS bietet den Krankenhäusern einen Wegweiser für den datenschutzgerechten Umgang mit ihrer Informationstechnik. Zusätzlich unterstützen wir die Krankenhäuser gern mit berlinspezifischen Hinweisen. Zukünftige Prüfungen werden zeigen, welche Reife die Krankenhäuser bei der datenschutzgerechten Gestaltung ihrer Abläufe und Informationstechnik erreicht haben.

5.4 Schweigepflichten in Praxisgemeinschaften

Wir haben die Einhaltung der ärztlichen Schweigepflicht in einer Praxisgemeinschaft geprüft, der ein rechtlich selbständiges Studienzentrum angeschlossen ist.

In Praxisgemeinschaften (PG) schließen sich verschiedene rechtlich selbständige Praxen zusammen, um gemeinsam Ressourcen wie Räume und Computertechnik, aber auch Personal zu nutzen. Die Behandlung der Patienten übernimmt nach wie vor eine einzelne Praxis. Allerdings kann sich ein Patient dafür entscheiden, bei Abwesenheit der Ärztinnen und Ärzte einer Praxis das ärztliche Personal einer anderen Praxis zu konsultieren.

Zwischen dem Personal der beteiligten Praxen ist die Schweigepflicht zu wahren. Nur im Vertretungsfall dürfen die Daten offenbart werden. Gemeinsames Personal kann dabei durchaus für mehrere Praxen tätig werden und Daten einsehen. Es untersteht dabei dem Direktionsrecht der jeweils im Einzelfall behandelnden Ärzte.

Dies muss sich auch technisch im Praxisverwaltungssystem (PVS) widerspiegeln, soweit dies gemeinsam genutzt wird. Ist dies der Fall, müssen im PVS Zugriffsberechtigungen eingerichtet werden, welche die Schranken der Schweigepflicht abbilden. Darüber hinaus muss es möglich sein, die Zugriffe nachzuvollziehen, um Offenbarungen auf ihre Zulässigkeit überprüfen zu können.

In der von uns geprüften PG wurde eine derartige Trennung nicht vollzogen. Passwörter wurden gemeinsam genutzt. Es war stets ein Zugriff auf die Daten aller Patienten möglich. Wir haben die Gesellschafter der PG aufgefordert, für

alle Beschäftigten individuelle Benutzerkonten mit eigenem Passwort und abgestimmten Zugriffsrechten einzurichten.

Ein allgemeiner Zugriff auf alle Patientendaten stand auch dem Personal des Studienzentrums offen. Erschwerend kam hinzu, dass nur ein Teil der Gesellschafter der PG auch Gesellschafter des Studienzentrums waren, so dass den unbeteiligten Ärztinnen und Ärzten gegenüber dem Personal des Studienzentrums keine Weisungsbefugnis zustand. Weiterhin mussten wir feststellen, dass auch Unterlagen der Praxisgemeinschaft im Studienzentrum gelagert wurden, die mit den dort durchgeführten Studien nichts zu tun hatten.

Wir haben Praxisgemeinschaft und Studienzentrum aufgefordert, eine Trennung der Daten und Systeme vorzunehmen. Übermittlungen zwischen Praxisgemeinschaft und Studienzentrum müssen nachvollziehbar sein, insbesondere für die am Studienzentrum unbeteiligten Ärztinnen und Ärzte, soweit deren Patienten betroffen sind. Auf unsere Aufforderung hin wurden die vorgefundenen PG-Unterlagen aus dem Studienzentrum zurück in die PG gebracht.

Die IT-Systeme von Praxisgemeinschaften sind so einzurichten, dass die ärztliche Schweigepflicht gewahrt werden kann. Die Wahl, welchen Ärztinnen und Ärzten Patientendaten offengelegt werden, muss bei den Patienten verbleiben.

5.5 Übergabe von Patientendaten an die Labor GmbH ohne Rechtsgrundlage

Mit Beschluss des Abgeordnetenhauses aus dem Jahr 2010 wurde die Labor Berlin-Charité Vivantes GmbH als Tochtergesellschaft der Charité Universitätsklinikum Berlin und der Vivantes Netzwerk für Gesundheit GmbH gegründet. Seit Beginn der Geschäftsaufnahme zum 1. Januar 2011 werden die Laboruntersuchungen von Patienten der Vivantes Netzwerk für Gesundheit GmbH und der Charité Universitätsmedizin Berlin durch die neue Labor GmbH durchgeführt. Wir haben geprüft, ob bei der Fusion der Laborbereiche von Vivantes und Charité dem Schutz der Patientendaten Rechnung getragen wurde.

Zusammen mit der Technik wurden dem neuen Laborunternehmen auch die Daten der vormals bei den beiden Krankenhäusern behandelten Personen übergeben. Diese Datenübermittlung hinter dem Rücken der Patienten stellt einen Verstoß gegen die ärztliche Schweigepflicht und den Datenschutz dar.

Wir haben die Labor GmbH aufgefordert, die Rückübertragung der unrechtmäßig erhobenen und gespeicherten Daten an die Vivantes Netzwerk für Gesundheit GmbH bzw. die Charité Universitätsmedizin Berlin in schriftlichen Vereinbarungen mit den genannten Stellen zu regeln und zu vollziehen. Die Labor GmbH will dieser Forderung entsprechen. Gleichzeitig haben wir zur Wiederherstellung eines rechtskonformen Zustandes sowohl die Charité Universitätsmedizin Berlin als auch die Vivantes Netzwerk für Gesundheit GmbH zur zügigen Rücknahme der Alt-Daten aufgefordert.

Werden im Gesundheitssektor neue, kostensparende Strukturen geschaffen und dabei Altsysteme übernommen, muss mit den Altdaten gesetzeskonform umgegangen werden. Es ist nicht zulässig, sie einfach als „Anhang" der Technik weiterzugeben.

5.6 Mangelhafte IT-Verfahren in Gesundheitsämtern

Prüfungen bei den Gesundheitsämtern der Bezirke Steglitz-Zehlendorf und Friedrichshain-Kreuzberg führten zu Beanstandungen.

In den Jahren 2012 und 2013 prüften wir die Verfahren der Beratungsstelle für behinderte Menschen, Krebs- und AIDS-Kranke des Gesundheitsamts Steglitz-Zehlendorf und des Kinder- und Jugendgesundheits-Dienstes des Gesundheitsamtes Friedrichshain-Kreuzberg.[142] Im erstgenannten Gesundheitsamt führte die irreguläre Erweiterung eines Verfahrens dazu, dass sensitive Daten ohne ausreichende Vertraulichkeit und Nachprüfbarkeit des Umgangs mit ihnen gespeichert wurden. Im zweiten war ein Verfahren mit ähnlichen Mängeln ganz ohne datenschutzrechtliche Betrachtung eingeführt worden.

142 JB 2012, 9.8; JB 2013, 8.8

Die Beanstandung bei dem Bezirksamt Steglitz-Zehlendorf wurde unumgänglich, da das Bezirksamt die Rückkehr zu einem rechtskonformen Betrieb des Verfahrens verweigerte. Es stellte hierbei eine effiziente Vorgangsbearbeitung und die Vermeidung der hierfür nötigen Investitionen über die Rechte der Klienten und die Sicherheit ihrer Daten. In dieses Bild passt, dass weder für das vorliegende Verfahren noch für das Bezirksamt als Ganzes Sicherheitsmaßnahmen konzeptionell geplant worden waren, obwohl diese Planung von Datenschutzgesetz und Verwaltungsvorschriften vorgegeben wird.[143] Die Stellungnahme auf die Beanstandung steht noch aus.

Die Beanstandung bei dem Bezirksamt Friedrichshain-Kreuzberg führte dagegen zur Einstellung des irregulär eingeführten Verfahrens. Ein Nachfolgeverfahren wurde angekündigt. Es liegen uns jedoch bisher keine aussagekräftigen Unterlagen über dieses avisierte Verfahren vor.

Die öffentliche Verwaltung ist bei der Erfüllung ihrer Aufgaben an die Einhaltung der gesetzlichen Normen gebunden. Wo sie dieser Verpflichtung nicht gerecht wird und der Berliner Beauftragte für Datenschutz und Informationsfreiheit schwerwiegende Verstöße gegen Datenschutzvorschriften feststellen muss, beanstandet er dies und fordert zur Beseitigung der Mängel auf.

5.7 Internetbasierte Nachsorge

Aus der Praxis

Wiederholt haben wir Anbieter beraten, die für ihre Dienstleistungen Gesundheitsdaten über das Internet erheben. Ein Anwendungsfeld ist die Befragung von Patienten, um die langfristige Wirkung einer Behandlung bestimmen zu können.

Wenn Ärztinnen und Ärzte die Qualität ihrer Behandlung einschätzen wollen, stehen sie vor einem Problem, wenn die Patienten sich bei ihnen im weiteren Verlauf nicht wieder vorstellen. Wie können sie erfahren, ob ihre Behandlung erfolgreich war? Hat die Patientin den Arzt gewechselt oder fühlt sie sich

143 Siehe 1.5

geheilt? Welche Lebensqualität hat der Patient nach Abschluss der Behandlung erreicht? Und wie steht es sechs Monate oder zwei Jahre später? Vielfach antworten die Befragten nicht, wenn sie angeschrieben werden. Können Erinnerungs-E-Mails und Fragebogen im Internet helfen?

Die behandelnden Ärztinnen und Ärzte sind dazu verpflichtet, über die Erkenntnisse, die sie bei der Behandlung gewonnen haben, zu schweigen. Sie dürfen diese Erkenntnisse nicht offenbaren, auch nicht dadurch, dass sie ein Medium verwenden, das allgemein verwendet wird, aber nicht gegen Kenntnisnahme Dritter geschützt ist: die E-Mail.

Bereits in der Absenderangabe einer E-Mail kann eine sensitive Information über einen Patienten stecken, z.B. dann, wenn sich der versendende Arzt auf eine bestimmte Erkrankung wie Krebs spezialisiert hat. Womöglich soll die Patientin gar noch an eine bestimmte Therapie erinnert werden und es wird in der E-Mail explizit darauf verwiesen. Aus der Therapieform lässt sich die zu behandelnde Erkrankung ablesen, eine Information, die die Patientin gewiss nicht zur Veröffentlichung in aller Welt vorgesehen hat.

So sind unverschlüsselte E-Mails für die Kommunikation der Leistungserbringer mit ihren Patienten grundsätzlich nicht geeignet. Eine Ausnahme mag allenfalls dann gelten, wenn eine Erinnerungs-E-Mail von einem beauftragten neutralen Dienstleister versandt und so neutral gehalten wird, dass sie nichts über den Empfänger verrät. Dies kann etwa eine Aufforderung sein, ein Merkblatt wieder zur Hand zu nehmen oder eine vereinbarte Webadresse zu besuchen.

Webdienste sind durchaus für die Erfassung auch von Gesundheitsdaten geeignet, allerdings unter drei Voraussetzungen: Zum Ersten sollte der Name der Patienten nicht erfasst werden. Dieser ist den ehemals behandelnden Ärztinnen und Ärzten bereits bekannt. Ein bei der Behandlung vereinbartes Pseudonym genügt. Zum Zweiten sollten die Patientinnen und Patienten eindeutig erkennen können, dass sie auf die richtige Webseite gelangt sind. Dazu gehört ein sog. Zertifikat mit erweiterter Validierung für den Webserver und ggf. ein Bestätigungscode, den nur die echte Webseite in Reaktion auf die Eingabe des gültigen Passworts durch den Patienten herausgeben kann. Zum Dritten gehört dazu neben der Verschlüsselung der Datenübertragung eine Reihe von

technischen Sicherheitsmaßnahmen für den empfangenden Webserver. Hierfür hält das Bundesamt für Sicherheit in der Informationstechnik detaillierte Empfehlungen bereit.

Der elektronischen Kommunikation und Erfassung von Gesundheitsdaten steht das Datenschutzrecht nicht grundsätzlich entgegen. Sie bedürfen jedoch sorgfältiger Schutzmaßnahmen und einer Einschränkung der Daten auf das nötige Minimum.

6 Beschäftigtendatenschutz

6.1 Zugangskontrollen von Beschäftigten

Anonym erhielten wir den Hinweis, dass das Zugangskontrollsystem eines Unternehmens auch zu Verhaltens- und Leistungskontrollen eingesetzt wurde, was in einem Fall sogar zur Kündigung einer Mitarbeiterin führte. Im Rahmen einer Betriebsprüfung wurde auch das Kontrollsystem überprüft. Die Zugangskontrollkarte stellt die Verbindung zwischen Zugangskontrollsystem und Zeiterfassungssystem dar. Nach Angaben des Unternehmens sei es erforderlich, die Zugangskontrollen mit Datum, Uhrzeit und Person zu speichern, um im Fall des Verlustes einer Zutrittskarte überprüfen zu können, ob und wann die Karte seit dem Verlust illegitim genutzt wurde. Trotz häufigen Kartenverlusts wurden die Zugangskontrolldaten jedoch nie für diesen Zweck genutzt.

Das Unternehmen bestätigte den Vorgang zur Kündigung der Beschäftigten und begründeten dies damit, der Vorgesetzte der Beschäftigten habe den Eindruck gewonnen, dass der Inhalt des Gleitzeitbogens und deren tatsächliche Anwesenheitszeit in eklatanter Weise voneinander abwichen. Daraufhin habe er sich die Zugangskontrolldaten der Beschäftigten ausdrucken lassen und mit den Angaben im Gleitzeitbogen verglichen. Im weiteren Verlauf der Angelegenheit stellte sich heraus, dass die Beschäftigte tatsächlich über ihre wahre Anwesenheitszeit getäuscht hatte. Mit der Betroffenen wurde weder vor dieser Maßnahme gesprochen noch wurde sie im Nachhinein darüber informiert. Auch der Betriebsrat und die Datenschutzbeauftragte waren nicht eingebunden.

Die Vorgehensweise des Unternehmens stellte einen Datenschutzverstoß dar. Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigtenverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist.[144] Da die Kontrolldaten im Zugangssystem zur Feststellung des Kartenmissbrauchs durch Dritte bei Verlust der Karte nach Angaben des Unternehmens nie genutzt wurden, war deren Erhebung und Speicherung im

144 § 32 Abs. 1 BDSG

Zugangskontrollsystem für die Feststellung eines Kartenmissbrauchs nicht erforderlich und damit rechtswidrig. Es bestand daher eine Pflicht zur Löschung dieser Daten.[145] Die Nutzung der im Kontrollsystem gespeicherten Personaldaten stellte eine rechtswidrige Zweckänderung dar, da sie nicht zur Feststellung eines Kartenmissbrauchs durch Dritte, sondern zu einer Verhaltens- und Leistungskontrolle der Beschäftigten führte.

Wir leiteten ein Bußgeldverfahren gegen das Unternehmen ein, das sich daraufhin zur Zahlung des Bußgeldes bereit erklärte und für eine datenschutzgerechte Gestaltung des Zugangskontrollsystems sorgte.

Bei der Erhebung, Verarbeitung und Nutzung von Personaldaten der Beschäftigten ist stets das Gebot der Erforderlichkeit, Zweckbestimmung und Verhältnismäßigkeit zu beachten.

6.2 Vorzeitige Erhebung von Bewerberdaten

Aus der Praxis

Eine Petentin übermittelte uns einen zwölfseitigen Bewerberfragebogen einer Klinik mit insgesamt 116 Fragen zu Gesundheit, Behinderungen, Hobbys und familiären Verhältnissen. Der Fragebogen musste noch vor dem ersten Vorstellungsgespräch ausgefüllt werden.

Die Erhebung und Verarbeitung der Daten ist zulässig, wenn dies zur Begründung des Beschäftigungsverhältnisses erforderlich ist.[146] Es dürfen nur solche Fragen gestellt werden, an deren wahrheitsgemäßer Beantwortung der Arbeitgeber ein berechtigtes und schutzwürdiges Interesse hat, aufgrund dessen die Belange der Bewerberinnen und Bewerber zurücktreten müssen. Dabei kommt es auch darauf an, in welchem Bewerbungsstadium sich die Bewerberin oder der Bewerber befindet.

145 § 35 Abs. 2 Nr. 1 BDSG
146 § 32 Abs. 1 BDSG

Im Bewerbungsverfahren selbst sind deshalb zunächst nur die Fragen zulässig, die für die Entscheidung notwendig sind, ob die Betroffenen überhaupt geeignet sind, um in die nähere Auswahl zu gelangen.

An der Beantwortung von Fragen persönlicher Art, die mit der ausgeübten Tätigkeit nichts zu tun haben, wie etwa Hobbys, eine Mitgliedschaft im Verein oder familiäre Verhältnisse, hat der Arbeitgeber zu keinem Zeitpunkt ein berechtigtes Interesse. Solche Fragen sind mithin unzulässig.

Insbesondere unterliegen Daten über die Gesundheit, Erkrankungen bzw. etwaige Behinderungen einem besonderen Schutz.[147] Der Arbeitgeber hat bezüglich dieser Daten nur dann einen Informationsanspruch, wenn sie Voraussetzung für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche sind.[148] Nach dem Allgemeinen Gleichbehandlungsgesetz sind Nachfragen zu gesundheitlichen Einschränkungen erlaubt, wenn diese konkrete Auswirkungen auf die Tätigkeit haben bzw. diese unmöglich machen.[149] Keinesfalls darf der Arbeitgeber Krankheitsdaten losgelöst von der zu besetzenden Stelle erheben.

Dies teilten wir dem Unternehmen mit, das unserer Auffassung folgte. Der Personalfragebogen wird in dieser Form nicht mehr verwendet. Die Bewerberfragebögen wurden neu strukturiert und enthielten insgesamt weniger Fragen.

Im Bewerbungsverfahren dürfen nur solche Fragen gestellt werden, an deren wahrheitsgemäßer Beantwortung der Arbeitgeber ein berechtigtes und schutzwürdiges Interesse hat.

147 § 3 Abs. 9 und § 28 Abs. 6 BDSG
148 § 28 Abs. 6 Nr. 3 BDSG
149 § 8 Abs. 1 AGG

6.3 E-Recruiting – das Jobportal der Berliner Verwaltung

Das Stellenportal Interamt.de wird in den meisten Einstellungsbehörden durch ein neues Jobportal abgelöst, das den besonderen Anforderungen der Personalsuche des Öffentlichen Dienstes für das Land Berlin entspricht.

Durch vollständig IT-gestützte und medienbruchfreie Geschäftsprozesse soll der Arbeitsaufwand sowohl auf Seiten der Bewerberinnen und Bewerber als auch für die Beschäftigten der Einstellungsbehörden stark reduziert werden. So bietet das IT-gestützte Bewerbungs- und Einstellungssystem den Bewerberinnen und Bewerbern nicht nur die Recherche nach einer Wunschstelle innerhalb der Berliner Verwaltung an, sondern auch die Möglichkeit, eine Bewerbung online abzugeben. Mit geringem Arbeitsaufwand können die Bewerbungsunterlagen übermittelt werden. Ein wesentlicher Bestandteil des neuen Verfahrens ist die IT-gestützte Eignungsdiagnostik. Hierdurch wird ermöglicht, dass Bewerberinnen und Bewerber Eignungstestverfahren online durchführen können. Die Einführung hat am 5. November begonnen. In dieser ersten Welle sollen in den meisten Bezirksämtern sowie einigen Senatsverwaltungen schwerpunktmäßig Nachwuchskräfte gewonnen werden.

Durch eine Präsentation des Projekts in einer Sitzung des IT-Koordinierungsgremiums wurden wir im Mai auf das Verfahren aufmerksam. Im Folgenden wurde das ambitionierte Projekt effizient durch die behördlichen Datenschutzbeauftragten der Einstellungsbehörden und uns begleitet. Die anfangs sehr eingeschränkten Unterlagen wurden zügig unseren Anforderungen angepasst, sodass das Projekt planmäßig gestartet werden konnte. Besonderes Augenmerk wurde vor allem auf die einzurichtenden Maßnahmen zum Schutz der personenbezogenen Daten als auch die fein granulierten Zugriffsrechte gelegt. Nacharbeiten sind jedoch noch notwendig – insbesondere bei der Ausarbeitung von weiteren Konzepten. Das Verfahren wird weiterhin aktiv begleitet und auf die Einhaltung der Maßnahmen zum Datenschutz kontrolliert.

Dank der engagierten Zusammenarbeit zwischen den Datenschutzbeauftragten und der Projektgruppe konnte das IT-Verfahren innerhalb kürzester Zeit ein angemessenes Datenschutzniveau erreichen. Zukünftig sollte jedoch eine frühzeitige Unterrichtung sowie die Übermittlung vollständiger prüffähiger Unterlagen erfolgen.

6.4 E-Mail-Accounts bei Toll Collect

Die Gesellschafter der Toll Collect GmbH, die Daimler AG und die Deutsche Telekom AG, planten einen umfangreichen Transfer von Geschäftspapieren der Toll Collect GmbH in ihren Herrschaftsbereich. Hiervon betroffen waren auch die E-Mail-Postfächer von 85 Beschäftigten der Toll Collect GmbH. Diese ist ein Unternehmen, das vom Bundesverkehrsministerium beauftragt wurde, das System zur Einnahme der LKW-Maut auf deutschen Autobahnen aufzubauen, zu betreiben und die Gebühren abzurechnen. Benötigt wurden die E-Mails im Rahmen einer Schadensersatzforderung des Bundes gegenüber den Gesellschaftern.

Problematisch war der Transfer der E-Mail-Accounts auch deshalb, weil den Beschäftigten die private Nutzung gestattet war. Damit ist es grundsätzlich verboten, in die E-Mail-Accounts Einsicht zu nehmen. Der Arbeitgeber hat das Fernmeldegeheimnis zu beachten.[150]

Der Transfer der Geschäftspapiere sollte in drei Stufen erfolgen. Zunächst sollten die betroffenen Mitarbeiterinnen und Mitarbeiter informiert und ihnen eine 14-Tage-Frist zur Sichtung der E-Mails nach privaten oder sensitiven Inhalten gegeben werden. Die so bereinigten Accounts sollten dann in einem zweiten Schritt an die Treuhänderin übermittelt werden. Dort sollten sie zu Beweiszwecken gesichert und zwischengespeichert werden. Letztlich sollte der Datenbestand mittels Screenings nach Schlagworten durchsucht werden. Die im Filter verbliebenen personalisierten Dokumente sollten dann den Gesellschaftern übergeben werden.

150 § 88 Telekommunikationsgesetz

In einem Beratungsgespräch mit den Gesellschaftern legten wir dar, dass die Übermittlung der Personaldaten an eine Treuhänderin nur zulässig ist, wenn dies erforderlich ist und es keine Anhaltspunkte gibt, dass schutzwürdige Interessen der betroffenen Beschäftigten überwiegen.[151] Schon die Erforderlichkeit war nicht gegeben, sodass eine Übermittlung an die Treuhänderin rechtswidrig gewesen wäre. Vielmehr sollte die Toll Collect GmbH mit der Treuhänderin einen Auftragsdatenverarbeitungsvertrag abschließen.[152] So ist sichergestellt, dass die Toll Collect GmbH selbst „Herrin der Daten" bleibt und die Entscheidungen über den Umgang mit den personenbezogenen Daten bei ihr verbleiben.

Die Übermittlung von Beschäftigtendaten ist nicht erforderlich, wenn eine weisungsgebundene Datennutzung durch einen Auftragsdatenverarbeiter möglich ist.

6.5 Telefonlisten im Internet

Aus der Praxis

Für Arbeitslose ist es häufig schwierig, die zuständige Sachbearbeiterin bzw. den zuständigen Sachbearbeiter im Jobcenter direkt anzurufen, viele Jobcenter verweisen nur auf eine Zentralnummer. Um dieses Problem zu lösen, hat die Piratenpartei auf Bundesebene interne Telefonlisten von fast 130 Jobcentern ins Internet eingestellt. Veröffentlicht wurden Name, Organisationseinheit, Zimmernummer, Telefon und Zuständigkeit (insbesondere Aufteilung nach Buchstaben), bei Teilzeitkräften wurden noch die Stundenanzahl und die Arbeitswochentage angegeben. Zum Schutz der Beschäftigten stellte die Partei sicher, dass die Jobcenter-Listen nicht durch Suchmaschinen indexiert werden. Die internen Telefonlisten stammten nur zu einem kleinen Teil von Anträgen auf Informationsfreiheit, die Mehrzahl der Listen hatte die Partei von „Aktivistinnen" und „Aktivisten" erhalten. Wie diese an die Daten gelangt sind, war der Partei nicht bekannt. Sie ging davon aus, dass die Veröffentlichung der Beschäftigtendaten aufgrund des Informationsfreiheitsgesetzes rechtlich nicht zu beanstanden sei. Gegen die Veröffentlichung der Listen sind bei uns mehrere Beschwerden eingegangen.

151 § 32 Abs. 1 Satz 1 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG
152 § 11 BDSG

Das für die Jobcenter geltende Informationsfreiheitsgesetz des Bundes (IFG)[153] sieht keine Verwendungsbeschränkungen, Einwilligungs- oder Zustimmungserfordernisse im Hinblick auf die Verwendung amtlicher Informationen vor. Die Piratenpartei darf daher die Telefonlisten von Jobcentern, die sie durch Anträge nach dem IFG erhalten hat, auch im Internet veröffentlichen.

Soweit die Telefonlisten jedoch nicht aus derartigen Informationszugängen bei den Jobcentern, sondern von „Aktivistinnen" und „Aktivisten" stammen, kann die Veröffentlichung dagegen nicht mit dem IFG gerechtfertigt werden. Denn das Recht auf freie Verwendung der Information setzt zwingend den rechtmäßigen Informationszugang bei dem Jobcenter voraus. Die Rechtmäßigkeit der Datenverarbeitung unabhängig vom IFG ist schon deshalb zweifelhaft, weil die Piratenpartei keine Kenntnis darüber hat, wie die „Aktivistinnen" und „Aktivisten" rechtmäßig unter Beachtung der Erhebungsvorschriften[154] in den Besitz der Jobcenter-Daten gelangt sind. Bei nachweisbar rechtmäßiger Datenerlangung durch die Piratenpartei kann die Veröffentlichung rechtmäßig sein.[155] Bei der Abwägung der berechtigten Interessen der Piratenpartei an einer Veröffentlichung der Daten mit den schutzwürdigen Interessen der Betroffenen ist die Rechtsprechung des Bundesverwaltungsgerichts[156] zu berücksichtigen, die die Veröffentlichung von bestimmten Beschäftigtendaten (Name, Dienstbezeichnung, dienstliche Telefonnummer, dienstliche E-Mail-Adresse) als rechtmäßig ansieht. Allerdings ist hier zu beachten, dass die Rechtsprechung auf die Veröffentlichung durch Dritte nicht vollständig übertragen werden kann. Denn nur die Dienststelle kann sicherstellen, dass die Daten immer aktuell und – falls nötig – diejenigen von gefährdeten Jobcenter-Beschäftigten von der Veröffentlichung ausgenommen bleiben.

Die Piratenpartei hat die personenbezogenen Daten zu den genauen Arbeitszeiten inzwischen gelöscht. Sie hat zugesagt, zukünftig nur Daten zu veröffentlichen, die sie nach dem IFG rechtmäßig erlangt hat. Wir haben empfohlen, die Datenbestände alle halbe Jahre zu aktualisieren.

153 § 50 Abs. 4 Satz 2 SGB II
154 § 4 Abs. 2, 3 BDSG
155 § 28 Abs. 1 Satz 1 Nr. 2 BDSG
156 Beschluss vom 12. März 2008 - 2 B 131.07

Nur wer personenbezogene Daten rechtmäßig erlangt, kann ein berechtigtes Interesse an ihrer Veröffentlichung haben.

6.6 Datenschutz bei einer Gewerkschaft

Beim Datenschutz innerhalb einer Gewerkschaft[157] ist zu beachten, dass es sich bei den verarbeiteten Daten fast ausschließlich um besondere Arten personenbezogener Daten handelt,[158] da sie direkt oder indirekt auf eine Gewerkschaftszugehörigkeit schließen lassen. Aufgrund einer Reihe besonderer Vorschriften für solche sog. sensitiven Daten unterliegen diese einem besonders hohen Schutzniveau. An Organisationen, die vorwiegend sensitive Daten verarbeiten, sind erhöhte Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen zu stellen. Vor diesem Hintergrund überprüften wir Ende 2013 die Sicherstellung des Datenschutzes bei der Vereinten Dienstleistungsgewerkschaft ver.di. Dabei wurden organisatorische und strukturelle Mängel festgestellt, von denen bisher nicht alle behoben wurden.

Die personelle Ausstattung der Datenschutzorganisation ist unzureichend. So ist neben dem betrieblichen Datenschutzbeauftragten nur eine weitere Sachbearbeiterstelle für den Bereich Datenschutz vorgesehen. Es ist für zwei Beschäftigte der Zentrale in Berlin jedoch nicht möglich, den Umgang mit den Daten von über zwei Millionen Mitgliedern und mehreren tausend Beschäftigten in einer Vielzahl von Geschäftsstellen bundesweit zu überblicken und Missstände schnell zu beheben. Wir haben gegenüber dem Bundesvorstand daher die Empfehlung ausgesprochen, den Bereich Datenschutz personell aufzustocken und insbesondere auf eine Dezentralisierung hinzuwirken. So sollte in allen Landesbezirken wenigstens eine Person als datenschutzrechtlicher Ansprechpartner bestellt werden. Diese regionalen Ansprechpartner sollen den betrieblichen Datenschutzbeauftragten in der Zentrale unterstützen, indem sie ihn über aktuelle datenschutzrelevante Vorhaben oder Problemstellungen frühzeitig

157 Siehe zuletzt JB 2013, 9.4
158 § 3 Abs. 9 BDSG

unterrichten und bei Fragen vor Ort beratend und informierend zur Seite stehen.

In Bezug auf die Mitgliederdatenverarbeitung bemängelten wir einen bundesweiten Lesezugriff auf die Mitgliederdatenbank für alle Beschäftigten, die mit der Mitgliederbetreuung betraut sind. Ziel dieser weiten Zugriffsrechte ist es, Mitgliedern unabhängig von deren originär zuständigen Geschäftsstellen deutschlandweit einen allumfassenden Service bieten zu können. Der legitime Servicegedanke befreit jedoch nicht von der Pflicht, durch geeignete Maßnahmen die Einhaltung des Datenschutzes sicherzustellen.[159] Eine angemessene Maßnahme, um missbräuchlichen Datenbankabrufen vorzubeugen, ist die Protokollierung aller getätigten Leseaufrufe und regelmäßige Stichprobenkontrollen durch den betrieblichen Datenschutzbeauftragten. Wie auch in anderen Bereichen, z.B. dem Bankensektor, haben wir eine solche Lösung von den Verantwortlichen gefordert.

Aus technisch-organisatorischer Sicht ist die Beratung von Mitgliedern bei der Erstellung der Lohnsteuererklärung durch ehrenamtliche Beschäftigte nicht unproblematisch. Zwar werden dafür gewerkschaftseigene Rechner zur Verfügung gestellt, jedoch kann der Einsatz von privaten Rechnern nicht ausgeschlossen werden. Dieses wirft Fragen z.B. zum Schutz der privaten Geräte und zur datenschutzgerechten Löschung von Daten nach Erfüllung der Aufgabe auf, die bisher nicht vollständig beantwortet werden konnten. Die Gewerkschaft hat zugesichert, die Risiken einer möglichen Nutzung privater Endgeräte zu dienstlichen Zwecken (Bring your own device – BYOD)[160] zu analysieren und einer Bewertung zu unterziehen. Kommen als gewerkschaftseigene Rechner mobile Geräte zum Einsatz, haben wir empfohlen, deren Speicher zu verschlüsseln, da ein Verlust dieser Geräte beim Transport nicht ausgeschlossen werden kann. Allein die Eingabe eines Passwortes für den Zugriff auf mobile Geräte sowie die Anwendungssoftware bietet keinen ausreichenden Schutz für die Vertraulichkeit der gespeicherten Daten.

Die Kommunikation per E-Mail mit und innerhalb der Gewerkschaft erfolgt bisher unverschlüsselt. Unsere Empfehlung, eine Ende-zu-Ende-

159 § 9 BDSG
160 JB 2012, 2.3

Verschlüsselung einzuführen, wurde im aktuellen Sicherheitskonzept aufgegriffen. Bereits jetzt besteht die Möglichkeit, bei der Kommunikation mit Mitgliedern oder Externen vertrauliche Dokumente in einem verschlüsselten Bereich zu hinterlegen. Nach Abholung oder Ablauf einer definierten Zeitspanne werden die dort hinterlegten Dokumente automatisch gelöscht.

Bei einer Gewerkschaft sind insbesondere aufgrund der Art der Daten, die verarbeitet werden, ausreichende personelle, technische, strukturelle und organisatorische Maßnahmen zu treffen, um das Risiko des rechtswidrigen Umgangs mit personenbezogenen Daten zu minimieren.

7 Stadtentwicklung und Tourismus

7.1 Exzessive Datenerhebung bei Mietinteressenten – keine Wohnung ohne „Datenstriptease“?

Erneut haben uns Eingaben von Mietinteressenten erreicht, die berichteten, dass Vermieter außergewöhnlich viele Daten von Wohnungssuchenden erheben. Wir sind diesen Hinweisen nachgegangen und mussten feststellen, dass diese Vorwürfe in vielen Fällen berechtigt waren.

Vermieter dürfen nur diejenigen Daten erheben, die für die Auswahl eines geeigneten Mieters erforderlich sind.[161] Dazu gehören auch Daten zur wirtschaftlichen Leistungsfähigkeit des potentiellen Mieters, da Vermieter ein berechtigtes Interesse an zahlungsfähigen Vertragspartnern haben. Nicht erlaubt ist dagegen das Sammeln von Daten, die für das Mietverhältnis nicht relevant sind. Hierunter fallen Informationen zu Heiratsabsichten, Schwangerschaften, Kinderwünschen, Partei-, Mietervereins- oder Gewerkschaftszugehörigkeit, persönlichen Vorlieben, Hobbys, Krankheiten oder Behinderungen.

Ebenso wichtig ist der Zeitpunkt der Datenerhebung. Grundsätzlich gilt, dass Daten zur wirtschaftlichen Situation erst dann erhoben werden dürfen, wenn sich die Interessenten nach der Wohnungsbesichtigung tatsächlich um eine bestimmte Wohnung bewerben. Rechtswidrig ist es hingegen, bereits vor dem Besichtigungstermin umfangreiche Daten zur wirtschaftlichen Situation aller Mietinteressenten auf Vorrat zu erheben, wenn noch unklar ist, ob sich die Person überhaupt um die Wohnung bewerben möchte. Vor dem Besichtigungstermin dürfen Angaben zur Identifikation, zur Erreichbarkeit, zu Wohnungswünschen, zu Haustieren und ggf. Daten aus dem Wohnberechtigungsschein erhoben werden. In einem Fall wollte ein Wohnungsunternehmen nur dann Termine für eine Wohnungsbesichtigung vergeben, wenn die Bewerber vorher eine entsprechende SCHUFA-Auskunft vorlegen konnten. Nachdem wir ein Anordnungsverfahren[162] eingeleitet haben, hat das Unternehmen seine Praxis entsprechend angepasst.

161 § 28 Abs. 1 Satz 1 Nr. 1 BDSG
162 Gemäß § 38 Abs. 5 Satz 1 BDSG

In weiteren Fällen, die uns bekannt wurden, haben wir die jeweiligen Vermieter auf diese Rechtslage hingewiesen. Dies hat in den meisten Fällen ausgereicht, dass diese ihre Datenerhebung eingeschränkt haben. Es ist aber zu vermuten, dass die Dunkelziffer derjenigen, die zu viele Daten erheben, beträchtlich höher ist. Viele Wohnungssuchende geben aus Angst, sonst keine Wohnung zu bekommen, ihre Daten von sich aus preis und beschweren sich nicht bei uns. Es besteht aber auch die Möglichkeit, unzulässige Fragen des Vermieters falsch zu beantworten, ohne dass dies einen Kündigungsgrund darstellt.

Der Düsseldorfer Kreis hat eine Orientierungshilfe erarbeitet, die die gesetzlichen Vorgaben konkretisiert.[163] Diese Orientierungshilfe soll es Vermietern erleichtern, die gesetzlichen Verpflichtungen einzuhalten. Zusätzlich haben wir gemeinsam mit dem Berliner Mieterverein e. V. eine Broschüre zum Datenschutz und zum Schutz der Privatsphäre im Mietverhältnis erstellt.[164] Diese Broschüre richtet sich an Mieterinnen und Mieter und soll über Datenschutzrechte im Mietverhältnis aufklären.

Vermieter dürfen von Wohnungssuchenden nur solche Daten erheben, die entweder zur Begründung oder Durchführung des Mietverhältnisses erforderlich sind oder an deren Erhebung sie ein berechtigtes Interesse haben. Unzulässige Fragen dürfen falsch beantwortet werden.

7.2 Zweckentfremdungsverbot-Gesetz – Datenerhebung im Internet?

Ende 2013 ist das sog. Zweckentfremdungsverbot-Gesetz in Kraft getreten. Eine Zweckentfremdung im Sinne dieses Gesetzes liegt z.B. vor, wenn Wohnraum wiederholt als Ferienwohnung vermietet wird. Damit soll erreicht werden, dass in den zentraleren Bezirken genügend bezahlbarer Wohnraum für die hier dauerhaft lebenden Menschen verbleibt. Bei der

163 Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“, siehe Dokumentenband 2014, S. 39

164 Ratgeber zum Datenschutz Nr. 10: „Meine Privatsphäre als Mieter“

Umsetzung des Gesetzes stellte sich die Frage, welche Datenerhebungsbefugnisse den Bezirken bei der Ermittlung zweckfremd genutzter Wohnungen zur Verfügung stehen. Insbesondere war fraglich, ob bei der Fahndung nach Ferienwohnungen im Internet personenbezogene Daten erhoben werden dürfen.

Das Gesetz räumt dazu den Bezirken weitreichende Befugnisse ein. § 5 berechtigt die zuständigen Behörden z.B. zum Betreten von Wohnungen und zur Erhebung personenbezogener Daten. Dabei müssen personenbezogene Daten aber grundsätzlich zuerst bei dem Betroffenen selbst erfragt werden. Nur falls dies nicht möglich ist, dürfen Daten von Dritten erhoben werden (Grundsatz der Direkterhebung). Eine Rechtsgrundlage für die Internet-Recherche ist in diesem Gesetz nicht verankert. Dies ist auch nicht erforderlich, da die rechtswidrige Nutzung einer Wohnung eine Ordnungswidrigkeit darstellt. Damit kann auf die Ermittlungsbefugnisse des Ordnungswidrigkeitenrechts zurückgegriffen werden, die eine Erhebung personenbezogener Daten im Internet zulassen.[165]

Voraussetzung dafür ist allerdings, dass ein Anfangsverdacht einer Ordnungswidrigkeit besteht. Diese Schwelle ist von Rechts wegen sehr niedrig angesetzt. Ein Anfangsverdacht liegt schon dann vor, wenn zureichende tatsächliche Anhaltspunkte für eine Ordnungswidrigkeit vorliegen. Er ist z.B. gegeben, wenn bei der Behörde Hinweise von Bürgerinnen und Bürgern eingehen oder im Internet in einem bestimmten Kiez wesentlich mehr Ferienwohnungen angeboten werden als genehmigt wurden. Eine Speicherung personenbezogener Daten aller angebotenen Ferienwohnungen auf Vorrat – unabhängig davon, ob der Verdacht einer Ordnungswidrigkeit besteht – ist dagegen unzulässig. Grund dafür ist, dass nicht alle im Internet angebotenen Wohnungen unter das Verbot fallen. So ist z.B. ein Wohnungstausch oder eine einmalige (Unter-) Vermietung unter bestimmten Voraussetzungen zulässig.[166]

165 § 46 Abs. 1 OWiG i. V. m. § 161 StPO

166 Siehe § 2 Abs. 1 Nr. 1 Zweckentfremdungsverbot-Gesetz mit Gesetzesbegründung

Zusammen mit der Senatsverwaltung für Stadtentwicklung und Umwelt haben wir die Bezirke in einem Rundschreiben darüber informiert, unter welchen Voraussetzungen personenbezogene Daten im Internet erhoben werden dürfen.

7.3 Fotografien von Privathäusern durch das Bezirksamt

Wir haben Hinweise erhalten, dass ein Mitarbeiter des Bezirksamts Mitte in einem bestimmten Kiez Fotografien von Häuserfassaden anfertigte. Die Bewohnerinnen und Bewohner wurden vorher weder um Erlaubnis gefragt noch über diese Maßnahme informiert. Sie erfuhren erst davon, als sie den Fotografen zufällig bei seiner Tätigkeit beobachtet und befragt hatten.

Auf unsere Nachfrage teilte uns das Bezirksamt mit, dass die Fotografien zu dienstlichen Zwecken des Stadtentwicklungsamtes angefertigt worden seien. Dazu wurde als Zweck allgemein die Bestandsaufnahme für die Ergänzung städtebaulicher Konzepte und Bebauungspläne im Bezirk angegeben. Nachdem wir einen Prüfbesuch angekündigt hatten, wurde uns mitgeteilt, dass die fraglichen Fotografien gelöscht worden seien.

Die Datenerhebung durch das Bezirksamt wurde beanstandet. Zwar darf das Stadtentwicklungsamt personenbezogene Daten erheben, wenn es dafür eine rechtliche Grundlage gibt. Solche Rechtsgrundlagen sind zum Beispiel im Stadtplanungsdatenverarbeitungsgesetz enthalten. Darin sind alle Daten genau beschrieben, die das Stadtentwicklungsamt für die Erfüllung seiner Aufgaben verarbeiten darf. Fotografien von Privathäusern werden dort nicht genannt und offenbaren weit mehr über die persönliche Lebensgestaltung der Bewohnerinnen und Bewohner als die dort angegebenen Maße und sonstigen Angaben. Außerdem sieht dieses Gesetz vor, dass die oder der Betroffene über die Datenerhebung zu informieren ist.[167]

Auch die Voraussetzungen anderer Rechtsgrundlagen waren hier nicht gegeben. Zwar sieht das Berliner Datenschutzgesetz vor, dass bestimmte offenkundige

167 § 6 Stadtplanungsdatenverarbeitungsgesetz

Daten verarbeitet werden dürfen, wenn schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.[168] Allerdings dürfen auch solche Daten grundsätzlich nur mit Kenntnis der Betroffenen erhoben werden, wobei darauf hinzuweisen ist, dass die Auskunft verweigert werden kann.[169] Außerdem muss die Datenerhebung für die rechtmäßige Erfüllung der behördlichen Aufgaben erforderlich sein.[170] Dass die Fotografien für die Erfüllung der Aufgaben des Stadtentwicklungsamts überhaupt nicht erforderlich waren, wurde auch daran deutlich, dass die Fotografien nach Ankündigung unseres Prüfbesuchs sofort gelöscht wurden.

Auf die Beanstandung hin hat das Bezirksamt erklärt, trotzdem an seiner Auffassung festzuhalten. Es sei rechtlich zulässig, dass das Stadtplanungsamt Fotos von Privathäusern erstellen könne, auch ohne die Bewohnerinnen und Bewohner zu informieren.

Die Anfertigung von Fotos von Privathäusern durch das Bezirksamt, ohne dass dies für die Aufgabenerfüllung erforderlich ist, ist unzulässig. Die Betroffenen sind wie gesetzlich vorgesehen in jedem Fall zu informieren.

7.4 Schutz der Intimsphäre auf der Hotel-Toilette

Aus einem Zeitungsbericht erfuhren wir, dass sich in einem neu eröffneten Berliner Hotel durch die bodentiefen Panorama-Fenster im 10. Stock nicht nur eine schöne Aussicht auf den anliegenden Zoologischen Garten und vor allem das Affenhaus bietet; auch die Zoobesucherinnen und -besucher hatten dem Bericht zufolge einen freien Blick in die im 10. Stock des Hotels liegende Bar, das Restaurant und die dort vorhandenen Sanitäreinrichtungen.

168 § 6 Abs. 1 Satz 2 BlnDSG
169 § 10 Abs. 1 und 2 BlnDSG
170 § 9 Abs. 1 BlnDSG

Daraufhin haben wir eine Vor-Ort-Kontrolle des Hotels durchgeführt. Wir konnten feststellen, dass seitens des Hotels Maßnahmen getroffen worden waren, um die Intimsphäre der Hotelbesucher im Sanitärbereich zu schützen. Auf den bis zum Boden durchgehend verglasten Fenstern wurden etwa einen Meter hohe Klebefolien angebracht, die einen Milchglaseffekt mit sich brachten. Dadurch wurde sichergestellt, dass auch vom Gelände des Zoologischen Gartens aus aufgrund des steilen Sichtwinkels im Bereich der aufgeklebten Sichtschutzfolie lediglich der Kopf einer Person zu erkennen ist, die die Toilette nutzt. Die Räumlichkeiten an sich sind von Zoobesuchern nicht als Toiletten zu erkennen.

Auch bei der Architektur und Raumgestaltung ist das Prinzip von „Privacy by Design" zu beachten.

7.5 Unsachgemäße Entsorgung von Visa-Anträgen

Aus der Praxis

Wir sind darüber unterrichtet worden, dass in einem Reisezentrum, das im Auftrag ausländischer Konsulate Reisevisa für Nicht-EU-Staaten ausstellt, Unterlagen der Antragsteller unsachgemäß behandelt werden. So wurden in einem öffentlich zugänglichen Müllcontainer des Reisezentrums zahlreiche Unterlagen aufgefunden, die nur zum Teil grob per Hand zerrissen waren und personenbezogene Daten wie z.B. Bilder, Namen, Krankenversicherungen und Reiserouten von Personen erkennen ließen, die Visa beantragt hatten.

Das Bundesdatenschutzgesetz[171] verpflichtet verantwortliche Stellen, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die datenschutzgerechte und sichere Erhebung, Verarbeitung und Nutzung zu erreichen. Nicht mehr benötigte Dokumente bzw. Unterlagen mit personenbezogenem Inhalt sind derart zu vernichten, dass deren Wiederherstellung nach dem gegenwärtigen Stand der Technik als ausgeschlossen angesehen werden kann.

171 § 9 BDSG

Wir forderten das Reisezentrum auf, umfassend zu prüfen, ob an allen seinen Standorten ausreichende Vorkehrungen getroffen sind, um eine den gesetzlichen Anforderungen entsprechende Vernichtung schriftlicher personenbezogener Unterlagen zu gewährleisten. Als technische Maßnahme wurde insbesondere sichergestellt, dass allen mit der Erhebung, Verarbeitung und Nutzung der Daten betrauten Beschäftigten Schredder zur Verfügung stehen, welche Dokumente entsprechend den Anforderungen der DIN 66399 vernichten. In organisatorischer Hinsicht teilte uns das Reisezentrum mit, dass eine interne schriftliche Arbeitsanweisung bestehe, welche sämtliche Mitarbeiter ausdrücklich verpflichte, schriftliche Unterlagen ausschließlich mittels Schreddern zu vernichten. Dies gelte ausdrücklich für nicht mehr benötigte Dokumente, Fehldrucke/Fehlkopien, Notizen und Gesprächsprotokolle. Die Geschäftsführung sicherte uns zu, dass diese Arbeitsanweisung in regelmäßigen Abständen und in geeigneter Weise, z.B. durch Rund-E-Mails oder persönliche Ansprachen, gegenüber den Beschäftigten kommuniziert wird. Der Vorfall wurde zum Anlass genommen, alle Beschäftigten nochmals und nachdrücklich auf die strikte Einhaltung der gesetzlichen Bestimmungen sowie der hierzu ergangenen unternehmensinternen Anweisungen hinzuweisen und stichprobenartige Kontrollen in regelmäßigen Abständen einzuführen, die zukünftig Vorfälle solcher Art unterbinden sollten.

Privatunternehmen sind verpflichtet, nicht mehr benötigte schriftliche Unterlagen mit personenbezogenem Inhalt so zu vernichten, dass deren Wiederherstellung durch unbefugte Dritte nach dem gegenwärtigen Stand der Technik als ausgeschlossen gelten kann. Die Vernichtung hat mit DIN-konformen Schreddern zu erfolgen.

8 Forschung, Bildung und Kultur

8.1 Forschung

8.1.1 Aufklärung von Arzneimitteltests in der DDR – nicht ohne Datenschutz

Aus der Praxis

Die Aufklärung von Arzneimitteltests internationaler Pharmaunternehmen in der DDR stößt auf großes öffentliches Interesse. Ein Forschungsprojekt des Instituts für Geschichte der Medizin der Charité hat sich bis Dezember 2015 die Aufarbeitung klinischer Arzneimittelforschung zwischen 1961 und 1989 zum Ziel gesetzt. Es werden u. a. Patientenakten analysiert.

Das Forschungsinstitut der Charité darf für das krankenhausinterne Forschungsvorhaben Patientendaten der Charité auch ohne Einwilligung der Betroffenen verarbeiten.[172] Zwar besteht grundsätzlich ein Geheimhaltungsinteresse der Patientinnen und Patienten an ihren Behandlungsdaten. An der Aufarbeitung der Arzneimittelversuche besteht allerdings ein erheblich überwiegendes berechtigtes Interesse der Allgemeinheit.

Betroffene müssen jedoch von der Datenverarbeitung Kenntnis erhalten können. Eine Recherche der aktuellen Adressdaten aller von der Aktenanalyse betroffenen Patientinnen und Patienten ist aufgrund des Zeitablaufs und der großen Anzahl der infrage kommenden Akten unzumutbar. Das Projekt muss stattdessen von einer angemessenen Öffentlichkeitsarbeit begleitet werden. Es muss die Möglichkeit bestehen, Widerspruch gegen die Verwendung der eigenen Patientendaten einzulegen. Konkrete Ansprechpartner und Verfahren zur Umsetzung von Widersprüchen müssen feststehen.

Für die Forschungsarbeit haben wir ein zweistufiges Verfahren vorgeschlagen. Bestimmte Beschäftigte des Instituts für Medizingeschichte sollen zunächst die nach dem Forschungskonzept infrage kommenden Patientenakten allgemein

172 § 25 Abs. 1 Nr. 3 Landeskrankenhausgesetz (LKG)

auf ihre Eignung hin überprüfen. Liegt eine Eignung vor, weil etwa bestimmte Schlagworte vorkommen, soll die Akte anonymisiert werden. Dann soll sie für die vertiefte, einzelfallbezogene Forschung an einen anderen Beschäftigten des Instituts übergeben werden.

Krankenhausinterne Forschung kann ohne Einwilligung von Patientinnen und Patienten zulässig sein. Die schutzwürdigen Interessen der Betroffenen sind durch geeignete Maßnahmen zu wahren.

8.1.2 Hausbesuche des Jugendamts in Familien

An der Freien Universität Berlin wird aktuell ein vom zuständigen Bundesministerium gefördertes Forschungsprojekt zur Bedeutung von Hausbesuchen im Kontext des Schutzauftrags bei Kindeswohlgefährdung („HabeK“) durchgeführt. Es sollen auch Akten bei Jugendämtern analysiert werden.

Sozialdaten, die einer Mitarbeiterin oder einem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, unterliegen einem besonderen Schutz.[173] Ohne Einwilligung der Betroffenen dürfen sie Dritten grundsätzlich nicht zugänglich gemacht werden. Vor einer Analyse von Akten der Jugendämter durch Forschende muss daher grundsätzlich eine Anonymisierung durchgeführt werden, sodass Rückschlüsse auf den konkreten Einzelfall ausgeschlossen sind.

Im Rahmen des Forschungsprojekts ist für diesen Vorgang ein Leitfaden entwickelt worden. Die Anonymisierung erfolgt durch die jeweilige Sachbearbeiterin bzw. den Sachbearbeiter des Jugendamts selbst. Angaben zum Jugendamt sowie zum konkreten Geburtstag und -monat werden geschwärzt. Angaben wie Namen und Orte werden ersetzt. Für den Anonymisierungsprozess werden Hilfslisten zur Verfügung gestellt, damit etwa Namen durch einheitliche Pseudonyme ersetzt werden und die Zusammenhänge nicht für die Forschungsar-

173 § 65 SGB VIII

beit verloren gehen. Der Leitfaden enthält den Hinweis, dass nach Abschluss der Bearbeitung die Liste mit den Originalnamen zu vernichten ist.

Fälle von Kindeswohlgefährdungen, die spezifische Besonderheiten aufweisen, müssen allerdings von der Forschungsarbeit ausgeschlossen werden. Auch mit dem im Übrigen vorgesehenen Anonymisierungsverfahren sind bei diesen Fällen Rückschlüsse auf einen konkreten Sachverhalt nicht ausgeschlossen. Denn über aufsehenerregende Fälle wird häufig in der Presse berichtet. Kriterien für den Ausschluss von der Untersuchung sind verbindlich festzulegen. Die Forschenden haben zugesagt, dies ebenfalls in den Leitfaden für die Jugendamtsbeschäftigten aufzunehmen.

Werden die Vorgaben des Leitfadens durch die Jugendämter umgesetzt, fehlt es nach Vernichtung der Liste an einer Zuordnungsmöglichkeit. Ab diesem Zeitpunkt ist bei Einhaltung aller weiteren Vorgaben grundsätzlich von einer Anonymität der Angaben auszugehen. Aus Datenschutzsicht ist dieses Vorgehen zu begrüßen.

Sozialdaten dürfen grundsätzlich nur in anonymisierter Form an Forschende herausgegeben werden. Fälle, die spezifische Besonderheiten (z. B. Berichterstattung in den Medien) aufweisen, sind in der Regel einer Anonymisierung nicht zugänglich. Denn Rückschlüsse auf konkrete Sachverhalte können nicht ohne Weiteres ausgeschlossen werden.

8.2 Hochschulen

8.2.1 Auslagerung des Bibliotheksmanagements

Berliner Hochschulen sind an uns mit der Frage herangetreten, ob das Bibliotheksmanagement auf einen „Software as a Service"-Dienst eines Anbieters außerhalb der Europäischen Union umgestellt werden kann. Mit der Software sollen u. a. Daten der Bibliotheksnutzenden wie Stammdaten, Ausleihhistorien und Gebührentatbestände verarbeitet werden. Für den Einsatz des Dienstleisters, der die Software bereitstellt sowie betreut und dabei auch

mit den Daten der Bibliotheksnutzenden in Berührung kommt, muss eine Rechtsgrundlage vorliegen.

In der Regel werden „Software as a Service"-Dienste als Auftragsdatenverarbeitung durchgeführt. Das Berliner Datenschutzgesetz sieht allerdings keine Möglichkeit vor, Datenverarbeitungen durch Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union ausführen zu lassen. Vorgesehen ist nur, dass Auftragsdatenverarbeitungen in einem anderen Bundesland oder einem Mitgliedstaat der Europäischen Union durchgeführt werden.[174] Die Auslagerungen von Datenverarbeitungen an einen Anbieter außerhalb der Europäischen Union sind somit nicht zulässig.[175]

Allenfalls reine Wartungen der Datenverarbeitungssysteme durch Stellen außerhalb der Europäischen Union können zulässig sein.[176] Wartungen sind zeitlich beschränkte Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen, die einer strengen Zweckbindung unterliegen. Zur Wartung zählen die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung, Reparatur und der Austausch von Hardware.

Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Wenn die Systemgestaltung dies nicht gewährleistet, ist durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugriff auf die für die Wartung unbedingt notwendigen personenbezogenen Daten beschränkt wird. Die schriftliche Regelung zur Wartung muss insbesondere vorsehen, dass nur bestimmtes Personal die Wartung vornimmt sowie mit welchem Verfahren der temporäre Wartungszugriff durch die verantwortliche Stelle freigeschaltet und kontrolliert werden kann.

Öffentliche Stellen des Landes Berlin können Datenverarbeitungen im Auftrag nur in einem anderen Bundesland oder einem Mitgliedstaat der Europäischen Union durchführen lassen.

174 § 3 Abs. 4 BlnDSG
175 Siehe oben 2.2
176 § 3 a Abs. 2 Satz 2 Nr. 10 BlnDSG

8.2.2 Keine Einsicht in die Prüfungsakte?

Ein Petent hat im Oktober 2012 bei der Senatsverwaltung für Bildung, Jugend und Wissenschaft die Einsichtnahme in seine Prüfungsakte zum Ersten Lehramtsstaatsexamen, das er im Oktober 2010 abgelegt hatte, beantragt. Die Einsichtnahme wurde von der Senatsverwaltung unter Hinweis auf die Erste Lehrerprüfungsordnung (1. LPO) bzw. den Zeitablauf abgelehnt.

In der 1. LPO ist geregelt, dass der Prüfungskandidat das Recht hat, innerhalb eines Jahres nach Bekanntgabe des Ergebnisses einer Teilprüfung sowie des Gesamtergebnisses der Prüfung die Prüfungsakte beim Prüfungsamt einzusehen.[177] Wir haben die Senatsverwaltung für Bildung, Jugend und Wissenschaft darauf hingewiesen, dass sich der Regelung nicht zwingend entnehmen lässt, dass nach Ablauf eines Jahres seit der Bekanntgabe des Prüfungsergebnisses eine Einsichtnahme ausgeschlossen sein soll. Insbesondere kann die 1. LPO das durch das Berliner Datenschutzgesetz (BlnDSG) zeitlich unbeschränkt gewährleistete Akteneinsichtsrecht nicht beschränken.[178] Hintergrund ist, dass nach der Verfassung von Berlin (VvB) Inhalt, Zweck und Ausmaß einer Verordnungsermächtigung im Gesetz bestimmt werden müssen.[179] Dies bedeutet, dass der Gesetzgeber festlegen muss, welche Fragen durch die Rechtsverordnung geregelt werden sollen. Die der 1. LPO zugrundeliegende Verordnungsermächtigung im Lehrerbildungsgesetz (LBiG) enthält jedoch keine Ermächtigung zur Beschränkung von Akteneinsichtsrechten.[180]

Der Petent hat sich auf unsere Argumentation im Verwaltungsgerichtsverfahren berufen. Daraufhin hat die Senatsverwaltung die Einsicht gewährt. Hierbei hat die Senatsverwaltung zunächst betont, die Einsicht ohne Anerkennung einer Rechtspflicht zu gewähren. Das Verfahren wurde schließlich für erledigt erklärt. Im Nachgang teilte die Senatsverwaltung uns mit, dass die Richtigkeit der von ihr ursprünglich vertretenen Rechtsauffassung in der Tat zweifelhaft sei.

177 § 21 Abs. 4 1. LPO
178 § 16 Abs. 4 BlnDSG
179 Art. 64 Abs. 1 Satz 2 VvB
180 § 7 Abs. 3 Nr. 1 LBiG

Ein Prüfungskandidat hat auch nach Ablauf eines Jahres seit der Bekanntgabe des Prüfungsergebnisses grundsätzlich das Recht, in seine Prüfungsakte zu seinem Ersten Lehramtsstaatsexamen Einsicht zu nehmen.

8.3 Schulen

8.3.1 Sprachförderverordnung

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat uns den Entwurf einer Sprachförderverordnung[181] vorgelegt. Die Verordnung regelt das Verfahren der Sprachstandsfeststellung und der vorschulischen Sprachförderung nach dem Schulgesetz.[182] Durch die verbindliche vorschulische Sprachförderung soll „Nicht-Kita-Kindern" mit Sprachförderbedarf ermöglicht werden, die für die erfolgreiche Teilnahme am Schulunterricht erforderlichen Kenntnisse der deutschen Sprache zu erwerben. Datenschutzrechtlich von Bedeutung ist insbesondere das Verfahren zur Ermittlung der betroffenen Kinder.

Das Schulamt des Bezirkes erhält die Meldedaten der betroffenen Kinder, um deren Eltern auffordern zu können, die Sprachstandsfeststellung bei ihrem Kind durchführen zu lassen. Da es hierbei lediglich um die „Nicht-Kita-Kinder" geht, erfolgt ein Datenabgleich der dem Schulamt gemeldeten Kinder mit denjenigen Kindern, die bereits eine Kindertageseinrichtung besuchen. Da die eine Kindertageseinrichtung besuchenden Kinder in dem in der Jugendhilfe berlinweit eingesetzten IT-Fachverfahren[183] registriert sind, erfolgt ein Abgleich mit dem dort enthaltenen Datenbestand. Auf diese Weise werden lediglich die Daten derjenigen Kinder herausgefiltert, die noch keine Kindertageseinrichtung besuchen. Wir haben gegenüber der Senatsverwaltung eingewandt, dass sie

181 Verordnung zur Regelung der Sprachstandsfeststellung und vorschulischen Sprachförderung von nicht in öffentlich finanzierten Tageseinrichtungen der Jugendhilfe oder öffentlich finanzierten Tagespflegestellen betreuten Kindern und zur Änderung der Grundschulverordnung

182 § 55 Schulgesetz (SchulG)

183 Integrierte Software Berliner Jugendhilfe - ISBJ

zwar das IT-Fachverfahren für die Jugendämter zur Verfügung stellt, die Hoheit über die dort erfassten Sozialdaten der Kinder und ihrer Familien jedoch allein beim Jugendamt des jeweiligen Bezirksamtes liegt. Die Senatsverwaltung wird im Auftrag der Bezirke tätig, die weiterhin die Verantwortung für die Daten der „Kita-Kinder" behalten. Auch im Rahmen der vorschulischen Sprachförderung ist es notwendig, der Bezirkshoheit über die im ISBJ-Verfahren gespeicherten Daten Rechnung zu tragen. Ein Abgleich der Daten der Kinder hat zwischen dem bezirklichen Schulamt und dem bezirklichen Jugendamt zu erfolgen. Technisch wird der Abgleich über das zentrale IT-Fachverfahren vorgenommen. Wir haben empfohlen, dies auch im Text der Verordnung zum Ausdruck zu bringen. Allerdings ist die Senatsverwaltung unserem Vorschlag nicht gefolgt. Mit der zwischenzeitlich in Kraft getretenen Sprachförderverordnung wurde eine Formulierung gewählt, die in Anlehnung an eine entsprechende Regelung im Schulgesetz[184] missverständlich ist.

In den Rechtsnormen für den Schul- und Jugendbereich ist klarzustellen, dass die Verwendung eines zentralen IT-Fachverfahrens nicht die datenschutzrechtliche Verantwortlichkeit auf die Senatsverwaltung übergehen lässt. Vielmehr bleibt die Bezirkshoheit und damit die datenschutzrechtliche Verantwortlichkeit der Jugend- bzw. Schulämter für die personenbezogenen Daten der Kinder und ihrer Familien unberührt. Wir erwarten, dass die Senatsverwaltung diese Anforderungen künftig bei der Normsetzung berücksichtigt.

8.3.2 Übergabe des Sprachlerntagebuchs an Schulen

Mit dem Sprachlerntagebuch sind wir seit der Einführung im Jahre 2006 immer wieder befasst. Zuletzt haben wir über das Anliegen der Bildungssenatorin berichtet, eine Weitergabe der Lerndokumentation als Teil des Sprachlerntagebuchs an die Grundschulen zu ermöglichen.[185] Zwischen der Senatsverwaltung für Bildung, Jugend und Wissenschaft und unserer Behörde wurde ein Verfahren abgestimmt, das nunmehr auf der Grundlage

184 § 64 Abs. 4 Satz 2 SchulG
185 JB 2013, 12.1.4

der Einwilligung der Eltern eine Weitergabe der Lerndokumentation an die Grundschulen erlaubt.

Wir haben stets deutlich gemacht, dass wir das zunächst von der Senatsverwaltung favorisierte Verfahren einer Widerspruchsmöglichkeit für die Eltern vor der Weitergabe der Lerndokumentation nicht mittragen können. Vielmehr bedarf es einer ausdrücklichen Einwilligung der Eltern. Erfreulicherweise hat die Senatsverwaltung daraufhin ein entsprechendes Verfahren entwickelt, das keinen datenschutzrechtlichen Bedenken mehr begegnet.

Das zum Schuljahr 2014/15 erstmalig praktizierte Verfahren lässt sich wie folgt zusammenfassen: Den Eltern wird kurz vor dem Übergang in die Grundschule von der Kindertageseinrichtung eine Einwilligungserklärung vorgelegt, mit der sie über den pädagogischen Nutzen der Weitergabe der Lerndokumentation aufgeklärt und in der sie gebeten werden, ihre Einwilligung in die Übermittlung an die Grundschule zu erteilen. Ist die künftige Grundschule des Kindes noch nicht bekannt, wird die Lerndokumentation zunächst verschlossen an das zuständige Schulamt gegeben. Den Eltern wird außerdem die Möglichkeit eingeräumt, ihre Einwilligung bis zu einem von der Kita festgelegten Zeitpunkt widerrufen zu können. Zu Beginn des 2. Schulhalbjahres der ersten Klasse reicht die Schule die Unterlagen an die Eltern zurück.

Mit dem gewählten Verfahren der Weitergabe der Lerndokumentation konnten die Datenschutzbedenken ausgeräumt werden. Den Eltern allein obliegt die Entscheidung, ob sie der – aus pädagogischen Gründen sicher sinnvollen – Datenübermittlung an die Grundschule zustimmen möchten. Wir gehen davon aus, dass allen Belangen angemessen Rechnung getragen wird und das Kapitel Sprachlerntagebuch damit geschlossen werden kann.

8.3.3 Schülerfotos auf der Schulhomepage – auf immer und ewig?

Ein Schüler hatte während seiner Schulzeit gegenüber der Schule eine Einwilligungserklärung unterzeichnet. Mit dieser stimmte er zu, dass Gruppenfotos von Exkursionen/Projekten, auf denen er (mit-)abgebildet ist, auf der Schulhomepage veröffentlicht werden dürfen. Nachdem er die Schule verlassen hatte, widerrief er seine Einwilligung und verlangte, dass die Fotos, auf denen er (mit-)abgebildet ist, von der Schulhomepage entfernt und von allen Speichermedien endgültig gelöscht werden. Die Schule lehnte dies mit der Begründung ab, dass die Einwilligung[186] nach dem Datenschutzrecht wirksam erteilt worden sei und nicht ohne wichtigen Grund widerrufen werden könne. Außerdem sei der Schüler überwiegend nicht in seiner vollen Gestalt abgebildet und deswegen auch nicht zu erkennen.

Bei Fotos, auf denen Personen abgebildet sind, handelt es sich grundsätzlich um personenbezogene Daten im Sinne des Datenschutzrechts.[187] Das gilt unabhängig davon, ob es sich um ein Einzel- oder Gruppenbild handelt. Dabei ist es unerheblich, ob die abgebildete Person in voller Gestalt, nur teilweise (z.B. Rückansicht) oder im Zusammenhang mit sonstigen Angaben (z.B. Name in der Bildunterschrift) abgebildet ist. Entscheidend ist, ob die Person auf dem Foto von einem anderen Betrachter als genau diese und keine andere Person (wieder-)erkannt werden kann. Auch wenn von der Person auf dem Foto nur Teilbereiche (z.B. verschwommene Umrisse) abgebildet sind, kann sie erkannt werden, wenn der Betrachter aus dem Zusammenhang ableiten kann, dass es sich nur um einen ganz bestimmten Kreis von Personen handeln kann (z.B. wenn in der Bildunterschrift steht: „Exkursion nach Schwerin vom 21.12.2012, Teilnehmer: 13. Jahrgang, Leistungskurs Politische Weltkunde"). Der Personenbezug kann möglicherweise auch ohne größeren Aufwand an Zeit hergestellt werden, wenn moderne Suchmaschinen und Bilderkennungssoftware genutzt werden. Erst wenn das Risiko, dass die abgebildete Person erkannt werden kann, so gering ist, dass es praktisch irrelevant erscheint, fehlt der entscheidende Per-

186 § 6 Abs. 4 Nr. 3 BlnDSG
187 § 4 Abs. 1 BlnDSG

sonenbezug. Jede Schule muss die Frage, ob ein Schülerfoto den Schüler eindeutig erkennen lässt, für jedes einzelne Foto prüfen.

Wenn die Schule solche Fotos an außenstehende Dritte übermittelt, verarbeitet sie personenbezogene Daten des Schülers. Eine solche Datenübermittlung liegt vor, wenn Außenstehende die Fotos, die auf dem Server der Schule bereitgehalten werden, abrufen, also die Fotos auf ihrem Bildschirm sichtbar machen können.

Die Schule darf personenbezogene Daten von Schülern aber nur dann verarbeiten, wenn dies zur Erfüllung ihrer schulischen Aufgaben erforderlich ist oder eine Einwilligung des Schülers vorliegt.[188]

Es ist für die Erfüllung der schulischen Aufgaben allerdings nicht erforderlich, dass die Schule ihre Homepage mit Fotos bestückt, um „lebendiger" über Ausflüge zu berichten. Daher ist die Veröffentlichung der Fotos nur solange erlaubt, wie der Schüler hierin eingewilligt hat. Wenn er eine Einwilligung gegeben hat, kann er sie für die Zukunft widerrufen. Dies kann auch ohne wichtigen Grund geschehen. Denn hier kommt es nicht – wie z.B. bei einem gedruckten Schulbuch – darauf an, dass die Fotos bereits in der Vergangenheit veröffentlicht worden sind und daher bereits „in der Welt" sind. Entscheidend ist, dass die Schule die Fotos für zukünftige Abrufe nicht mehr auf dem Server bereithalten darf.

Der ehemalige Schüler hatte ab dem Zeitpunkt seines Widerrufs einen Anspruch darauf, dass die Schule diejenigen Fotos von der Homepage und von sämtlichen Speichermedien löscht, auf denen er von anderen Personen erkannt werden konnte.

Die Schule darf personenbezogene Daten von Schülerinnen und Schülern in Form von Schülerfotos nur dann verarbeiten, wenn eine Einwilligung der (mit-)abgebildeten Personen vorliegt. Dabei ist jedes Foto von der Schule daraufhin zu überprüfen, ob ein Personenbezug hergestellt werden kann. Eine Einwilligung, dass die Schule Fotos auf der Internetseite veröffentlichen darf, kann jederzeit für die Zukunft widerrufen werden.

188 § 64 Abs. 1 und Abs. 5 Satz 2 SchulG

8.4 Kultur

8.4.1 Novellierung des Landesarchivgesetzes

Aus der Praxis

Bereits 2011 haben wir einen Novellierungsbedarf im Landesarchivgesetz geltend gemacht.[189] Veränderte rechtliche, soziale und technische Gegebenheiten machen eine Neufassung der datenschutzrechtlichen Bestimmungen des Gesetzes notwendig. Es ist erfreulich, dass die Senatskanzlei – Kulturelle Angelegenheiten – nunmehr einen entsprechenden Gesetzentwurf erarbeitet hat.

Wir wurden im Entwurfsstadium eingebunden und konnten bereits im Vorfeld des Gesetzgebungsverfahrens Änderungsvorschläge einbringen. Inhaltlich ist es zu begrüßen, dass der Gesetzentwurf eine Harmonisierung der Regelungen mit dem Berliner Informationsfreiheitsgesetz (IFG) vorsieht, um den aktuell bestehenden Widerspruch zwischen dem Archiv- und dem Informationsfreiheitsrecht im Hinblick auf die nach dem IFG frei zugänglichen Akten der Verwaltung, die nach Abgabe an das Archiv auf Grund der archivrechtlichen Sperrfristen derzeit geheim zu halten sind, auflösen zu können. Auch die vorgesehene Aufnahme einer Möglichkeit zur Verkürzung der Schutzfristen bei Personen der Zeitgeschichte und damit eine Erleichterung der Forschungstätigkeit bewerten wir positiv. Da eine Verkürzung der Schutzfristen lediglich in Betracht kommt, wenn die schutzwürdigen Belange der Betroffenen bei der Entscheidung angemessen berücksichtigt werden, und damit eine Abwägung der kollidierenden Grundrechte auf Informationsfreiheit und informationelle Selbstbestimmung stattfindet, wird den Datenschutzbelangen ausreichend Rechnung getragen. Hinsichtlich der Benutzung von sensitiven Unterlagen, die der Schweigepflicht[190] unterliegen, wie z.B. Patientenakten,[191] wurde eine Harmonisierung mit dem Bundesarchivgesetz vorgenommen. Es wird nunmehr sichergestellt, dass die Benutzung auch nach Erlöschen der Geheimhaltungspflicht eingeschränkt oder versagt werden kann, soweit dies zur Wahrung schutzwürdiger Belange Betroffener erforderlich ist. Wir empfehlen dem

189 JB 2011, 8.1.5
190 § 203 Abs. 1 oder 3 Strafgesetzbuch (StGB)
191 Siehe dazu JB 2008, 9.1

Gesetzgeber weiterhin, angesichts des wissenschaftlichen Interesses an der Forschung mit Patientenakten eine Anpassung des Landeskrankenhausgesetzes vorzunehmen, um eine entsprechende Anbietungspflicht der (auch privatrechtlich organisierten) Krankenhäuser zu schaffen.[192]

Mit den Neuregelungen im Landesarchivgesetz wird ein angemessener Ausgleich zwischen dem Schutz der Persönlichkeitsrechte derjenigen, über die sich personenbezogene Daten in den Archiven befinden, und den Interessen der Archive sowie der Benutzerinnen und Benutzer an der Nutzung des Archivgutes hergestellt.

8.4.2 Ehrenamtliche Bibliotheksbeschäftigte und RFID-Technik

Seit einigen Jahren berichten wir über die flächendeckende Einführung der RFID-Technik in den öffentlichen Bibliotheken.[193] Mit Hilfe dieser Technik soll auch der unzulässige berlinweite Zugriff der Beschäftigten in ehrenamtlich geführten Bibliotheken auf die Nutzerdaten im Rechnerverbund des Verbundes Öffentlicher Bibliotheken Berlins (VÖBB) ausgeschlossen werden. Verbuchungsvorgänge sollen in diesen Bibliotheken ausschließlich mithilfe von Selbstverbuchungsanlagen durchgeführt werden.

Seit diesem Jahr steht in der von Ehrenamtlichen geführten Thomas-Dehler-Bibliothek in Schöneberg der Selbstverbuchungsautomat einschließlich der EC-Kartenfunktion zur Verfügung. Der Zugriff der Beschäftigten auf das Ausleihverbuchungssystem wurde in dieser Bibliothek zwischenzeitlich ausgeschlossen. Es können dort zwar keine Bibliotheksausweise mehr ausgestellt oder verlängert werden, allerdings können die Nutzerinnen und Nutzer dies in jeder anderen Berliner Bibliothek vornehmen lassen. Bisherige Barzahlungen werden durch EC-Kartenzahlungen abgelöst. Im Übrigen ist die Ausleihe

192 Dazu schon JB 2011, 8.1.5
193 Zuletzt JB 2012, 12.1.4

oder Rückgabe von Medien weiterhin wie gewohnt unter Nutzung der Selbstverbuchungsautomaten möglich. Für die Bibliotheksnutzenden sind lediglich geringfügige Einschränkungen hinzunehmen. Die Beschäftigten können sich statt auf administrative Tätigkeiten auf die inhaltliche Beratung und Betreuung der Nutzenden konzentrieren. Auch in der ebenfalls rein ehrenamtlich geführten Kurt-Tucholsky-Bibliothek in Pankow[194] steht mittlerweile die EC-Kartenfunktion zur Verfügung. Bis Jahresende 2014 sollte die Umstellung auf eine datenschutzkonforme Situation erfolgen.

Lösungsmöglichkeiten zum Erhalt der ehrenamtlich geführten Bibliotheken sind seinerzeit angesichts ihrer bildungspolitischen Bedeutung zwischen allen Beteiligten intensiv diskutiert worden.[195] Im Ergebnis wurde eine mit der Einführung der RFID-Technik verbundene technische Lösung vom VÖBB favorisiert und umgesetzt. In der Öffentlichkeit, aber auch in den Bezirken, wird diese Lösung offenbar gelegentlich in Frage gestellt. Nach der geltenden Rechtslage ist ein berlinweiter Zugriff Ehrenamtlicher auf die Daten der Nutzenden unzulässig und daher auszuschließen.[196] In welcher Weise die gesetzlichen Anforderungen umgesetzt werden, entscheiden die Beteiligten.

Sollten Ehrenamtlichen darüber hinausgehende Zugriffsrechte gegeben werden, müsste der Gesetzgeber dies mit bibliothekarischen Qualitätsanforderungen verbinden.

194 JB 2012, 12.1.4
195 JB 2009, 8.1; JB 2011, 8.1.6
196 Ausführlich zur Rechtslage JB 2009, 8.1

9 Wirtschaft

9.1 Banken und Versicherungen

9.1.1 SCHUFA-Einmeldung nach 35 Jahren

Aus der Praxis

Ein Bürger hatte 1978 bei einer Bank ein Girokonto eröffnet. Die SCHUFA-Klausel musste er nicht unterschreiben, zu diesem Zeitpunkt arbeitete die Bank noch nicht mit der SCHUFA zusammen. Im August 2013, also nach 35 Jahren, übermittelte die Bank Daten über das Girokonto und die in der Zwischenzeit bewilligte Kreditlinie an die SCHUFA. Aus der Einmeldung ging nicht hervor, wann das Konto eröffnet wurde. Die Bank begründete die Einmeldung damit, dass sie nach dem 2010 in Kraft getretenen § 28a Abs. 2 BDSG berechtigt sei, auch ohne Einwilligung des Betroffenen Girokontodaten an die SCHUFA zu übermitteln. In der Zwischenzeit habe sie alle „Altfälle" eingemeldet. Sie vermutete, dass die Einmeldungen für die Betroffenen nur positiv seien, insbesondere deren Score-Wert verbessert würde.

§ 28a Abs. 2 BDSG ermöglicht grundsätzlich die Übermittlung von Girokontoinformationen (Positivdaten) ohne Einwilligung der Betroffenen. Die Formulierung zeigt, dass der Gesetzgeber diese Norm nur für Neukundinnen und -kunden geschaffen hat.[197] Die rückwirkende Anwendung dieser Norm ist nicht möglich. Die Bank hat die Betroffenen nicht einmal vorab über die verspätete SCHUFA-Einmeldung informiert. Kritisiert haben wir auch, dass die Bank der SCHUFA nicht den Tag der Girokontoeröffnung mitgeteilt hat, sodass diese nur den Tag der Einmeldung speicherte. Es ist davon auszugehen, dass ein längerer Girokontovertrag zu einem besseren Score-Wert führt als ein kürzerer. Die Annahme der Bank, die Einmeldung würde bei den Betroffenen zu einer Verbesserung des Score-Wertes führen, ist reine Spekulation. So ist

197 Siehe § 28a Abs. 2 Satz 2 BDSG: Der Betroffene ist vor Abschluss des Vertrages hierüber [die Datenübermittlung] zu unterrichten.

bekannt, dass der Besitz mehrerer Girokonten zu einer Verschlechterung des Score-Wertes führen kann.

Die SCHUFA hat die personenbezogenen Daten des Petenten inzwischen gelöscht. Bezüglich der anderen Altfälle haben wir die Bank gebeten, die SCHUFA aufzufordern, alle eingemeldeten Altfälle zu löschen.

35 Jahre nach Eröffnung eines Kontos muss kein Bankkunde mehr mit einer SCHUFA-Einmeldung rechnen.

9.1.2 Online-Einwilligung in SCHUFA-Erklärung

Aus der Praxis

Bei dem Online-Kreditkartenantrag einer Bank wird auf die Bedingungen und Erklärungen verwiesen, die zum Download zur Verfügung stehen. Durch einen roten Balken wird im Text besonders hervorgehoben, dass die Unterlagen eine Einwilligung zum Datenaustausch zwischen der Bank und der SCHUFA sowie einer weiteren Auskunftei enthalten. Außerdem muss der Kunde die folgende Erklärung anklicken: „Ich bestätige, die vorgenannten Bedingungen und Erklärungen vollständig heruntergeladen sowie gespeichert und/oder ausgedruckt zu haben."

Offline gilt für die SCHUFA-Einwilligungserklärung das Schriftformerfordernis.[198] Es stellt sich immer wieder die Frage, wie Formvorschriften, die für den Offline-Bereich geschaffen wurden, im Online-Bereich umgesetzt werden. In gewissem Umfang wird man an die modernen Kommunikationsformen Zugeständnisse machen müssen. Der Schutzzweck, der hinter der jeweiligen Formvorschrift steht, ist im Internet aber ausreichend abzubilden. Der Antrag enthält zwar eine hervorgehobene Information über ein vorhandenes Formular zur Einwilligung; nähere Informationen über die Datenflüsse, in die man einwilligen soll, fehlen aber. Diese Informationen erhält man auch nicht durch die Bestätigung, die SCHUFA-Erklärung heruntergeladen sowie gespeichert bzw. ausgedruckt zu haben.

198 § 4a Abs. 1 Satz 3 BDSG

Die Informations- und Warnfunktion des Schriftformerfordernisses in § 4a BDSG erfordert es, dass die Bank sicherstellt, dass die Kundinnen und Kunden dazu veranlasst werden, die SCHUFA-Erklärung tatsächlich auch in vollständiger Textform zur Kenntnis zu nehmen. Wir haben der Bank deshalb empfohlen, datenschutzrechtliche Einwilligungserklärungen zu Pflichtfeldern zu machen und sich die Kenntnisnahme durch „Anklicken" bestätigen zu lassen.

Durch die Nutzung des Mediums Internet darf sich das Datenschutzniveau nicht verschlechtern.

9.1.3 Datenspeicherung ohne Geschäftsbeziehung

Bei dem Besuch einer Bankfiliale aus einem konkreten Anlass erfuhr ein Bürger, dass die Bank personenbezogene Daten zu seiner Person speicherte, obwohl er die Geschäftsbeziehung zu der Bank vor mehr als zehn Jahren beendet hatte. Gespeichert waren u. a. Name, Anschrift, Geburtsdatum, Familienstand und berufliche Stellung (arbeitslos). Die Bank empfahl ihm, einen Antrag auf Datenlöschung zu stellen, dem würde dann entsprochen. Eine Information, warum die Daten weiter gespeichert waren, erhielt der Kunde trotz Nachfrage nicht.

Aus der Praxis

Nach Abschluss der Geschäftsbeziehung haben die Banken die personenbezogenen Daten der ehemaligen Kunden zu löschen bzw. zu sperren.[199] Einen Antrag auf Löschung muss der Betroffene nicht stellen. Die Speicherung der Petentendaten war also rechtswidrig.

Unsere Ermittlungen ergaben, dass die Bank bei Beendigung der Kontobeziehung fälschlicherweise davon ausging, dass der Kunde noch ein Schließfach besitze. Deshalb seien seine Daten nicht gelöscht worden. Wieso die Bank es für erforderlich erachtete, von einem Schließfachnutzer das Datum „arbeitslos" zu speichern, blieb offen. Es überrascht auch, dass der aufgetretene Fehler über zehn Jahre niemandem aufgefallen war.

199 § 35 Abs. 2 Satz 2 Nr. 3, Abs. 3 Nr. 1 BDSG

Verantwortliche Stellen sind verpflichtet, durch ein Lösch- und Sperrkonzept sicherzustellen, dass sich nur erforderliche Daten im operativen Geschäft befinden.

9.1.4 Einblick in Überweisungen am Terminal ohne PIN?

Aus der Praxis

Mehrere Kundinnen und Kunden der Berliner Sparkasse haben sich darüber beschwert, dass an Überweisungsautomaten der Bank vorherige Überweisungen ohne Eingabe der PIN sichtbar sind. Bei einem Diebstahl oder Verlust der Karte könnten Dritte hierdurch feststellen, an wen die Betroffenen Geld überwiesen haben. Das Problem besteht bei allen Sparkassen. Eine frühere PIN-Eingabe lehnten die Sparkassen ab, da eine PIN-Eingabe erst in dem Moment erforderlich sei, in dem es zu einer Verfügung komme. Die Inhaberinnen und Inhaber der Sparkassencard müssten sich vor Verlust und Diebstahl der Karte schützen. Außerdem bestehe die Möglichkeit, die Karte sperren zu lassen.

Die Sparkassen übersehen, dass sich auf den Überweisungen nicht nur die personenbezogenen Daten der Karteninhaberinnen und -inhaber befinden, sondern auch und gerade die Daten Dritter, die keinen Einfluss darauf haben, ob mit den Karten sorgfältig umgegangen wird. Deshalb sollte eine PIN-Eingabe erfolgen, sobald am Kundenterminal nicht nur der Kontoauszug gedruckt wird, sondern darüber hinausgehende Informationen zur Verfügung gestellt werden, wie etwa eine Liste mit den Kontoverbindungen der Personen, an die regelmäßig Geld überwiesen wird.

Diese Forderung haben die Sparkassen zwar nicht erfüllt, sie haben aber ihr Verfahren zumindest deutlich verbessert. Für SEPA-Überweisungen können die Kundinnen und Kunden neuerdings durch ein entsprechendes Häkchen bei jedem Überweisungsvorgang festlegen, ob sie die Empfängerin oder den Empfänger mit der Kontoverbindung „in den Speicher legen“ möchten. Im Mai 2015 wird der Speicher (einmalig) vollständig geleert. Durch Nichtsetzen des Häkchens kann man dann eine Anzeige von Überweisungsdaten verhindern.

Bei Überweisungen am SB-Terminal sind auch die personenbezogenen Daten von Dritten zu schützen.

9.1.5 Familienanamnese im Versicherungsantrag

Ein Fachanwalt für Versicherungsrecht hat alle Aufsichtsbehörden um Bewertung der folgenden Frage an die zu versichernde Person bezüglich der Familienanamnese gebeten: „Sind bei Ihren Eltern oder Geschwistern vor dem Alter von 65 Jahren Herz-Kreislauf-Erkrankungen, Schlaganfall, Krebs, Zuckerkrankheit, Alzheimer, Parkinson, Multiple Sklerose oder andere Erbkrankheiten vorgekommen?“

Familienanamnesen sind regelmäßig datenschutzrechtlich bedenklich, da hier sensitive Daten Dritter erhoben werden. Derartige Daten können grundsätzlich nur mit Einwilligung der Eltern bzw. Geschwister verarbeitet werden. Dies gilt umso mehr, wenn die zu versichernden Personen, die die Frage nach Erbkrankheiten mit „Ja“ ankreuzen, nach weiteren Einzelheiten gefragt werden. Die Versicherungen sollten deshalb auf die Erhebung von Familienanamnesedaten verzichten.

Denkbar ist allenfalls, für die Familienanamnese die Grundsätze des Gendiagnostikgesetzes (GenDG) anzuwenden. Danach wäre eine Familienanamnese für bestimmte Risikoversicherungen möglich, wenn eine Leistung von mehr als 300.000 Euro oder mehr als 30.000 Euro Jahresrente vereinbart wird.[200] In diesem Fall müssten die Versicherungen verpflichtet werden, die erlangten Daten nur für den Zweck der Antragsprüfung zu verwenden. Im Übrigen müssten die Daten gesperrt werden. Eine Konkretisierung, welches Familienmitglied erkrankt ist, sollte unterbleiben.

Die generelle Frage nach Familienanamnesedaten durch Versicherungen ist rechtlich bedenklich.

200 § 18 Abs. 1 Satz 2 GenDG

9.1.6 Vermischung von Versicherten- und Behandlerdaten

Eine Psychotherapeutin erhielt von ihrer privaten Krankenkasse eine neue Versicherungscard, bei der der Familienname falsch geschrieben war. Nach Reklamation erhielt sie eine neue Card mit ihrem richtigen Namen. Im nächsten Monat wurde ihr wieder eine Versicherungscard mit falschem Namen zugeleitet. Nach weiteren Reklamationen wiederholte sich das Spiel monatlich. In der Zwischenzeit erhielt sie auch mehrere Schreiben ihrer Lebensversicherung. Auch dort wurde sie nicht mit ihrem richtigen Namen angeschrieben.

Die Krankenversicherung und die Lebensversicherung gehören zu einer Versicherungsgruppe. Sie sind deshalb berechtigt, Stammdaten von Versicherten in einer gemeinsamen Datenbank zu führen.[201] Allerdings wird die Betroffene nicht nur als Versicherte geführt, sondern in einer weiteren Datenbank als Behandlerin. Die Behandlerdaten werden jeden Monat von einem Adresshändler auf Aktualität überprüft. Anschließend werden die Behandlerdaten mit den Versichertendaten abgeglichen. Bei dem Adresshändler war die Betroffene mit dem falschen Namen gespeichert. Dies führte dazu, dass ihr Name nach jeder „Korrektur" wieder geändert wurde.

Art. 9 des Verhaltenskodexes der Versicherungswirtschaft beschränkt die gemeinsame Verarbeitung von Daten innerhalb einer Unternehmensgruppe grundsätzlich auf Stammdaten von Antragstellern und Versicherten. Die Stammdaten weiterer Personen dürfen nur dann in gemeinsam nutzbaren Datenverarbeitungsverfahren erhoben, verarbeitet und genutzt werden, soweit dies für den jeweiligen Zweck erforderlich ist.[202] Hier ist schon nicht erkennbar, warum Behandlerdaten für andere Versicherungen als die Krankenversicherung relevant sein könnten. Auch gibt es keinen Grund, diese Daten mit Versichertendaten abzugleichen. Das Verfahren der Versicherungen verstößt damit gegen Art. 9 Abs. 2 Satz 1 CoC.

201 Siehe Art. 9 Abs. 1 Verhaltenskodex (Code of Conduct (CoC)) des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV); hierzu JB 2012, 15.1

202 Art. 9 Abs. 2 Satz 2 CoC

Die gemeinsame Verarbeitung von Daten innerhalb von Unternehmensgruppen ist grundsätzlich auf Antragsteller und Versicherte zu beschränken.

9.2 Bonitätsprüfungen durch Auskunfteien und andere Stellen

9.2.1 Scoring-Urteil des Bundesgerichtshofs: Der Gesetzgeber ist gefordert

Bürgerinnen und Bürger werden bei ihrer Teilnahme am Wirtschaftsleben zunehmend mit sog. Scores bewertet. Der Bundesgerichtshof hat eine lang erwartete Entscheidung zur Auskunft über die Berechnung solcher Score-Werte gefällt.[203] Die Gewichtung der in diese Werte eingeflossenen Merkmale sowie Angaben zu Vergleichsgruppen müssen nicht mitgeteilt werden. Betroffene haben damit kaum eine Möglichkeit, die Berechnungsergebnisse zu hinterfragen.

Score-Werte sind Wahrscheinlichkeitswerte, die von Stellen wie Auskunfteien über Bürgerinnen und Bürger etwa zu deren Zahlungsfähigkeit errechnet werden. Banken errechnen oder beziehen solche Score-Werte z.B., um über die Vergabe von Krediten zu entscheiden. Aber auch im Handel, der Telekommunikations- oder etwa der Versicherungsbranche werden Score-Werte immer häufiger eingesetzt.

Auskunftsansprüche zu Wahrscheinlichkeitswerten sind in § 34 BDSG geregelt. Bürgerinnen und Bürger haben einen Anspruch darauf zu erfahren, welche Datenarten zur Berechnung genutzt und wie der Wahrscheinlichkeitswert zu ihrer Person zustande gekommen ist. Obwohl der Wortlaut insofern eindeutig scheint, herrschte über den konkreten Umfang der Auskunft bisher Unklarheit. Die Unternehmen berufen sich auf Geschäftsgeheimnisse.

203 Urteil vom 28. Januar 2014 - VI ZR 156/13

Der Bundesgerichtshof folgte dem insoweit, als er die Methode der Score-Berechnung (die Score-Formel) als Geschäftsgeheimnis geschützt sieht. Dies ist nachvollziehbar, da hieran vor allem gegenüber der Konkurrenz tatsächlich ein Geheimhaltungsinteresse besteht. Für Bürgerinnen und Bürger wird die mathematische Formel in der Regel auch keinen Erkenntnisgewinn bringen. Um eine gewisse Kontrolle hinsichtlich der Berechnungen ausüben zu können, benötigen sie aber Auskünfte zur Gewichtung der in die Berechnung eingeflossenen Faktoren. Der Bundesgerichtshof hält jedoch auch dies sowie Angaben über Vergleichsgruppen für einen wesentlichen Bestandteil der Score-Formel und somit vom Geschäftsgeheimnis umfasst. Die Kenntnis sämtlicher in die Berechnung eingeflossener Einzeldaten soll ohne Rangfolge ausreichen, um das Zustandekommen eines Score-Werts nachzuvollziehen.

Praktisch besteht für Bürgerinnen und Bürger allein anhand dieser Informationen jedoch keine Möglichkeit, den zur eigenen Person errechneten Wahrscheinlichkeitswert einzuordnen. Dies erscheint umso problematischer, als die Einsatzbereiche von Score-Berechnungen in einer zunehmend automatisierten Handelswelt ständig ansteigen – mit zum Teil existenzieller Bedeutung für die betroffenen Bürgerinnen und Bürger. Der Gesetzgeber ist jetzt aufgerufen, das Transparenzdefizit zu beheben.

Der Gesetzgeber sollte eine Lösung schaffen, die sowohl den Geheimhaltungsinteressen der Wirtschaft als auch den Informationsinteressen der Betroffenen Rechnung trägt. Es sollte jedenfalls die Auskunft darüber zu erteilen sein, mit welcher Gewichtung welche Merkmale in die Berechnung eingeflossen sind.

9.2.2 Bonitätsabfragen ohne Sinn und Verstand durch Online-Händler

Aus der Praxis

Wir erhielten häufig Beschwerden von Bürgerinnen und Bürgern über Bonitätsabfragen durch Internetversandhändler bei Auskunfteien. Grundsätzlich sind solche Abfragen nur dann gesetzlich erlaubt, wenn das Unternehmen ein sog. „kreditorisches Risiko“ trägt. Ein solches liegt vor allem

dann vor, wenn der Verkäufer mit der Versendung der Ware in Vorleistung tritt und eine Rechnungs- oder eine Ratenzahlung vereinbart wird.

In den uns berichteten Fällen hatten Internetversandhändler auch dann Bonitätsabfragen durchgeführt, wenn die Ware mit Kreditkarte oder im Voraus bezahlt wurde. In diesen Fällen bestand kein Risiko des Verkäufers, das es abzusichern galt. Die Abfrage war damit überflüssig. Für die Kunden hingegen können häufige Bonitätsabfragen sehr nachteilig sein. So beziehen einige Auskunfteien die Anzahl der getätigten Abfragen in ihren Score-Wert mit ein. In einem Fall hat uns ein Petent berichtet, dass dies zu einer solchen Verschlechterung seines Score-Werts geführt hat, dass er bei der Aufnahme eines Kredits einen Risikozuschlag bezahlen musste.

Die betroffenen Unternehmen argumentierten, dass es einfacher sei, bei jeder Bestellung automatisch eine Bonitätsprüfung durchzuführen. Außerdem stimme die Kundin oder der Kunde beim Online-Kauf durch Setzen eines Hakens der Bonitätsprüfung zu. Damit kann jedoch nicht die gesetzgeberische Grundentscheidung umgangen werden, dass Händler Bonitätsabfragen nur bei kreditorischem Risiko durchführen dürfen. Insbesondere sind sich viele Kundinnen und Kunden nicht der Tragweite dieser Einwilligung bewusst.

Wir sind auf mehrere große Internetversandhändler zugegangen, um zu erreichen, dass diese unnötigen Bonitätsabfragen abgestellt werden. Manche Unternehmen haben sich einsichtig gezeigt. So hat ein großer Spielzeugversandhändler bereits angekündigt, ab Mitte 2015 eine Einkaufsmöglichkeit anzubieten, bei der keine Bonitätsprüfung durchgeführt wird und nur mit sicheren Zahlungsarten bezahlt werden kann. Wir hoffen, dass auch andere Unternehmen diesem positiven Beispiel folgen und auf datenschutzfreundliche Verfahren umstellen werden.

Bonitätsabfragen dürfen nur dann durchgeführt werden, wenn der Verkäufer ein kreditorisches Risiko trägt. Versandhandelsunternehmen sollten unnötige Abfragen abstellen, da sie für die Kundinnen und Kunden sehr nachteilige Folgen haben können.

9.2.3 Übertragung der Benachrichtigungspflicht auf Dritte

Aus der Praxis

Ein Bürger erhielt irrtümlich Mahnschreiben eines Inkassobüros. Das Inkassounternehmen hatte seine Adresse aufgrund einer Verwechslung von einem Berliner Adresshändler erhalten. Der Bürger beschwerte sich darüber, dass dieser ihn bei Übermittlung seiner Daten nicht benachrichtigt hat. So hätte der Fehler früher aufgedeckt und Ärger vermieden werden können. Der Adresshändler teilte mit, die Benachrichtigung sei Sache des Inkassobüros gewesen.

Auskunfteien und Adresshändler übermitteln Daten von Bürgerinnen und Bürgern an ihre Kunden, z.B. Inkassounternehmen. Dies erfolgt etwa, um die aktuelle Anschrift nicht erreichbarer Schuldner zu ermitteln. Betroffene sind grundsätzlich von der erstmaligen Übermittlung ihrer Daten zu benachrichtigen.[204] Dies dient der Transparenz der Datenverarbeitung, wodurch insbesondere die Kontrollierbarkeit der Datenflüsse hergestellt wird. Damit dieser grundlegende Zweck erreicht wird, darf es keine Verantwortlichkeitslücken geben. Die Benachrichtigungspflicht trifft die Stelle, die die Übermittlung vornimmt.

Eine Pflicht zur Benachrichtigung besteht ausnahmsweise dann nicht, wenn der Betroffene auf andere Weise von der Speicherung oder Übermittlung Kenntnis erlangt hat.[205] Diese Kenntnis kann z.B. aufgrund der Information einer anderen Stelle wie einem Inkassobüro, das mit dem Betroffenen in direktem Kontakt steht, erlangt werden. Auch eine vertragliche Übertragung der Benachrichtigungsaufgabe auf die andere Stelle ändert allerdings nichts an der rechtlichen Verantwortlichkeit der übermittelnden Stelle.

Wenn die Information durch eine andere Stelle vorgenommen werden soll, ist der verantwortlichen Stelle zu raten, hierzu eine umfassende vertragliche Regelung zu treffen. Formulierungen und Verfahren der Benachrichtigung müssen verbindlich vorgegeben werden. Die Einhaltung der Vorgaben muss – zumindest stichprobenartig – kontrolliert werden.

204 § 33 Abs. 1 Satz 2 BDSG
205 § 33 Abs. 2 Nr. 1 BDSG

Die Benachrichtigungspflicht kann nicht mit abstrakten Informationen zu möglicherweise zukünftig stattfindenden Datenübermittlungen erfüllt werden. Dieses Vorgehen widerspricht dem Sinn und Zweck der Benachrichtigungspflicht. Abstrakte und für die Betroffenen nicht zutreffende Informationen dienen nicht der Transparenz von Datenflüssen, sondern erschweren sie sogar. Werden nur bei bestimmten Ereignissen wie Verzug und Unerreichbarkeit des Schuldners Abfragen durchgeführt, ist er über die konkrete Übermittlung zu benachrichtigen. Die Information kann auch im Rahmen des Anschreibens erfolgen, das etwa von einem Inkassobüro anhand der ermittelten Adresse an den Betroffenen gerichtet wird.

Die Verantwortlichkeit für die ordnungsgemäße Benachrichtigung trägt die übermittelnde Stelle, auch wenn eine andere Stelle mit der Information der Betroffenen beauftragt wird. Die Benachrichtigung wird nur ordnungsgemäß erfüllt, wenn sie auch inhaltlich Transparenz über die tatsächlichen Datenflüsse gewährleistet.

9.3 Kundenbindung bei der Berlin Partner für Wirtschaft und Technologie GmbH

Die Berlin Partner für Wirtschaft und Technologie GmbH (früher: Berlin Partner GmbH) ist durch Ausgliederung aus der Senatsverwaltung für Wirtschaft, Technologie und Frauen entstanden. Aufgabe der GmbH ist es, entsprechend den Leitlinien der Wirtschaftspolitik des Landes Unternehmen zu beraten und hierdurch eine Stärkung der Wirtschaftskraft Berlins zu erreichen. Für ihre Arbeit nutzte die GmbH das von Oracle angebotene Produkt „CRM on Demand“. CRM steht für „Customer Relationship Management“ (Kundenbindung). Dabei wurden Kunden- und Beschäftigtendaten in den USA verarbeitet. Da die GmbH von der Senatsverwaltung finanziert wird und für sie eine Geschäftsbesorgung ausführt, wollte die Senatsverwaltung einen lesenden Zugriff auf die im CRM gespeicherten Kunden- und Beschäftigtendaten erhalten. Auch die anderen externen Partner (z.B. Bezirke, IHK, Handwerkskammer) interessierten sich für die CRM-Daten.

Die Verarbeitung der CRM-Daten in den USA erfolgte rechtswidrig. Die GmbH hatte nicht einmal mit Oracle USA einen Auftragsdatenverarbeitungsvertrag abgeschlossen. Außerdem war übersehen worden, dass bei Auftragsdatenverarbeitungen in Drittländern auch dann eine Rechtsvorschrift den Datenfluss erlauben muss, wenn der Vertragspartner in den USA Safe Harbor-zertifiziert ist.[206] Die GmbH hat den Mangel behoben und arbeitet inzwischen mit einem Open Source-Produkt ohne Datenübermittlung in Drittländer.

Die Senatsverwaltung darf auf die bei privaten Ausgliederungen gespeicherten Daten nicht vollständig zugreifen, da die GmbH rechtlich eine eigenständige verantwortliche Stelle ist. Deshalb erhält die Senatsverwaltung neben bestimmten Grunddaten wie Name, Adresse, Ansprechpartner nur noch bestimmte Zusatzinformationen wie z.B. den Hinweis, wann Gespräche mit dem Unternehmen stattgefunden haben. Bei Bedarf erstellen die Beschäftigten der GmbH spezielle Vermerke für die Wirtschaftsverwaltung. Das jetzige Verfahren ist datenschutzrechtlich unproblematisch.

Das CRM der Berlin Partner für Wirtschaft und Technologie GmbH ist inzwischen datenschutzkonform.

9.4 Ich mach' mir die Welt, wie sie mir – mit Auftragsdatenverarbeitung – gefällt

Unternehmen lagern gerne (z.B. aus Kostengründen) Aufgaben aus (Outsourcing). Datenschutzrechtlich sind solche Auslagerungsprozesse nicht einfach zu bewältigen. Da es kein Konzernprivileg im Datenschutzrecht gibt, ist die Weitergabe von personenbezogenen Daten auch zwischen wirtschaftlich verbundenen Unternehmen grundsätzlich eine Datenübermittlung, die einer Rechtsvorschrift bedarf. Einzige Ausnahme: Datenflüsse bei datenverarbeitenden Hilfsfunktionen nach Weisungen des Auftraggebers auf Grundlage eines schriftlichen Auftragsdatenverarbeitungsvertrages. Welche Grenzen gibt es hierbei?

206 § 3 Abs. 8 BDSG, § 4 Abs. 3 Nr. 3 BlnDSG

Immer wieder werden uns Auftragsdatenverarbeitungsverträge von Unternehmen vorgelegt, bei denen die gesetzlichen Voraussetzungen[207] nicht erfüllt sind. Die Datenweitergabe erfolgt in solchen Fällen nicht zum Zwecke der Erhebung, Verarbeitung oder Nutzung von Daten, also nicht für datenverarbeitende Hilfsfunktionen (z.B. zum Einscannen von Dokumenten), sondern zur Erledigung einer anderen Aufgabe, die dem beauftragten Unternehmen in eigener Verantwortung übertragen wird (z.B. Wirtschaftsprüfung). Die Weitergabe von Daten stellt sich in diesen Fällen als notwendiges Beiwerk der übertragenen Aufgabe (Funktion) dar und bedarf einer Einwilligung des Betroffenen oder einer Rechtsgrundlage. Vertraglich können die Rollen „Auftraggeber" und „Auftragnehmer" nicht beliebig zugewiesen werden. Ansonsten hätten es die Unternehmen in der Hand, die datenschutzrechtliche Verantwortung nach eigenem Belieben zuzuweisen, und der Grundsatz, dass die Weitergabe von Daten ohne Vorliegen eines Erlaubnistatbestandes oder einer Einwilligung verboten ist, könnte leicht durch eine solche Vereinbarung umgangen werden. Gesetzliche Verantwortlichkeiten können vertraglich nicht aufgehoben werden, da es sich um zwingendes Recht handelt. Beispielsweise können Arbeitgeber in Bezug auf Daten ihrer Beschäftigten nicht zum Auftragnehmer gemacht werden. Entsprechendes gilt für Unternehmen in Bezug auf ihre Kundendaten. Beim Outsourcing müssen Unternehmen deshalb genau prüfen, wie die Auslagerung datenschutzrechtlich zu bewerten ist und ob diese als eine Auftragsdatenverarbeitung abgebildet werden kann.

Das Verbot mit Erlaubnisvorbehalt für Datenübermittlungen darf nicht durch eine „gewillkürte Auftragsdatenverarbeitung" umgangen werden.

9.5 Schulessen garniert mit unbefugten Datenübermittlungen

Eine Petentin beschwerte sich über die Verwechslung ihrer personenbezogenen Daten mit denen einer anderen Kundin beim Vertragsabschluss für das Schulessen ihres Kindes. Beide hatten jeweils im Vertragsbestätigungsschreiben des Unternehmens die Daten der anderen Kundin erhalten.

207 § 11 BDSG

Obwohl die Petentin das Unternehmen auf diesen Fehler aufmerksam machte, versandte das Unternehmen ihren geänderten Datensatz wiederum an die andere Kundin.

Häufig sind Datenschutzverstöße auf mangelhafte Organisationsabläufe oder technisch-organisatorische Regelungen im Unternehmen zurückzuführen. Schnell können solche Fehler in der Unternehmensstruktur – wie vorliegend – zu unbefugten Datenübermittlungen führen. Gerade bei Start Up-Unternehmen werden datenschutzrechtliche Anforderungen häufig bei der Gründung nicht mitbedacht. Klein angefangen und schnell gewachsen hatte auch dieses Unternehmen seine Organisation vorrangig an der Auftragserfüllung ausgerichtet und sich nicht mit datenschutzrechtlichen Anforderungen beschäftigt. Ein Verfahrensverzeichnis, die Verpflichtung der Beschäftigten auf das Datengeheimnis und die Bestellung eines betrieblichen Datenschutzbeauftragten waren nicht erfolgt. Bei einer Vor-Ort-Kontrolle haben wir die Geschäftsleitung über die notwendigen Maßnahmen aufgeklärt. Das Unternehmen hat die Mängel daraufhin unverzüglich beseitigt.

Auch Start Up-Unternehmen müssen datenschutzrechtliche Anforderungen bei der Gestaltung ihrer Organisation von Anfang an mitbedenken, um Datenschutzverstöße zu vermeiden.

9.6 Augen auf beim Datenkauf – Ankauf von personenbezogenen Daten für die Telefonwerbung

Aus der Praxis

Mehrfach beschwerten sich Petenten bei uns über unerwünschte Werbeanrufe. In einigen Fällen wussten sie nicht, wie die Unternehmen an ihre Daten gekommen waren. Obwohl die Betroffenen versicherten, zu keiner Zeit der Verarbeitung ihrer Daten für Telefonwerbung zugestimmt zu haben, verwiesen die Unternehmen ihrerseits auf vorhandene Einwilligungserklärungen.

Es ist eine gängige Praxis, dass Datensätze für Telefonwerbung bei Adresshändlern gekauft werden. Dieses Vorgehen ist nur zulässig, wenn die Betrof-

fenen in die Erhebung, Verarbeitung oder Nutzung ihrer Daten zu diesem Zweck eingewilligt haben.[208] Häufig entsprechen die Einwilligungserklärungen, die die Adresshändler oder Dritte z.B. im Rahmen von Gewinnspielaktionen oder Vertragsabschlüssen einholen, jedoch nicht den gesetzlichen Anforderungen. Die erteilten Einwilligungserklärungen sind unwirksam, und die Erhebung, Verarbeitung bzw. Nutzung dieser Daten für Telefonwerbung ist rechtswidrig. Soll dies vermieden werden, muss den Betroffenen mit dem Einwilligungstext verdeutlich werden, für welche Datenverarbeitungsvorgänge, zu welchen Zwecken und für welche Daten das Einverständnis erteilt wird. Die Einwilligung ist regelmäßig schriftlich zu erteilen. Bei Einwilligungen für Telefonwerbung muss aus der Erklärung deutlich hervorgehen, für welche Produktart geworben werden soll und dass die Daten für diese Zwecke an dritte Unternehmen übermittelt werden. Sofern die Einwilligung in andere Erklärungen eingebunden ist (z.B. in die AGB oder Datenschutzerklärung), ist sie optisch deutlich hervorzuheben.[209] Die Zustimmung muss vor dem eigentlichen Werbeanruf erteilt werden.

Käufer von Datensätzen versuchen uns gegenüber häufig, die Verantwortung für die rechtswidrigen Datenverarbeitungsvorgänge auf den Adresshändler abzuwälzen, da diese die unwirksamen Einwilligungserklärungen eingeholt haben. Oftmals werden hierzu vertragliche Regelungen oder Vertragsstrafen vereinbart. Diese Regelungen lassen die gesetzlich zugewiesenen Verantwortlichkeiten im Datenschutz jedoch nicht entfallen. Datenkäufer sind selbst verantwortliche Stellen und daher verpflichtet, durch geeignete Maßnahmen sicherzustellen, dass die Daten rechtmäßig erhoben und verarbeitet werden.[210] Die bloße vertragliche Zusicherung des Verkäufers, dass wirksame Einwilligungserklärungen vorliegen,[211] genügt nicht.[212]

Stattdessen muss sich das ankaufende Unternehmen in einer ersten Stufe durch die Vorlage der verwendeten Blanko-Einwilligungstexte des Verkäufers vergewissern, dass die vom Händler eingeholten Einwilligungserklärungen über-

208 § 28 Abs. 3 Satz 1 BDSG
209 § 4a Abs. 1 BDSG
210 § 3 Abs. 7 BDSG
211 Adresshändler erwecken diesen falschen Eindruck häufig, indem sie ihren zum Kauf angebotenen Adressen eine „Opt-In-Qualität“ bescheinigen.
212 Beschluss des Kammergerichts vom 29. Oktober 2012 - 5 W 107/12

haupt formal den gesetzlichen Anforderungen entsprechen. Diese Prüfung ist zu dokumentieren.

In einer weiteren Stufe sollte das ankaufende Unternehmen die Plausibilität der Datenerhebung durch den Verkäufer prüfen. Unstimmigkeiten bei Gewerbeanmeldungen oder Gewinnspiele, bei denen augenscheinlich veraltete Geräte verlost werden, sprechen nicht gerade für die Seriosität des Verkäufers. Regelmäßig können auch Minderjährige nicht in die Weitergabe ihrer Daten an Dritte zu Werbezwecken einwilligen.[213] Der Bundesgerichtshof hat zudem festgestellt, dass die Speicherung einer IP-Nummer nicht ausreichend ist, um eine Einwilligungserklärung des Betroffenen für Werbeanrufe nachzuweisen, da hiermit nicht belegt werden kann, ob der Betroffene tatsächlich die Daten angegeben hat. Außerdem wird durch eine Bestätigungsmail im elektronischen Double-Opt-In-Verfahren weder ein Einverständnis in Werbeanrufe belegt noch führt sie für sich allein zu einer Beweiserleichterung zugunsten des Werbenden.[214] Eine aussagekräftige stichprobenhafte Überprüfung der angekauften Datensätze sollte nicht durch einen Telefonanruf, sondern schriftlich erfolgen.

Selbst im Falle einer bewussten Täuschung über die Einwilligungsqualität der Datensätze durch den Verkäufer hat der Datenkäufer Sorgfaltspflichten zu beachten: Er muss weitere Telefonaktionen mit unrechtmäßig erhobenen Daten unverzüglich beenden.

Beim Ankauf von Datensätzen für Telefonwerbung darf der Käufer sich nicht allein auf die Zusicherung des Verkäufers zur Qualität der Einwilligungen verlassen. Er muss hierzu selbst sorgfältige Prüfungen vornehmen.

213 BGH, Urteil vom 22. Januar 2014 - I ZR 218/12
214 BGH, Urteil vom 10. Februar 2011 - I ZR 164/09

9.7 Da kann ja jeder kommen – Identitätsnachweis bei Auskunftsersuchen

Jeder hat das Recht, bei privaten und öffentlichen Stellen ohne Angabe von Gründen eine Auskunft über die dort zur eigenen Person gespeicherten Daten zu verlangen.[215] Regelmäßig beschweren sich Petenten bei uns, weil Unternehmen ihre Selbstauskunftsersuchen nicht beantwortet haben. Unternehmen aus dem Bereich Online-Handel verwiesen uns gegenüber wiederholt darauf, dass nicht eindeutig gewesen sei, ob es sich bei der postalisch anfragenden Person um dieselbe handle, die sich mit ihrer E-Mail-Adresse auf der Online-Plattform registriert hatte. Die Auskunftsersuchen seien nicht beantwortet worden, weil nicht ausgeschlossen werden konnte, dass ein Dritter versucht habe, unbefugt Kundendaten zu erschleichen.

Das Bundesdatenschutzgesetz regelt nicht ausdrücklich, inwieweit die auskunftspflichtige Stelle dazu verpflichtet ist, die Identität der Auskunftbegehrenden zu überprüfen. Allerdings ergibt sich die Verpflichtung zu einer entsprechenden Prüfung aus dem Verbot, Daten unbefugt an Dritte zu übermitteln.[216] Eine Überprüfung der Identität ist daher in Zweifelsfällen geboten. Allerdings rechtfertigen Zweifel an der Identität der Auskunftssuchenden es nicht, dass Unternehmen überhaupt nicht auf eine Anfrage reagieren oder ein Ersuchen schlichtweg ablehnen. Die gesetzliche Auskunftspflicht datenverarbeitender Stellen verlangt vielmehr, die Anfragenden aktiv aufzufordern, einen angemessenen Nachweis über ihre Identität zu erbringen.

Im Online-Handel wird es in der Regel genügen, die Anfragenden dazu aufzufordern, das Auskunftsersuchen über ihre E-Mail-Accounts, mit denen sie registriert sind, zu bestätigen. In anderen Wirtschaftsbereichen kann auch die Übersendung der Kopie eines amtlichen Dokuments zur Identitätsprüfung erforderlich werden, wenn z.B. die Anschrift der Anfragenden von der dem Unternehmen bekannten Adresse abweicht. In diesen Fällen sollten die Daten,

215 § 34 Abs. 1 Satz 1 BDSG
216 § 4 Abs. 1 BDSG

die zur Identitätsprüfung nicht erforderlich sind, wie z.B. die Personalausweisnummer, geschwärzt werden.

Es ist unzulässig, Selbstauskunftsersuchen aufgrund von Zweifeln an der Identität der Anfragenden zu ignorieren oder abzulehnen. Unternehmen sind vielmehr dazu verpflichtet, die Anfragenden aufzufordern, ihre Identität nachzuweisen.

9.8 Auskunftsrecht der Erben im Todesfall?

Trotz zunehmender Internetnutzung treffen nur wenige Bürgerinnen und Bürger bezüglich ihrer digitalen Kommunikation Vorsorge für den Todesfall. Für die Erben und Hinterbliebenen ergeben sich hierdurch zahlreiche Probleme. Nicht immer haben Unternehmen ein Interesse daran, personenbezogene Daten von Verstorbenen aus ihren Beständen zu entfernen. Können Erben einen datenschutzrechtlichen Auskunftsanspruch geltend machen?

Mit dem Tode einer Person geht deren Vermögen auf die Erben über. Höchstpersönliche Ansprüche sind dagegen nicht vererbbar. Erben können daher grundsätzlich keine Auskunft über zum Erblasser gespeicherte Daten nach dem Bundesdatenschutzgesetz verlangen, da es für die Geltendmachung von Rechten eine lebende Person voraussetzt.[217] Der höchstpersönliche Auskunftsanspruch kann ausnahmsweise dann vom Erben geltend gemacht werden, wenn die Auskunft zwingende Voraussetzung für die Geltendmachung vermögensrechtlicher Ansprüche ist. In diesem Fall hat der höchstpersönliche Informationsanspruch eine vermögensrechtliche Komponente und ist ausnahmsweise vererblich.[218] Soweit die Durchsetzung vermögensrechtlicher Ansprüche die Auskunftserteilung oder Einsichtnahme des Erben voraussetzt, erstreckt sich der Auskunftsanspruch des Erben auf die mit dem Erbberechtigten verknüpften Daten. Letztendlich sind damit bei der verantwortlichen Stelle gespeicherte Daten zum Verstorbenen betroffen. Da die auskunfterteilende Stelle sicher-

217 § 3 Abs. 1 BDSG
218 Siehe auch JB 2011, 13.3 (S. 193 f.)

zustellen hat, dass Daten nicht an Unbefugte gelangen, bedarf es eines Identitätsnachweises des Erben. Dies muss nicht in jedem Falle durch die Vorlage eines Erbscheines geschehen, da der Erbe nach der Rechtsprechung auch die Möglichkeit hat, diesen Nachweis in anderer Form zu erbringen (z.B. eröffnetes Testament).

Bei vermögensrechtlichen Ansprüchen des Erben kann dieser ausnahmsweise einen datenschutzrechtlicher Auskunftsanspruch geltend machen.

10 Aus der Arbeit der Sanktionsstelle

10.1 Entwicklung von Anordnungen

Wenn Unternehmen nicht bereit sind, festgestellte Verstöße zu beseitigen, können wir eine Anordnung treffen.[219] Wir legen mit einer solchen Anordnung verbindlich fest, welche Maßnahmen in Bezug auf den Datenschutz im Unternehmen zu treffen oder zu unterlassen sind. Vor dem Erlass einer solchen Anordnung hören wir die Unternehmen grundsätzlich zur Sach- und Rechtslage an. Da wir als oberste Landesbehörde kein Widerspruchsverfahren durchführen,[220] ist dies für die Unternehmen die letzte Gelegenheit, die Angelegenheit gütlich beizulegen. Andernfalls erlassen wir eine gebührenpflichtige Anordnung, die nur mit einer Klage vor dem Verwaltungsgericht beseitigt werden kann. In drei Fällen haben wir ein Anordnungsverfahren eingeleitet.

Zur Beseitigung von festgestellten Datenschutzverstößen können wir gebührenpflichtige Anordnungen erlassen.

10.2 Etappensieg: Keine Werbeanrufe unter dem Deckmantel von Zufriedenheitsabfragen

Die Axel Springer SE nutzte 2012 telefonische Zufriedenheitsabfragen zur Qualität des Lieferservices bei ihren Zeitungsabonnentinnen und -abonnenten, um Einwilligungen in Werbung per Telefon, E-Mail oder SMS zu anderen Medienangeboten zu erlangen. Die Betroffenen hatten bei Vertragsschluss in die Nutzung ihrer Telefonnummern für Werbezwecke nicht eingewilligt. Wir hatten diese unrechtmäßige Praxis per Anordnung untersagt.[221] Das Verwaltungsgericht hat nunmehr entschieden, dass die Nutzung der Telefonnummer

219 § 38 Abs. 5 BDSG
220 § 68 Abs. 1 Satz 2 Nr. 1 VwGO
221 JB 2012, 13.6 (S. 140)

zur Einholung der Einwilligung in Werbung (Opt-In) nicht zulässig ist, weil die Betroffenen hierin nicht eingewilligt haben und diese Nutzung gesetzlich nicht erlaubt ist.[222] Solche Opt-In-Abfragen unterfallen als Vorbereitungsmaßnahme dem datenschutzrechtlichen Werbebegriff, der im Interesse eines umfassenden Schutzes der Persönlichkeitsrechte der Betroffenen weit auszulegen ist. Das Urteil ist noch nicht rechtskräftig. Das Oberverwaltungsgericht Berlin-Brandenburg wird über den Fall zu entscheiden haben.

10.3 Entwicklung von Ordnungswidrigkeitenverfahren

Wir haben 25 Bußgeld- oder Verwarnungsbescheide erlassen und Geldbußen in Höhe von insgesamt 88.205 € festgesetzt. In 17 Fällen haben wir einen Strafantrag gestellt.

Obwohl der Europäische Gerichtshof zur Unabhängigkeit der Datenschutzaufsicht bereits 2010 entschieden hat, dass es exekutiven Stellen verwehrt ist, unmittelbar oder mittelbar Einfluss auf Entscheidungen der Datenschutzaufsicht zu nehmen,[223] entspricht das datenschutzrechtliche Bußgeldverfahren diesen Vorgaben bisher nicht. Nach Einlegung eines Einspruchs und bei Aufrechterhaltung des Bußgeldbescheides ist die Datenschutzaufsichtsbehörde verpflichtet, die Akten der Staatsanwaltschaft zu übersenden, die dann vollständig die Verfahrensherrschaft übernimmt. Sie kann beispielsweise ungeachtet der Auffassung der Datenschutzaufsichtsbehörde über die Einstellung des Verfahrens bei Gericht und eine etwaige obergerichtliche Überprüfung der Entscheidung des „Bußgeldgerichts“ bestimmen.[224] Aus den europarechtlichen Vorgaben folgt jedoch, dass Aufsicht und Sanktionsbefugnis in einer Hand liegen müssen und Entscheidungen über Bußgelder ausschließlich der richterlichen Überprüfung unterliegen. Die Datenschutzaufsichtsbehörde muss verfahrensrechtlich als Vertreterin des öffentlichen Interesses an die Stelle der Staatsanwaltschaft treten. Wir haben erfolglos versucht, anlässlich der Änderung des Bundesdatenschutzgesetzes über den Bundesrat hier eine Änderung zu erreichen.

222 VG Berlin, Urteil vom 7. Mai 2014 - 1 K 253.12
223 Urteil vom 9. März 2010, Rechtssache C-518/07, NJW 2010, 1265 ff.
224 § 69 Abs. 4, §§ 72, 75 Abs. 2, §§ 77b, 79 OWiG

Aufsicht und Sanktionen stehen für den Vollzug des Bundesdatenschutzgesetzes in einem untrennbaren Zusammenhang. Der Bundesgesetzgeber bleibt aufgefordert, den europarechtswidrigen Zustand bei datenschutzrechtlichen Bußgeldverfahren zu beseitigen.

10.4 Beispielsfälle

Ein **Bußgeld in vierstelliger Höhe** setzten wir **gegen ein soziales Netzwerk** fest. Die Verantwortlichen unterbanden nämlich trotz Widerspruch eines Betroffenen nicht die weitere Versendung von Weiterempfehlungs-E-Mails („Tell-a-Friend-Button“) über die Internetseite des Netzwerks.[225] Das Unternehmen konnte sich nicht darauf berufen, dass es lediglich eine technische Hilfe zur Kontaktaufnahme vermittelte, die Einladung allein den privaten Absendern zuzurechnen sei und daher keine Werbung darstelle. Durch seinen Widerspruch hatte der Betroffene deutlich zu erkennen gegeben, dass er eine solche Vermittlerrolle des Netzwerkes nicht wünschte. Der Bundesgerichtshof hat bereits entschieden, dass eine Werbe-E-Mail auch dann vorliegt, wenn ein Anbieter auf seiner Webseite die Möglichkeit für Nutzende schafft, Dritten unverlangt eine Empfehlungs-E-Mail zu schicken.[226]

Bereits 2013 haben wir berichtet, dass wir ein fünfstelliges Bußgeld gegen ein Unternehmen festgesetzt haben, dass 3.765 Datensätze von Abonnenten rechtswidrig an ein anderes Unternehmen weitergegeben hatte.[227] Das **Kammergericht** hat unseren **Bußgeldbescheid** auch der Höhe nach inzwischen in der letzten Instanz **bestätigt**.

Ein **fünfstelliges Bußgeld** erließen wir auch **gegen eine Immobiliengesellschaft**, die die Daten eines Immobilieneigentümers aus dem Liegenschaftskataster eines Berliner Vermessungsamtes erhoben hatte. Die Vermessungsämter dürfen Eigentümerdaten grundsätzlich nur an Personen herausgeben, die ein berechtigtes Interesse an dem Erhalt der Daten haben.[228] Das Immobilienun-

225 § 43 Abs. 2 Nr. 5b BDSG
226 Urteil vom 12. September 2013 - ZR 208/12, Rn. 19
227 JB 2013, 14.3 (S. 163)
228 § 17 Abs. 1 Satz 2 Nr. 2 Vermessungsgesetz Berlin; siehe JB 2013, 10.2

ternehmen hatte die Daten unter dem Vorwand abgefragt, von einem bereits vorhandenen Kaufinteressenten beauftragt worden zu sein. Tatsächlich nutzte das Unternehmen die Daten jedoch, um dem Betroffenen allgemeine Informationsmaterialien zu übersenden und für seine Dienste zu werben. Die Erhebung und Speicherung der Daten für diese Zwecke waren rechtswidrig, da das Liegenschaftskataster kein allgemein zugängliches Verzeichnis ist. Die Immobiliengesellschaft hat das Bußgeld gezahlt.

Gegen einen gemeinnützigen Verein, der sich den Schutz von Kapitalanlegern „auf die Fahne geschrieben hat", setzten wir ein **vierstelliges Bußgeld** fest, weil die Verantwortlichen ihrer gesetzlichen Speicherpflicht nicht nachgekommen waren.[229] Der Verein hatte von einer Immobilieneigentümerin, die Unterstützung begehrt hatte, die Kontaktdaten der übrigen Mitglieder der Eigentümergesellschaft erhalten. Diese wurden sodann vom Verein über die vermeintlichen Missstände beim Verkauf der Immobilie informiert und mit den Leistungen des Vereins beworben. Auf Nachfrage konnte der Verein den Betroffenen jedoch nicht beauskunften, von welcher Miteigentümerin er die Daten erhalten hatte, weil diese Information nicht gespeichert worden war. Zweifelhaft ist bereits, ob der Verein die Daten der Miteigentümer überhaupt erheben und für Werbezwecke nutzen durfte. Jedenfalls wäre er dann jedoch dazu verpflichtet gewesen, die Information, wer ihm die Daten der Betroffenen übermittelt hat, für zwei Jahre zu speichern und Auskunft darüber zu erteilen.[230] Das angerufene Amtsgericht Tiergarten hat unsere Rechtsauffassung in dieser Sache bestätigt.

In einem weiteren Fall von Anlegerwerbung nahm es eine **Rechtsanwaltskanzlei**, die die Interessen einer Fondsanlegerin vertrat, mit dem Datenschutz nicht so genau. Per gerichtlichen Beschluss hatte sie für ihre Mandantin die Herausgabe der Kontaktdaten der übrigen Mitgesellschafter von der Geschäftsführung des Fonds erstritten. Die daraus resultierende Übermittlung der Daten erfolgte streng zweckgebunden zur Durchsetzung der rechtlichen Interessen ihrer Mandantin. Dennoch ließ es sich die Kanzlei nicht nehmen, die Daten der übrigen Anleger dafür zu nutzen, um diese mit ihren Leistungen und Konditionen zu bewerben. Für diese zweckfremde Nutzung personenbezogener

229 § 43 Abs. 1 Nr. 8a BDSG
230 § 34 Abs. 1a BDSG

Daten setzten wir ein **Bußgeld in vierstelliger Höhe** fest.[231] Da die Kanzlei Einspruch eingelegt hat, dem wir nicht stattgegeben haben, wird das Amtsgericht Tiergarten über den Ausgang des Verfahrens entscheiden.

In einem Fall nicht rechtzeitig erteilter Auskünfte setzten wir **ein vierstelliges Bußgeld gegen eine Hausverwaltung** fest. Diese hatte einen Dienstleister damit beauftragt, in einem von ihr verwalteten Haus ein „intelligentes" Gerät zur Messung des Energieverbrauchs der Mieter bereitzustellen. Um auf Bitten eines Petenten die Rechtmäßigkeit der Verwendung dieses Geräts zu überprüfen, forderten wir die Hausverwaltung auf, uns die technischen Details der Datenaufzeichnungen und -übermittlungen im Einzelnen darzulegen. Die Geschäftsführer bestritten jedoch über einen Zeitraum von sechs Monaten ihre Auskunftspflicht. Dies begründeten sie damit, keine Kenntnisse über die Funktionsweise und die technischen Details des eingesetzten Geräts zu haben, da dieses von dem Dienstleister betrieben werde. Darüber hinaus handle die Hausverwaltung auch nur im Auftrag des Hauseigentümers, der die Verantwortung trage. Aus datenschutzrechtlicher Sicht war jedoch die Hausverwaltung die verantwortliche Stelle[232] und somit auskunftspflichtig. Der Dienstleister verarbeitet die Energieverbrauchsdaten der Mieter ausschließlich im Auftrag der Hausverwaltung. In diesem klassischen Auftragsdatenverarbeitungsverhältnis bleibt die Hausverwaltung für die Daten ihrer Mieter verantwortlich.[233] Auch auf den Immobilieneigentümer konnte die Verantwortung nicht abgewälzt werden, da die Auslagerung der Immobilienverwaltung dem Verwalter eine eigenverantwortliche Aufgabenwahrnehmung in kaufmännischer und technischer Hinsicht eröffnet. Im Einspruchsverfahren bestätigte das Amtsgericht Tiergarten unsere Auffassung zur Auskunftspflicht des Immobilienverwalters.

Einige verantwortliche Stellen werden erst durch die Verhängung von Bußgeldern dazu veranlasst, die datenschutzrechtlichen Vorgaben zu beachten.

231 § 43 Abs. 1 Nr. 4 BDSG
232 § 3 Abs. 7 BDSG
233 § 11 Abs. 1 BDSG

11 Europäischer und internationaler Datenschutz

11.1 EU-Datenschutz-Grundverordnung: Nach einem verlorenen Jahr ein Ende des Reformstaus?

Im letzten Jahr hatten wir berichtet, dass im Europäischen Parlament endlich ein Durchbruch bei der europäischen Datenschutzreform erzielt worden war.[234] Nach der Verhandlung von ca. 5.000 Änderungsanträgen wurde ein fraktionsübergreifend befürworteter Kompromissvorschlag am 12. März nahezu einstimmig beschlossen, der ein auf die Herausforderungen der digitalen Welt angepasstes modernes Datenschutzrecht einführen soll.

Leider hat sich seitdem zu wenig getan. Trotz fast dreijährigen Verhandlungen ist es dem Rat, in welchem die Regierungen der Mitgliedstaaten vertreten sind, nicht gelungen, sich auf eine gemeinsame Position zur EU-Datenschutz-Grundverordnung zu verständigen.

Vielmehr wurden grundsätzliche Konzeptionen des Entwurfs, wie zum Beispiel seine Geltung im öffentlichen Bereich oder seine Internettauglichkeit, in Frage gestellt. Dabei war es lange Zeit gerade die Bundesregierung, die den Rechtsakt nicht mit der gebotenen Konsequenz vorangetrieben hat. Zwar hat die Bundesregierung sich stets öffentlich zu einem hohen Datenschutzniveau bekannt. Gleichzeitig verfolgt sie im Rat jedoch einen sog. risikobasierten Ansatz. Dieser sieht vor, dass datenverarbeitende Stellen nur dann besondere Anforderungen erfüllen müssen, wenn ihre Tätigkeiten bzw. die genutzten personenbezogenen Daten in hohem Maße riskant sind. Der Grundsatz, dass besonders risikoreiche Datenverarbeitungen an besonders strengen Maßstäben zu messen sind, ist zwar seit jeher im Datenschutzrecht verankert. Dieser Ansatz darf aber nicht dazu führen, dass bestimmte – scheinbar „harmlose“ – personenbezogene Daten keinem ausreichenden gesetzlichen Schutz unterfallen.[235] Denn im Zeitalter des

234 JB 2013, 2.1

235 Siehe Arbeitspapier der Art. 29-Datenschutzgruppe (bislang nur englische Fassung): Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks vom 30. Mai 2014 (WP 218)

Internets können auch auf den ersten Blick belanglose Daten leicht zu einem detaillierten Persönlichkeitsprofil kombiniert werden, das weitreichende Folgen für die Privatsphäre der Betroffenen hat.

Deshalb haben wir auch einen Vorschlag des Bundesministeriums des Innern und des Bundesministeriums der Justiz und für Verbraucherschutz für eine gesonderte Regelung zur Profilbildung in der Datenschutz-Grundverordnung unterstützt, die auch der Bundesrat gefordert hatte.[236]

Aufgrund der Besonderheiten des europäischen Gesetzgebungsverfahrens ist es also möglich, dass ein Rechtsakt, auf den sich die direkt gewählten Volksvertreter schon seit über einem Jahr fraktionsübergreifend im Europäischen Parlament geeinigt haben, von einzelnen Regierungen im Rat blockiert werden kann. Dies deutet nicht nur auf ein Demokratiedefizit des europäischen Gesetzgebungsverfahrens hin. Es ist auch aus datenschutzpolitischer Sicht fatal, denn der geplante Rechtsakt stärkt nicht nur die Rechte der Menschen in Europa. Er wird auch von der europäischen Wirtschaft dringend benötigt, da ansonsten eine Verfestigung des Wettbewerbsnachteils gegenüber ausländischen, insbesondere US-amerikanischen Datenverarbeitern droht, die sich bislang nur eingeschränkt an europäischen Datenschutzvorgaben messen lassen müssen.

Zuletzt war zu hören, dass das Projekt „Europäische Datenschutzreform“ bis Ende 2015 abgeschlossen werden soll. Dazu haben vor allem die Vorschläge der italienischen Ratspräsidentschaft im zweiten Halbjahr beigetragen. Es bleibt zu hoffen, dass der Reformstau jetzt endlich beendet wird.

11.2 Ende der Vorratsdatenspeicherung

Der Europäische Gerichtshof hat die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten[237] für nichtig erklärt.[238] In seinem wegweisenden Urteil erteilt der Europäische Gerichtshof der undif-

236 Beschluss vom 28. November 2014, BR-Drs. 550/14
237 Richtlinie 2006/24/EG
238 EuGH, Urteil vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12

ferenzierten und automatischen Totalerfassung von Verkehrsdaten in der Telekommunikation eine klare Absage. Zwar ist der Gerichtshof der Auffassung, dass die Vorratsdatenspeicherung einem legitimen Zweck dient. Er weist jedoch darauf hin, dass die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff in das Recht auf Schutz des Privatlebens und auf Schutz personenbezogener Daten darstellt, die in der Europäischen Grundrechte-Charta verbrieft sind.[239] Diese dürfen nur eingeschränkt werden, soweit dies absolut notwendig ist. Nach Auffassung des Gerichtshofs greift die für nichtig erklärte Richtlinie unverhältnismäßig in diese Grundrechte der Unionsbürger ein, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung von Verkehrsdaten verpflichtete.

Eine im Einklang mit der Europäischen Grundrechte-Charta stehende, eventuelle zukünftige Neuregelung müsse insbesondere den Schutz der Träger von Berufs- und besonderen Amtsgeheimnissen (Ärzte, Anwälte, Steuerberater, Parlamentarier und Journalisten) besser berücksichtigen. Für unverhältnismäßig hält der Gerichtshof auch, dass die betreffende Richtlinie in umfassender Weise alle Personen betrifft, die elektronische Kommunikationsdienste nutzen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte.[240] Überdies werde kein Zusammenhang zwischen den Daten, deren Speicherung auf Vorrat vorgesehen ist, und einer eventuellen Bedrohung der öffentlichen Sicherheit vorausgesetzt. Die Vorratsdatenspeicherung werde weder auf die Daten des bestimmten Zeitraums, eines bestimmten geografischen Gebiets oder eines bestimmten Personenkreises beschränkt, der in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.[241] Auch fehlten objektive Kriterien zur Beschränkung des Zugriffs der zuständigen nationalen Behörden auf hinreichend schwere Straftaten, die den damit verbundenen Eingriff in die Grundrechte rechtfertigen.

239 Art. 7, 8 der Charta
240 Rn. 58 des Urteils
241 Rn. 59 des Urteils

Mit diesen Anforderungen geht der Europäische Gerichtshof in Teilen noch über die Feststellungen des Bundesverfassungsgerichts in seiner Entscheidung zur Vorratsdatenspeicherung aus dem Jahr 2010[242] hinaus. Ob und wie die Anforderungen des Gerichtshofs in einer eventuellen Nachfolgevorschrift der für nichtig erklärten Richtlinie 2006/24/EG umgesetzt werden können, ist derzeit völlig offen. Klar dürfte sein, dass das Konzept der vorauseilenden flächendeckenden Speicherung von Verkehrsdaten aller Telekommunikationsteilnehmer keine Zukunft hat. Insbesondere ist kein grundrechtskonformes Verfahren vorstellbar, mit dem bei einer anlasslosen Vollspeicherung die Berufsgeheimnisse geschützt werden können. Mit dem Wegfall der europarechtlichen Grundlage ist auch die Bundesregierung von ihrem Vorhaben abgerückt, schnell ein Gesetz zur Vorratsdatenspeicherung zur Vermeidung eventueller Strafzahlungen zu verabschieden. Diese Absichtserklärung der Bundesregierung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt.[243] Die Konferenz spricht sich dafür aus, zunächst etwaige Diskussionen auf europäischer Ebene abzuwarten.

Die anlasslose Vorratsspeicherung aller Telekommunikations-Verkehrsdaten verstößt gegen die in der Grundrechte-Charta der Europäischen Union festgelegten Rechte auf Schutz des Privatlebens und der personenbezogenen Daten.

11.3 Gibt es ein Recht auf Vergessen?

Im Sommer hat der Europäische Gerichtshof eine weitere spektakuläre Entscheidung zur Entfernung von Links aus Google-Suchergebnissen getroffen.[244] Damit hat er erheblich zur Stärkung der Datenschutzrechte Betroffener beigetragen. In diesem Zusammenhang wurde auch diskutiert, ob die Entscheidung ein sog. „Recht auf Vergessen" im Internet begründet.

Aus der Praxis

242 BVerfGE 125, S. 260 ff., siehe auch JB 2010, 13.1.
243 Entschließung vom 25. April 2014: Ende der Vorratsdatenspeicherung in Europa!, Dokumentenband 2014, S. 21
244 EuGH, Urteil vom 13. Mai 2014 – C-131/12, NJW 2014, 2257

Das Internet vergisst nicht. Einmal im Internet veröffentlichte Informationen können noch über Jahrzehnte abrufbar sein. Dies gilt ebenso für Belanglosigkeiten und Peinlichkeiten wie für Sachverhalte von höherer Bedeutung. Während z.B. Fotografien oder Briefe aus der Jugendzeit der heute über Dreißigjährigen in Schachteln im Keller verstauben, müssen diejenigen, die mit dem Internet aufgewachsen sind, damit rechnen, auch Jahrzehnte später – z.B. bei einem Bewerbungsgespräch – auf frühere Äußerungen oder Fotografien angesprochen zu werden. Daran kann auch das Urteil des Europäischen Gerichtshofs nichts ändern. Es minimiert aber dieses Risiko deutlich, indem es dem Einzelnen ein Recht gibt, von Suchmaschinen zu verlangen, dass bestimmte Links bei der Eingabe seines Namens nicht angezeigt werden.

Dennoch ist das Urteil des Europäischen Gerichtshofs harsch kritisiert worden. Insbesondere wurde angeführt, die Meinungs- und Pressefreiheit komme dabei zu kurz. Bei genauerer Betrachtung wird aber deutlich, dass das Urteil an keiner Stelle verlangt, dass Presseartikel oder Inhalte z.B. aus Wikipedia gelöscht oder ihre allgemeine Auffindbarkeit unmöglich gemacht werden soll. Vielmehr besagt die Entscheidung lediglich, dass in der Google-Ergebnisliste bestimmte Links nicht mehr angezeigt werden dürfen, wenn nach einem bestimmten Namen gesucht wird. Bei der Eingabe aller anderen relevanten Suchbegriffe ist der gesuchte Inhalt weiterhin auffindbar. Er wird auch nicht gelöscht.

Grund dafür ist, dass der Europäische Gerichtshof zu Recht speziell in der Namenssuche eine besondere Gefahr für das Persönlichkeitsrecht sieht. Denn durch die Namenssuche erhält man mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet erhältlichen Informationen. Diese können zahlreiche Aspekte des Privatlebens betreffen, die ansonsten nicht oder nur sehr schwer hätten miteinander verknüpft werden können. So kann ein mehr oder weniger detailliertes Profil der Person erstellt werden, ohne dass die oder der Betroffene bislang Einfluss auf eine einseitige oder veraltete Darstellung ihrer bzw. seiner Person nehmen konnte. Für die Fälle, in denen die Öffentlichkeit ein Recht darauf hat, etwas über eine bestimmte Person zu erfahren, da sie z.B. ein öffentliches Amt innehat, soll diese Person aber auch nach dem Urteil des Gerichtshofs die Anzeige entsprechender Links nicht verhindern können.

Zudem wurde kontrovers diskutiert, ob das Urteil zur Folge hat, dass die Suchmaschinen jetzt eigenmächtig entscheiden können, was der Einzelne vom Internet zu sehen bekommt. Immerhin sollen sich die Betroffenen zunächst direkt an Google oder die Anbieter anderer Suchmaschinen wenden, um die Entfernung eines Links zu beantragen. Das Unternehmen soll dann entscheiden, ob der Antrag berechtigt ist. Allerdings konnten Suchmaschinenbetreiber schon vor dem Urteil selbst entscheiden, welche Suchergebnisse an welcher Stelle der Ergebnisliste angezeigt werden. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzenden in welcher Reihenfolge angezeigt werden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Andererseits unterlagen Betreiber von Suchmaschinen bereits vor der Entscheidung des Gerichtshofs bei der Gestaltung der Suchergebnisse rechtlichen Beschränkungen. Presseberichten zufolge erhält Google täglich ca. eine Million Löschanträge allein aus urheberrechtlichen Gesichtspunkten. Mit dem Urteil wird klargestellt, dass Suchmaschinenbetreiber neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Insgesamt ist das Urteil des Europäischen Gerichtshofs ein Meilenstein, der die Rechte der Betroffenen stärkt. Wir haben deshalb Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[245] sowie der Art. 29-Datenschutzgruppe[246] unterstützt, die die Umsetzung des Urteils ohne Einschränkungen fordern. Insbesondere darf seine Anwendung nicht auf bestimmte nationale Domains wie z.B. google.de beschränkt werden, da das Urteil ansonsten ohne Schwierigkeiten durch Nutzung außereuropäischer Angebote umgangen werden könnte. Ein durchsetzbares Recht, dass bestimmte Tatsachen im Internetzeitalter vergessen werden, begründet es aber nicht.

245 Entschließung vom 8./9. Oktober 2014: Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen, Dokumentenband 2014, S. 26

246 Bisher nur englische Fassung: Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales", C-131/12, vom 26. November 2014 (WP 225)

Wer durch ein Google-Suchergebnis in seinen Persönlichkeitsrechten verletzt wird, kann künftig von Google die Entfernung dieses Links bei der Namenssuche verlangen. Dazu haben Google und auch andere Suchmaschinen Formulare bereitgestellt.[247]

11.4 Ergebnisse der Art. 29-Datenschutzgruppe

Die Art. 29-Datenschutzgruppe, in der Berlin die Bundesländer vertritt, hat wieder zahlreiche Stellungnahmen beschlossen. So hat sie anhand von Fallbeispielen und vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) untersucht, welche behördlichen Maßnahmen im Bereich der **Freiheit, der Sicherheit und des Rechts** den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit entsprechen, und ihr Verhältnis zum Datenschutz geklärt.[248] Die Anforderungen an **die Informationspflicht** der datenverarbeitenden Stelle bei Datenlecks hat sie unter Heranziehung konkreter Fallszenarien analysiert.[249] Vor dem Hintergrund, dass die EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung in Drittländern[250] nicht auf die Fälle anwendbar sind, in denen nur der Unterauftragnehmer im Drittland ansässig ist, hat die Art. 29-Gruppe ein **Vertragsmodell** für ebendiese Situation erarbeitet, um den praktischen Erfordernissen Rechnung zu tragen.[251] Bereits zuvor hatte die Gruppe zu einem Regelwerk für die Anforderungen an **verbindliche Unternehmensregelungen** Stellung genommen, die den Datenschutzbehörden in Europa vorgelegt werden, und an entsprechende Regelungen für den grenzüberschreitenden Datenschutz, die im asiatisch-pazifischen

247 https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de; https://www.bing.com/webmaster/tools/eu-privacy-reguest

248 Stellungnahme 1/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung vom 27. Februar 2014 (WP 211), Dokumentenband 2014, S. 55

249 Stellungnahme 3/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten vom 25. März 2014 (WP 213)

250 Beschluss 2010/87/EU

251 Arbeitsdokument 1/2014 zum Entwurf von Ad-hoc-Vertragsklauseln „EU-Datenverarbeiter an Unterauftragsverarbeiter außerhalb der EU“ vom 21. März 2014 (WP 214)

Raum zunehmend verankert werden.[252] Trotz weiterhin bestehender Unterschiede zeichnet sich ab, dass sich das Konzept der unternehmensinternen Regelungen zum Datenschutz, das ursprünglich in Deutschland unter maßgeblicher Beteiligung unserer Behörde entwickelt wurde,[253] inzwischen auch weltweit durchsetzt.

Angesichts der Snowden-Enthüllungen zu den nachrichtendienstlichen Aktivitäten der NSA hat die Art. 29-Gruppe zwei Grundsatzpapiere verfasst. Während das eine die menschenrechtliche Situation und die unzureichenden Befugnisse der Datenschutzbehörden im Hinblick auf die europäischen **Nachrichtendienste** untersucht,[254] erfolgt im zweiten Papier eine detailliertere rechtliche Analyse, die auch Empfehlungen zum weiteren Vorgehen der Aufsichtsbehörden in Europa enthält.[255]

Ein weiteres Dokument analysiert die Wirksamkeit und Grenzen von **Anonymisierungstechniken** und spricht Empfehlungen für den Umgang mit ihnen aus.[256] Ein Grundsatzpapier befasst sich mit dem **Begriff des „berechtigten Interesses"** der datenverarbeitenden Stelle.[257] Daneben hat die Gruppe das Urteil des Europäischen Gerichtshofs zur Nichtigkeit der Richtlinie zur **Vorratsdatenspeicherung** begrüßt und grundsätzliche Empfehlungen für die nationalen Gesetzgeber formuliert.[258] Ausführlich befasste sich die Gruppe mit den Auswirkungen des **„Internet der Dinge"**.[259] Ebenfalls untersucht wurden

252 Stellungnahme zu einem Regelwerk für die Anforderungen an verbindliche unternehmensinterne Regelungen, die den nationalen Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents" vorgelegt werden, vom 27. Februar 2014 (WP 212)

253 Siehe JB 2002, 3.2 und 4.7.3

254 Stellungnahme 4/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken vom 10. April 2014 (WP 215), Dokumentenband 2014, S. 85

255 Bisher nur englische Fassung: Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes vom 5. Dezember 2014 (WP 228)

256 Stellungnahme 5/2014 zu Anonymisierungstechniken vom 10. April 2014 (WP 216)

257 Bisher nur englische Fassung: Opinion 6/2014 on the Notion on Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC vom 9. April 2014 (WP 217)

258 Bisher nur englische Fassung: Statement on the Ruling of the Court of Justice of the European Union (CJEU) Which Invalidates the Data Retention Directive vom 1. August 2014 (WP 220)

259 Bisher nur englische Fassung: Opinion 8/2014 on the Recent Developments on the Internet of Things vom 16. September 2014 (WP 223)

Techniken, die als **Alternativen zu Cookies** verwendet werden, um das Erfordernis der Einwilligung zu umgehen.[260] Mit den Konsequenzen des Urteils des Europäischen Gerichtshofs zum **Recht auf Vergessen**[261] hat sich die Art. 29-Gruppe ebenfalls befasst und dabei Richtlinien für die Suchmaschinenbetreiber sowie einen Kriterienkatalog verabschiedet, um eine möglichst einheitliche Auslegung des Urteils durch die Aufsichtsbehörden in Europa zu erreichen.[262] Festgelegt wurde auch ein neues **Kooperationsverfahren** für die Fälle, in denen einer Aufsichtsbehörde ein Datenexportvertrag vorgelegt wird, der von den EU-Standardvertragsklauseln abweicht, aber gleichwohl vom Datenexporteur als mit diesen vereinbar angesehen wird.[263] Schließlich hat die Art. 29-Gruppe in einer **Grundsatzerklärung** die globalen Herausforderungen der digitalen Welt skizziert, in der die europäischen Datenschutzstandards mit weltweiten Sicherheitsinteressen in Einklang gebracht werden müssen. Zu diesem 15 Punkte-Katalog sind Stellungnahmen interessierter öffentlicher oder privater Interessenvertreter willkommen.[264]

11.5 Weitergabe von Studierenden- und Beschäftigtendaten in die USA

Ein Beschäftigter einer US-amerikanischen Universität hat uns darüber informiert, dass Daten der Beschäftigten und der Studierenden zwischen der Niederlassung in Berlin und der Hauptniederlassung in den USA ausgetauscht würden. Die Universität teilte mit, dass es sich bei dem Büro am Standort Berlin um eine unselbständige Niederlassung handele.

260 Bisher nur englische Fassung: Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting vom 25. November 2014 (WP 224)

261 Siehe 11.3

262 Bisher nur englische Fassung: Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales", C-131/12, vom 26. November 2014 (WP 225)

263 Bisher nur englische Fassung: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual Clauses" Considered as Compliant With the EC Model Clauses vom 26. November 2014 (WP 226)

264 Gemeinsame Erklärung der europäischen Datenschutzbehörden im Rahmen der Art. 29-Datenschutzgruppe vom 26. November 2014 (WP 227), Dokumentenband 2014, S. 105

Der Zugriff auf die Beschäftigtendaten stellt aufgrund der Unselbständigkeit des Berliner Büros formal keine Datenübermittlung dar.[265] Datenweitergaben an Niederlassungen außerhalb des Europäischen Wirtschaftsraums sind allerdings im Lichte der Europäischen Datenschutzrichtlinie[266] auszulegen. Damit sind sie als Datenübermittlungen zu behandeln.

Personenbezogene Daten dürfen nur dann an Stellen in Staaten außerhalb des Europäischen Wirtschaftsraumes, sog. Drittstaaten, übermittelt werden, wenn gewährleistet ist, dass beim Datenempfänger ein angemessenes Datenschutzniveau besteht. Dies ist z.B. dann der Fall, wenn für den Drittstaat von der EU-Kommission ein angemessenes Datenschutzniveau festgestellt wurde. Wenn eine solche Feststellung – wie im Fall der USA – nicht vorliegt, können Datenübermittlungen erfolgen, wenn beim Datenempfänger ausreichende Datenschutzgarantien vorhanden sind. Solche ausreichenden Garantien können u. a. durch die Vereinbarung der von der EU-Kommission anerkannten Standardvertragsklauseln geschaffen werden.

Zwischen einer Organisation und ihren rechtlich unselbständigen Niederlassungen können Standardverträge nicht abgeschlossen werden. Dies würde ein unzulässiges In-Sich-Geschäft darstellen. Gleichwohl können Standardvertragsklauseln inhaltlich verwendet werden, wenn sich die Organisation auf sie verpflichtet, intern umsetzt sowie intern und extern zugänglich macht. Die vom Datentransfer betroffenen Personen müssen ggf. ihre Rechte wirksam geltend machen können. Zur Herstellung externer Verbindlichkeit bietet sich eine Garantieerklärung an, durch die ein Vertrag mit den betroffenen Personen zustande kommt. Dies kann erfolgen, indem die Standardvertragsklauseln nebst entsprechender Erklärung, sich an sie zu halten, in das Internet/Intranet (je nach betroffenem Personenkreis: Studierende oder Beschäftigte) gestellt oder in sonstiger Weise gegenüber den betroffenen Personen zugänglich gemacht werden.

Im Sinne rechtlicher Verbindlichkeit insbesondere zugunsten der von einem Datentransfer betroffenen Personen können auch zwischen einer Hauptniederlassung und einer unselbständigen Niederlassung Standardvertragsklauseln verwendet werden.

265 Es handelt sich nicht um einen „Dritten“ im Sinne von § 3 Abs. 8 Satz 2 BDSG.
266 95/46/EG

12 Datenlecks

12.1 Datenlecks in der Wirtschaft

12.1.1 Verantwortlichkeit eines Insolvenzverwalters

Die Kassenärztliche Vereinigung Berlin informierte uns, dass in den ehemaligen Räumlichkeiten eines Medizinischen Versorgungszentrums Patientenunterlagen gefunden wurden. Diese wurden der Hausverwaltung übergeben. Da das Medizinische Versorgungszentrum insolvent war, wurde ein Insolvenzverwalter bestellt. Er veranlasste schließlich die gesicherte Versendung an ein anderes Medizinisches Versorgungszentrum.

Vorab war die Frage zu klären, ob der Insolvenzverwalter in die Pflichten des alten Medizinischen Versorgungszentrums als Schuldner eintritt. Allgemein geht die Verwaltungs- und Verfügungsbefugnis über das Vermögen des Schuldners mit der Eröffnung des Insolvenzverfahrens auf den Insolvenzverwalter über.[267] Er erhält damit die Befugnis, alle mit den Patientenunterlagen verbundenen Prozesse zu führen und wird auch zur datenschutzrechtlich verantwortlichen Stelle.

Entscheidend war, dass die Kenntnisnahme durch Dritte zu einem Zeitpunkt erfolgte, als das Medizinische Versorgungszentrum bereits insolvent war. Damit hatte der Insolvenzverwalter sicherzustellen, dass niemand von den Unterlagen Kenntnis nimmt. Er ist damit nicht in die Pflichten des Versorgungszentrums eingetreten, sondern war selbst nach dem Datenschutzrecht verpflichtet, bestimmte Maßnahmen zu ergreifen.

Im Ergebnis war allerdings nicht von einer schwerwiegenden Beeinträchtigung für die Rechte und Interessen der Betroffenen auszugehen. Zwar ist von einer drohenden schwerwiegenden Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen in der Regel auszugehen, wenn

267 § 80 Insolvenzordnung

sensitive personenbezogene Daten wie Gesundheitsdaten[268] betroffen sind. Im vorliegenden Fall hatte allerdings nur die Hausverwaltung die Patientenunterlagen gesichtet. Die möglichen nachteiligen Folgen waren auch angesichts der Zeitspanne zwischen Auszug des Medizinischen Versorgungszentrums und Fund der Unterlagen überschaubar.

Der Insolvenzverwalter wird mit Eintritt des Insolvenzverfahrens zur eigenen verantwortlichen Stelle. Ihm obliegt daher die Pflicht zur Einhaltung der gesetzlichen Vorschriften des Bundesdatenschutzgesetzes. Der Insolvenzverwalter hat daher für die unverzügliche sichere Verwahrung personenbezogener Unterlagen zu sorgen.

12.1.2 Aktenfund in der ehemaligen Kinderklinik Weißensee

Der Polizeipräsident in Berlin informierte uns über einen Aktenfund in der ehemaligen Kinderklinik Weißensee. Diesen hatte ein Bürger mit einer anonymen E-Mail bei einer regionalen Tageszeitung gemeldet, die daraufhin die Polizei verständigte.

Wir haben unverzüglich eine Ortsprüfung durchgeführt. Dabei haben wir mehrere Müllsäcke mit personenbezogenen Daten in einem Kellerraum des verfallenen Gebäudes sichergestellt. Bei den Akten handelte es sich um Bewerbungsunterlagen und personenbezogene Unterlagen von Prüfungen vor der Berliner Ärztekammer, zum Teil mit Patientenbezug, die allerdings keiner beruflichen Aufbewahrungspflicht unterlagen.

Es stellte sich heraus, dass es sich um Papiere aus dem Privathaushalt einer verstorbenen Ärztin handelte. Ein von den Erben mit der Haushaltsauflösung beauftragter Dienstleister hatte die Papiere zusammen mit anderen Haushaltsgegenständen „entsorgt“. Die von uns kontaktierten Erben wussten von alledem nichts, erklärten sich jedoch unverzüglich bereit, die aufgefundenen Unterlagen datenschutzgerecht zu vernichten.

268 § 42a Satz 1 Nr. 1 i. V. m. § 3 Abs. 9 BDSG

In diesem wie in anderen Fällen von Aktenfunden arbeiten wir eng mit der Polizei zusammen. Wir werden künftig allerdings nur noch Stichproben von gefundenen personenbezogenen Unterlagen in Gewahrsam nehmen, um die datenschutzrechtliche Verantwortlichkeit und die Einleitung von Bußgeldverfahren zu prüfen. Die Sicherstellung ganzer personenbezogener Aktenbestände, die dem Zugriff Unbefugter ausgesetzt sind, ist dagegen Aufgabe der Polizei. Dies haben wir dem Polizeipräsidenten mitgeteilt und ihn um Unterstützung gebeten.

Auch unabhängig von etwaigen gesetzlichen Aufbewahrungspflichten unterliegen patientenbezogene Daten der ärztlichen Schweigepflicht. Diese sind aufgrund ihrer Sensitivität zwingend in der Form zu entsorgen, dass eine Kenntnisnahme durch Dritte künftig nicht mehr möglich ist.

12.1.3 Widerrechtliche Entnahme von Spenderdaten

Ein Verein zur Unterstützung von Tierrechtsprojekten berichtete, dass Daten aus seiner Spendendatei entnommen und gegen den Willen des Vereins für Werbezwecke verwendet worden seien. In den Werbe-E-Mails wurde auf eine andere Tierrechtsorganisation verlinkt und für diese um Spenden geworben.

Eine Sachverhaltsaufklärung durch den Verein führte zu dem Ergebnis, dass über die Namen und reinen E-Mail Adressen hinaus keine weiteren Daten betroffen waren. Ein zunächst angenommener Abgriff von Kontodaten der Betroffenen konnte nicht festgestellt werden.[269] Eine Pflicht zur Benachrichtigung war daher nicht gegeben.

Wir machten den Verein zur Vermeidung weiterer Entwendungen von Spenderdaten darauf aufmerksam, dass ihm als verantwortliche Stelle die Einhaltung der gesetzlichen Vorschriften obliegt. Der Verein haftet demnach auch für Datenlecks, wenn die Verursacherin eine konkurrierende Organisation ist. Da die Weitergabe der Spenderdaten an die Konkurrentin durch eine ehemalige

269 § 42a Satz 1 Nr. 4 BDSG

Mitarbeiterin im Raum stand, empfahlen wir, künftig den Beschäftigten nur die nötigen Rechte für den Zugriff auf die Spenderdatenbank zu geben. Zudem sollte es keine Downloadmöglichkeit von Spenderdaten sowie die Möglichkeit des Anschlusses von mobilen Datenspeichern an die Rechner geben. Schließlich rieten wir zu einer revisionssicheren Protokollierung von Zugriffen.

Die verantwortliche Stelle hat durch eigene Vorkehrungen dafür zu sorgen, dass es nicht zu einer unrechtmäßigen Entwendung der Daten durch externe Personen oder durch eigene Beschäftigte kommt.

12.2 Datenlecks in der Verwaltung

12.2.1 Diebstahl von Laptops im Zahnärztlichen Dienst

Der Zahnärztliche Dienst des Bezirksamtes Charlottenburg-Wilmersdorf meldete den Verlust von drei Laptops. Auf diesen war ein Programm gespeichert, welches zahnärztliche Befunde von Kindern und Jugendlichen einschließlich ihrer Geburtsdaten und Adressen erfasste. Die Daten selbst waren nicht verschlüsselt. Das Bezirksamt ging zunächst nicht von einer Pflicht zur Benachrichtigung der Eltern aus.

Das Bezirksamt nahm zunächst an, dass keine Missbrauchsgefahr mit diesen Daten sowie keine Diskriminierungen drohen. Ein Kariesschaden falle schließlich ohnehin auf. Der Zahnärztliche Dienst befürchtete, dass es durch die Benachrichtigung zu einem Vertrauensverlust bei den Eltern komme. Dies könnte dazu führen, dass zukünftig keine Einverständniserklärungen für die zahnärztliche Untersuchung erteilt werden.

Auch wenn die Zahnbefunde keine Grundlage für einen Missbrauch darstellen, hat das behandelte Kind allerdings ein schutzwürdiges Interesse daran, dass seine Diagnose und die damit verbundene Behandlung geheim gehalten werden. Eine schwerwiegende Beeinträchtigung für die Rechte war gegeben, da es sich bei den Daten um Gesundheitsdaten handelte und der Gesetzgeber diese

unter einen besonderen Schutz gestellt hat.[270] Aus dem Beispielsdatensatz war auch für den Laien erkennbar, wie der Zahnstatus des behandelten Kindes war. Eine zu erwartende Verunsicherung der Eltern sowie eine mögliche Belastung des Vertrauensverhältnisses hatten daher bei der Bewertung außer Betracht zu bleiben. Eine etwaige Rücknahme der Einverständniserklärung ist zudem nur für den Kitabereich möglich, da für den schulischen Bereich die zahnärztliche Untersuchung verbindlich ist.[271]

Letztlich hat sich das Bezirksamt Charlottenburg-Wilmersdorf entschlossen, die Eltern der betroffenen Kinder über den Datenverlust zu unterrichten. Dabei verzichtete das Bezirksamt aus Kostengründen auf ein individuelles Anschreiben und wählte einen Aushang in der Schule.[272] Allerdings enthielt der Aushang keinen Hinweis, welche konkreten Daten betroffen waren. Zudem war nicht sichergestellt, dass auch die Eltern von dem Aushang Kenntnis nehmen.

Um ähnliche Vorfälle zukünftig zu vermeiden, hat der Zahnärztliche Dienst auf unseren Rat hin die neu angeschafften Laptops mit Verschlüsselungstechnik ausgestattet.

Die Information der Öffentlichkeit muss geeignet sein, die konkret Betroffenen zu erreichen. Ein Aushang in der Schule genügt hierfür nicht. Da Eltern von Schulkindern nicht täglich in der Schule anwesend sind, muss garantiert sein, dass diese von dem Vorfall unterrichtet werden. Dies kann z. B. durch einen Elternbrief oder durch Übergabe eines Informationsschreibens bei einem Elternabend erfolgen.

12.2.2 Falschversand von Erhebungsbögen Verstorbener

Im Rahmen der Nacherhebung von Daten zu verstorbenen Patientinnen und Patienten übersandte die Vertrauensstelle des Gemeinsamen Krebsregisters Erhebungsbögen an einen niedergelassenen Arzt, der jedoch nicht

270 § 6 a BlnDSG i. V. m. Art. 8 Abs. 1 Europäische Datenschutzrichtlinie 95/46/EG
271 § 52 SchulG
272 Information der Öffentlichkeit nach § 18a Abs. 2 Satz 5 BlnDSG

der Leichenschauarzt bzw. der behandelnde Arzt war. Bei der Nacherhebung werden regelmäßig fehlende Angaben zur Krebserkrankung auf Grundlage des Leichenschauscheins ergänzt.

Da der betreffende Arzt an der gleichen Adresse wie ein Medizinzentrum niedergelassen ist, wurde er diesem per Meldenummer zugeordnet. Diese Erstzuordnung basierte auf einem menschlichen Eingabefehler. Er erhielt daher die Bögen zur Nacherhebung für das Medizinzentrum.

Anders als das Bundesdatenschutzgesetz, das den Datenschutz an lebende natürliche Personen knüpft,[273] geht das Berliner Datenschutzgesetz weiter. Dort ist geregelt, dass die Daten Verstorbener geschützt werden, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.[274] Daten Verstorbener können gleichzeitig auch Lebende betreffen. Angaben über eine vererbbare Krankheit wie Krebs betreffen auch Nachkommen und sind deshalb personenbezogene Daten der Nachkommen.

Allerdings war in diesem Fall keine schwerwiegende Beeinträchtigung für die Rechte und Interessen der Nachkommen anzunehmen, da der Empfänger als Arzt der beruflichen Schweigepflicht unterlag. Eine Missbrauchsgefahr war daher fernliegend.

Dagegen war die Erstellung bzw. Überarbeitung von organisatorischen Abläufen und Arbeitsrichtlinien des Gemeinsamen Krebsregisters, mit denen eine Wiederholung des Geschehens in Zukunft ausgeschlossen werden kann, erforderlich. Daneben wurde die Anpassung der programmtechnischen Unterstützung angekündigt.

Der Datenschutz von Betroffenen endet nach dem Berliner Datenschutzgesetz nicht mit dem Tod. Gegebenenfalls müssen bei Verlust von sensitiven Daten Verstorbener deren Angehörige benachrichtigt werden.

273 § 3 Abs. 1 BDSG
274 § 4 Abs. 1 Satz 2 BlnDSG

13 Telekommunikation und Medien

13.1 Schutz der Privatsphäre bei SmartTV

Moderne Fernsehgeräte („SmartTV“)[275] ermöglichen neben dem Empfang des Fernsehkanals auch den Aufruf von Diensten im Internet. Damit können die Sender den Zuschauern zeitgleich zum laufenden Programm zusätzliche Inhalte aus dem Web auf dem Fernsehbildschirm anzeigen. Technisch wird dies durch den „Hybrid broadcast broadband TV“ (HbbTV)-Standard ermöglicht. Die bestehende Verbindung zum Internet ermöglicht auch den Zugang zu eigenen Web-Plattformen der Endgerätehersteller, über die verschiedenste Internetdienste angeboten werden. Vielfach ermöglichen die Geräte – wie Smartphones – auch die Installation von Apps.

Anders als beim herkömmlichen Fernsehen entsteht durch die Internet-Verbindung ein Rückkanal, der Fernsehsendern, Endgeräteherstellern, sonstigen Dritten oder deren Auftragnehmern die Erhebung und Verarbeitung von Daten über das individuelle Nutzungsverhalten der Betroffenen ermöglicht. Damit ist die Möglichkeit zur anonymen Nutzung von Fernsehen als wesentliche Voraussetzung für eine freie Meinungsbildung und zur Wahrnehmung des verfassungsrechtlich geschützten Rechts auf freien Informationszugang als Grundbedingung einer freiheitlich-demokratischen Grundordnung gefährdet.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) haben mit den Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten eine gemeinsame Position zum Schutz der Privatsphäre bei Smart-TV veröffentlicht,[276] die auch von der Konferenz der Direktoren der Landesmedienanstalten unterstützt wird. Darin fordern sie, eine anonyme Nutzung von Fernsehangeboten auch bei Smart-TV-Nutzung zu gewährleisten. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

275 Allgemein dazu JB 2011, 12.6

276 „Smartes Fernsehen nur mit smartem Datenschutz“ vom 20. Mai 2014, Dokumentenband 2014, S. 49

Für die „interaktiven" Teile von Web- oder HbbTV-Diensten sind die datenschutzrechtlichen Anforderungen des Telemediengesetzes zu beachten. Danach sind Anbieter u. a. verpflichtet, die Nutzer spätestens bei Beginn der Nutzung umfassend über die Datenerhebung und -verwendung zu informieren.[277] Eine Verwendung von Nutzungsdaten nach dem Ende des Nutzungsvorgangs ist in der Regel nur zu Abrechnungszwecken gestattet. Nutzungsprofile dürfen nur unter Pseudonym erstellt werden; dem Betroffenen ist ein Widerspruchsrecht gegen die Erstellung solcher Profile einzuräumen.

Soweit Gerätehersteller darüber hinaus Daten über die Nutzung ihrer Geräte für eigene Zwecke erheben, darf dies nur auf Grundlage der Einwilligung der Betroffenen erfolgen, wobei die Nutzung wesentlicher Funktionen – insbesondere der Internetfunktionen – nicht von der Einwilligung abhängig gemacht werden darf.

Die Aufsichtsbehörden und die Datenschutzbeauftragten der Rundfunkanstalten fordern darüber hinaus die Beachtung des Prinzips „Privacy by Default". Die Grundeinstellungen der Smart-TV-Geräte und Internet-Angebote müssen durch die verantwortlichen Stellen so gestaltet werden, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Dies bedeutet z.B., dass auf die Übermittlung von dauerhaften Geräteidentifikationsnummern verzichtet wird. Stattdessen können temporäre Kennungen mit kurzer Laufzeit oder generische Typenkennzeichnungen verwendet werden. Auch müssen die auf den Geräten gespeicherten Daten der Kontrolle des Nutzers unterliegen; insbesondere müssen Möglichkeiten zur Verwaltung von Cookies bestehen. Die verantwortlichen Stellen haben schließlich auch dafür Sorge zu tragen, dass die Geräte und der Datenverkehr vor dem Zugriff unbefugter Dritter geschützt sind.

Auf der Grundlage dieses Positionspapiers überprüfen die Datenschutzbehörden der Länder gegenwärtig die Verarbeitung personenbezogener Daten durch Hersteller von Smart-TV-Geräten und Programmanbietern. Die Datenschutzbeauftragten haben darüber hinaus gegenüber der HbbTV-Association Änderungen zum besseren Schutz der Privatsphäre bei der Neufassung der HbbTV-Standards angeregt.

277 § 13 Abs. 1 TMG

Bei der Nutzung von „SmartTVs“ entsteht durch die Internetverbindung ein Rückkanal, der unter Umständen zahlreichen Parteien die Erhebung und Verarbeitung von Daten über das individuelle Nutzungsverhalten der Betroffenen ermöglicht. Damit ist die Möglichkeit zur anonymen Nutzung von Fernsehen als wesentliche Voraussetzung für eine freie Meinungsbildung in der freiheitlich-demokratischen Gesellschaft gefährdet.

13.2 Verfolgung des Nutzerverhaltens im Internet mit Cookies

Schon in der Vergangenheit haben wir mehrfach auf den steigenden Einsatz und die zunehmende Bedeutung von Cookies und verwandten Technologien für die Verfolgung des Nutzerverhaltens im Internet hingewiesen.[278] Nach einer neueren Umfrage konnten demgegenüber weniger als die Hälfte (45 %) der Befragten erklären, was Cookies überhaupt sind.[279] Die schon 2009 geänderte Europäische E-Privacy-Richtlinie[280] erfordert eine Einwilligung, wenn Anbieter Informationen auf Geräten von Nutzenden speichern wollen. Dies betrifft insbesondere die Verwendung von Cookies[281].

Das Bundeswirtschaftsministerium (BMWi) hat es bisher abgelehnt, die Regelungen der Richtlinie in nationales Recht zu überführen. Das BMWi behauptet unzutreffend, Umsetzungsbedarf in deutsches Recht bestehe nicht, da die Regelungen im nationalen Recht bereits der Richtlinie entsprechen. Das Telemediengesetz (TMG) setzt die europarechtlichen Vorgaben jedoch nur unvoll-

278 Siehe zuletzt JB 2012, 16.4.1

279 Initiative D21: D21-Digital-Index 2014, S. 10

280 Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Dokumentenband 2010, S. 34

281 Siehe JB 2010, 2.6. Nach Auffassung der Art. 29-Datenschutzgruppe sind die Regelungen des Art. 5 Abs. 3 der Richtlinie auch auf das „Device Fingerprinting“ (einer weiteren Technologie zur Verfolgung des Nutzerverhaltens, bei der ein Browser aufgrund seiner spezifischen Einstellungen mit einer gewissen Sicherheit bei einem erneuten Besuch wiedererkannt werden kann) anwendbar; siehe Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting vom 25. November 2014 (WP 224, bislang nur englische Fassung)

ständig in nationales Recht um.[282] Weder setzt § 15 Abs. 3 TMG, wie europarechtlich gefordert, schon bei der Speicherung von Informationen im Endgerät der Nutzer an (die Regelung greift erst bei der Erstellung von pseudonymen Nutzungsprofilen), noch müssen die Betroffenen in die Verwendung ihrer Daten einwilligen – das TMG lässt hier ein Widerspruchsrecht ausreichen.

Ohne eine Umsetzung in nationales Recht können die Aufsichtsbehörden für den Datenschutz die Regelungen zur Einwilligung aus Art. 5 Abs. 3 der Richtlinie gegenüber den Anbietern von Telemedien in Deutschland nicht durchsetzen. Die Untätigkeit der Bundesregierung hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre im Internet aus Art. 5 Abs. 3 der E-Privacy-Richtlinie selbst (z.B. vor den Zivilgerichten) durchsetzen müssen. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei Nutzung des Internets vorenthalten. Die Bundesregierung muss die Regelungen der Richtlinie jetzt unverzüglich und vollständig in nationales Recht überführen. Bis dahin kann man den Nutzenden nur raten, durch entsprechende Einstellungen ihrer Browser Selbstschutzmaßnahmen gegen Tracking zu ergreifen.[283]

Die fehlende Umsetzung der Regelungen des Art. 5 Abs. 3 der Richtlinie 2002/58/EG führt dazu, dass den Aufsichtsbehörden gegenüber den Anbietern die Hände gebunden sind. Die Bundesregierung muss jetzt umgehend die Regelungen der Richtlinie in nationales Recht überführen.

13.3 Real World Tracking

Bereits seit einiger Zeit arbeiten Unternehmen weltweit daran, die im Internet verbreitete Verfolgung (Tracking) der Nutzenden auf die physische Welt – insbesondere im Einzelhandel oder in Shoppingcentern – zu übertragen. Tech-

282 Siehe Dokumentenband 2010, S. 28

283 Detaillierte Hinweise auf die existierenden Möglichkeiten zum Selbstschutz haben wir veröffentlicht im JB 2010, 2.6, und im JB 2012, 16.4.

nisch nutzen diese Verfahren den Umstand aus, dass die meisten Menschen heute Smartphones mit sich herumtragen, auf denen die Funktechnik „WLAN“ ständig aktiviert ist. Mit dem Smartphone können sie zu Hause und an anderen Orten mit WLAN-Versorgung schneller und kostengünstiger (ohne Verbrauch des mobilen Datenvolumens) Internetdienste nutzen.

Damit ein Smartphone sich automatisch in einem WLAN-Netz anmelden kann, sendet es regelmäßig eine Art Suchruf mit seiner sog. MAC-Adresse, eine weltweit eindeutige Nummer des Smartphones.[284] Das Smartphone ruft gewissermaßen ständig seinen eigenen Namen in die Umwelt.

Die „Sensoren“ des Trackingunternehmens lauschen nun auf solche Suchrufe und merken sich die „Namen“ der Smartphones. Bei der späteren Analyse kann man so festellen, wie lange einzelne Kundinnen und Kunden sich in welchem Geschäft aufgehalten haben, wo sie nur vorbeigegangen sind und ggf. in welchen Abteilungen sie sich besonders lang aufgehalten haben. Auch mittels der Funktechnik Bluetooth – eingesetzt z.B. für kabellose Kopfhörer – ist Vergleichbares möglich.

Bei der Ausgestaltung solcher Verfahren sind folgende Rahmenbedingungen zu beachten:

- Wer das Geschäft besucht, muss zu Beginn der Datenerhebung auf verständliche Weise über die erhobenen personenbezogenen Daten, die Zwecke der Verarbeitung, die Speicherdauer und Möglichkeiten der Verhinderung der Verarbeitung (Ausschalten der WLAN-Schnittstelle oder des gesamten Smartphones, Widerspruch) informiert werden. Konkret könnte sich der Hinweis an der Eingangstür eines Geschäftes befinden.
- Daten von Passanten dürfen ohne deren vorherige Einwilligung nicht verwendet werden.
- Eine Verarbeitung von Daten über das Besuchsende hinaus darf nur unter Pseudonym erfolgen.

284 MAC = Media Access Control

- Den Besuchenden ist zumindest ein Widerspruchsrecht zu gewähren. Widersprüche müssen bei einer automatisierten Datensammlung auch technisch umgesetzt werden.
- Die Dauer der Speicherung der Daten darf nicht exzessiv sein und muss sich auf den unbedingt notwendigen Zeitraum zur Erreichung eines legitimen Zweckes beschränken. Die betreffenden Firmen werben damit, Stammkunden wiedererkennen zu können. Personenbezogene Daten der Besuchenden zu diesem Zweck dauerhaft oder länger als einige Tage zu speichern, ist allerdings unzulässig.
- Die Datenverarbeitung sollte lokal erfolgen. Insbesondere darf kein übergreifendes Tracking der Besuchenden über mehrere Geschäfte hinweg möglich sein.
- Soweit die Inhaber der Ladengeschäfte die Daten durch Dienstleister verarbeiten lassen, sind Verträge zur Auftragsdatenverarbeitung zu schließen. Dabei sind die Festlegungen des § 11 BDSG zu beachten.

Da die genannten datenschutzrechtlichen Anforderungen sich nur schlecht mit dem Geschäftsmodell einiger Unternehmen vereinbaren lassen, bezweifeln diese teilweise, dass es sich bei den MAC-Adressen (die vom Smartphone „gerufenen Namen“) um personenbezogene Daten handelt. Mit der MAC-Adresse wird zwar nur eine Nummer verarbeitet, diese ist aber zumindest als pseudonymes Datum anzusehen, da damit eine Identifizierung des Besitzers – ggf. unter Mithilfe Dritter – möglich ist. Zudem sind die von einigen Unternehmen genutzten „Anonymisierungsfunktionen“ vielfach nahezu wirkungslos und bewirken allenfalls eine weitere Pseudonymisierung, jedoch keine Anonymisierung.

Neben den Aufsichtsbehörden für den Datenschutz haben auch Hersteller von Smartphone-Betriebssystemen das Problem erkannt. Bei manchen Herstellern kann man den oben beschriebenen Suchruf unterbinden oder zumindest dafür sorgen, dass nicht mehr die eigene MAC-Adresse gesendet wird. Dies schränkt die Tracking-Möglichkeiten erheblich ein.

Smartphone-Nutzern ist unabhängig davon zu raten, WLAN und Bluetooth abzuschalten, wenn diese Funktionen gerade nicht benutzt werden.

Bei eingeschaltetem WLAN oder Bluetooth können die Besucher von Geschäften auf Schritt und Tritt verfolgt werden. Der Einsatz solcher Verfahren setzt jedoch die Beachtung der datenschutzrechtlichen Rahmenbedingungen voraus. Deutsche Firmen nutzen diese Verfahren bisher noch für die Erstellung von Statistiken zu Besucherströmen. US-Unternehmen, die nahezu keinen Restriktionen ausgesetzt sind, nutzen die Technik bereits zu werbewirksamen persönlichen Ansprachen.

13.4 Privacy Sweep: Prüfung von Smartphone-Apps

Zum zweiten Mal nahmen wir an der international koordinierten Datenschutzprüfung „Privacy Sweep" teil. An der Prüfaktion beteiligten sich weltweit 26 Datenschutzaufsichtsbehörden. Im Vergleich zu der Aktion im Jahr 2013 ist die Anzahl der teilnehmenden Aufsichtsbehörden um ca. 45 % gestiegen. Die Prüfung von 1211 Smartphone-Apps umfasste zudem nicht nur die Datenschutzerklärungen der Unternehmen, sondern auch die tatsächliche Verarbeitung personenbezogener Daten durch die Apps bzw. die mit der App verknüpften Online-Dienste der Unternehmen.

Geprüft wurden verstärkt die durch die Apps eingeforderten Zugriffsrechte auf Sensoren und gespeicherte personenbezogene Daten wie z.B. GPS-Position, Kamera, Mikrofon, Kalender- und Kontaktdaten, Nachrichten sowie Geräte-Identifikationsnummern (IDs). Diese wurden in Beziehung gesetzt zu den Informationen in der Datenschutzerklärung und den Zwecken der von der jeweiligen App angebotenen Dienste. Idealerweise sollten nur die minimal zur Erfüllung der Dienstleistungen der App notwendigen Zugriffsrechte eingefordert werden. Zudem müssen die Nutzer über alle Datenverarbeitungen und deren Zwecke verständlich informiert werden.

Bei den Ergebnissen zeigt sich ein erhebliches Verbesserungspotenzial: Während die Mehrheit der Apps eine oder mehrere Zugriffsrechte auf Sensoren und personenbezogene Daten einfordert, treffen weltweit nur 43 % der Apps Aussagen zum Datenschutz und nur 15 % erklären klar, welche Daten bzw.

welche Rechte zu welchen Zwecken erhoben bzw. eingefordert werden. 31 % der Apps forderten zudem Rechte ein, die zumindest für die offensichtlichen Funktionen der App nicht erforderlich waren.

Die Ergebnisse der von uns geprüften Apps von Berliner Anbietern bzw. mit engem Bezug zu Berlin wiesen in eine ähnliche Richtung. Insbesondere die konkreten Angaben zum Zweck der Einholung von bestimmten weitgehenden Rechten können oft noch verbessert werden. Allerdings konnten nach Berücksichtigung der Beschreibungstexte und der einzelnen Funktionalitäten der Apps in 75 % der Fälle auf plausible Zwecke geschlossen werden. Bei 10 % der geprüften Apps wurden jedoch Defizite in einem Umfang festgestellt, die unsere Intervention erforderlich machten. So wird beispielsweise von einer Lieferservice- und einer Gutschein-App die Berechtigung zum Zugriff auf die Kamera eingefordert. Ein Anbieter hat dies bisher plausibel mit einer Funktion zum Scannen von Rabatt-Coupons erklärt. Der andere Anbieter erklärt, dieses Recht für eine Funktion zum automatischen Einlesen von Kreditkarten zu benötigen. Allerdings wird dies nirgends in den Apps offengelegt, und die entsprechenden Funktionen sind kaum aufzufinden. Ein Anbieter hat zugesagt, auf die Einforderung dieses Rechtes ab der nächsten Version zu verzichten und die Datenschutzerklärung nachzubessern. Der andere Anbieter ist der Ansicht, dass es genügt, zukünftig zumindest auf die deutsche Version der Datenschutzerklärung zu verlinken, die jedoch bisher keine Aussagen zu der App enthält, wie beispielsweise zu den eingeforderten Rechten.

Häufiger wurde die Erhebung der Geräte-ID festgestellt. Mittels dieser oder vergleichbarer IDs ist es möglich, ein Gerät eindeutig, dauerhaft und zudem über verschiedene Apps hinweg zu identifizieren. Da die oft unzulässige und exzessive Nutzung dieser Identifikationsnummern insbesondere durch Werbe- und Trackingdienstleister erhebliche Medienresonanz hervorgerufen hat, haben die Betriebssystemhersteller bereits reagiert und die Nutzung dieser IDs eingeschränkt. Die meisten Apps haben daher im Laufe des Jahres die Nutzung der IDs eingestellt.

Insbesondere für App-Anbieter und App-Entwickler haben die Datenschutzaufsichtsbehörden zudem eine Orientierungshilfe veröffentlicht, in der die

rechtlichen und auch technischen Rahmenbedingungen konkretisiert werden, die sich insbesondere aus gesetzlichen Regelungen ergeben.[285]

Problematisch kann aber auch die Einräumung solcher Rechte sein, die erforderlich erscheinen. So erheben 65 % der in Berlin geprüften Apps den jeweils aktuellen Standort des Smartphones mit hoher Genauigkeit. Zwar wurde bei genauerer Prüfung immer eine (Neben-)Funktionalität gefunden – meist eine Karte mit eingezeichneten Standorten und Navigationsmöglichkeit – die die Anforderung des präzisen Standortes erklärt. Dennoch stellt diese Funktionalität ein erhebliches Risiko dar, da jede dieser Apps umfangreiche Bewegungsprofile der Nutzer erstellen könnte. Selbst wenn diese Profile unter Pseudonym erstellt werden, sind oft schon wenige für eine Person markante Punkte (z.B. die Kombination aus Wohn- und Arbeitsort) zur Identifizierung ausreichend. Nutzende sollten daher in jedem Einzelfall prüfen, ob eine bestimmte App und deren Anbieter tatsächlich Zugriff auf die jeweils angeforderten Daten erhalten sollen.

Hilfreich hierfür sind verbindliche und abschließende Aufzählungen zu den Verwendungszwecken, Speicherzeiträumen und den Verknüpfungen der erhobenen Daten. Auch ist es sinnvoll, bestimmte Rechte nur dann (und erst dann) einzufordern, wenn die Funktionalität genutzt wird, die diese Rechte benötigt. Dies stellt allerdings auch Anforderungen an die Hersteller der Smartphone-Betriebssysteme. Bei manchen Anbietern müssen alle jemals im Betrieb notwendigen Rechte bei der Installation eingeräumt werden. Ein Entzug der Rechte ist dort nur durch Deinstallation der jeweiligen App möglich.

75 % der geprüften Apps von Berliner Anbietern erheben nur die notwendigen Daten und informieren die Nutzer in ausreichendem Maße. Bezüglich der Nutzerinformation bestehen jedoch Verbesserungsmöglichkeiten. Eine Orientierungshilfe der Datenschutzaufsichtsbehörden gibt Anbietern und Programmierern Hilfestellung.

285 http://www.datenschutz-berlin.de/attachments/1047/OH_Apps.pdf

13.5 Aus der Arbeit der „Berlin Group“

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. „Berlin Group“) hat unter unserem Vorsitz in ihren Sitzungen am 5. – 6. Mai in Skopje und am 14. – 15. Oktober in Berlin zwei Arbeitspapiere verabschiedet:

Das Arbeitspapier zu **Big Data und Datenschutz**[286] analysiert die durch den zunehmenden Einsatz von Big Data-Technologien entstehenden Risiken für die Privatsphäre. Es enthält Empfehlungen zum datenschutzkonformen Einsatz dieser Technologien.

In dem Arbeitspapier Datenschutz- und Sicherheits-Risiken bei der **Nutzung eigener Endgeräte in Firmennetzwerken** („Bring your own device“ – BYOD)[287] erläutert die Arbeitsgruppe Risiken, die für den Schutz der Privatsphäre der Betroffenen, aber auch für die Sicherheit von Unternehmensnetzwerken durch den Einsatz von privaten Endgeräten entstehen können. Das Papier enthält darüber hinaus Empfehlungen, wie diesen Risiken begegnet werden kann.[288]

286 Dokumentenband 2014, S. 117
287 Dokumentenband 2014, S. 138
288 Siehe bereits JB 2012, 2.3

14 Informationsfreiheit

14.1 Informationsfreiheit in Europa

Der Europäische Gerichtshof hat ein wichtiges Urteil für mehr Transparenz gefällt und den Geheimverhandlungen von Europas Regierungen mit Drittländern wie den USA eine Absage erteilt.[289] Es gab einer niederländischen EU-Abgeordneten Recht, die auf der Grundlage der europäischen Transparenzverordnung[290] beim Rat erfolglos Einsicht in die Stellungnahme der Ratsjuristen zur Rechtsgrundlage der SWIFT-Verhandlungen mit den USA[291] begehrt hatte. Der Rat hatte unter Verweis auf den „Schutz internationaler Beziehungen" nur einen Teil des Dokuments offengelegt. Die Begründung hielt der Gerichtshof für unzureichend; der Rat sei den Nachweis schuldig geblieben, aus welchem Grund das öffentliche Interesse durch die Veröffentlichung der Stellungnahme zur Rechtsgrundlage gefährdet sei.

Die Auswirkung dieses Urteils auf weitere Verhandlungen der EU mit Drittstaaten, insbesondere den USA, liegt auf der Hand. So hat die für den Informationszugang bei europäischen Einrichtungen zuständige Ombudsfrau Emily O'Reilly sich dafür ausgesprochen, dass der Rat das Verhandlungsmandat der EU für das heftig umstrittene Freihandelsabkommen TTIP[292] mit den USA veröffentlicht. Erst auf den zunehmenden öffentlichen Druck hin vollzog die Europäische Kommission im Herbst die Kehrtwende und stellte das Dokument online. Es bleibt jedoch fraglich, ob diese Aktion genügt, um die öffentliche Kritik an den hinter verschlossenen Türen geführten Handelsgesprächen verstummen zu lassen. Ziel des im Rahmen der Welthandelsorganisation (WTO) angestrebten Abkommens ist der Abbau von Handelshemmnissen zwischen Europa und den USA, was durch möglichst freie Datenflüsse zwischen den Kontinenten gewährleistet werden soll. Zwar gelten nationale Datenschutzgesetze nach den Regeln der WTO gerade nicht als abzubauende Handelshemmnisse und sind deshalb auch nicht Bestandteil des TTIP-Verhandlungsmandats

289 EuGH, Urteil vom 3. Juli 2014, C-350/12 P
290 1049/2001/EG
291 Siehe zuletzt JB 2013, 15.1
292 Transatlantic Trade and Investment Partnership

der EU-Kommission. Dennoch besteht ein politischer Zusammenhang zwischen TTIP und dem unzureichenden Datenschutzniveau in den USA. Der Abschluss des Freihandelsabkommens könnte zu einer Herabsetzung der europäischen Datenschutzstandards führen. Bevor es geschlossen wird, muss die EU von den USA grundlegende Datenschutzreformen einfordern.[293]

Möglicherweise werden die europäischen Datenschutzstandards aber noch einschneidender durch ein weiteres multilaterales Abkommen bedroht, über das wiederum derzeit noch geheim verhandelt wird. Bereits seit Anfang 2012 laufen die Verhandlungen zu TiSA,[294] mit dem Handelshemmnisse im Dienstleistungssektor von ca. 50 Ländern beseitigt werden sollen. Da dieses Abkommen außerhalb der WTO geschlossen werden soll, könnten in seinem Rahmen nationale Datenschutzvorschriften als abzubauende Handelshemmnisse angesehen werden. Der im Internet geleakte Entwurf sieht eine Geheimhaltung des Dokuments für fünf Jahre nach Inkrafttreten des Abkommens vor. Tritt es nicht in Kraft, ist das Dokument für fünf Jahre nach Beendigung der Verhandlungen geheim zu halten. In einem Rechtsstaat sind nur veröffentlichte Normen verbindlich. Nichts anderes kann für völkerrechtliche Verträge gelten.

14.2 Informationsfreiheit in Deutschland

Das **Bundesverfassungsgericht** hat entschieden, dass die Bundesregierung Rüstungsexportgeschäfte bis zur abschließenden Genehmigung gegenüber anfragenden Bundestagsabgeordneten geheim halten darf. Die parlamentarische Kontrolle erstrecke sich nur auf bereits abgeschlossene Vorgänge.[295] Damit bleibt es dabei, dass nur der (neuerdings halbjährliche) Rüstungsexportbericht der Bundesregierung für eine begrenzte Transparenz in diesem Bereich sorgt.

Das **Bundesverwaltungsgericht** urteilte, dass die Presse grundsätzlich einen presserechtlichen Anspruch hat, die Namen von an Gerichtsverfahren mitwir-

293 Siehe hierzu die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und Länder vom 13./14. März 2013: Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten, Dokumentenband 2013, S. 16

294 Trade in Services Agreement

295 BVerfG, Urteil vom 21. Oktober 2014, Az.: 2 BvE 5/11

kenden Personen zu erfahren. Das gelte für die Namen von Berufsrichtern und Schöffen, aber auch für die der Staatsanwälte und Verteidiger, weil das Persönlichkeitsrecht dieser Personen hinter dem grundrechtlich geschützten Auskunftsinteresse der Presse zurückstehen muss. Nur der Name der Urkundsbeamtin durfte geschwärzt werden.[296]

In einer weiteren Entscheidung hat das **Bundesverwaltungsgericht** einen Anspruch der Presse auf Informationszugang nach dem Informationsfreiheitsgesetz des Bundes insofern bejaht, als es um den Auskunftsanspruch gegen die Bundestagsverwaltung betreffend die Verwendung der Sachmittelpauschale der Gesamtheit der Abgeordneten ging. Soweit personenbezogene Auskünfte zu einzelnen Abgeordneten (z. B. für wertvolle Füllfederhalter) begehrt würden, stünden diese Informationen im Zusammenhang mit dem Mandat und seien besonders geschützt.[297]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** wies in einer Entschließung darauf hin, dass **Urheberrechte** Dritter nicht pauschal, sondern nur ausnahmsweise einem Informationszugangsbegehren entgegengehalten werden dürfen.[298] Im Hinblick auf die fortschreitende **Privatisierung öffentlicher Aufgaben**, bei denen zumeist große Finanzvolumina eine Rolle spielen, erinnerte die IFK daran, dass Auskunftsansprüche auch direkt gegenüber den Unternehmen geschaffen werden müssen.[299] Die IFK hat auch gefordert, dass die Veröffentlichung amtlicher Informationen ausschließlich über von den öffentlichen Stellen selbst gesteuerte Veröffentlichungsmedien erfolgen muss. Die Nutzung von **Plattformen kommerzieller Internetdiensteanbieter** wie Facebook oder Twitter verbietet sich.[300] Die IFK hat außerdem betont, dass Transparenz betreffend die Arbeit von **Sicherheitsbehörden** Voraussetzung für eine effiziente demokratische Kontrolle und Grund-

296 BVerwG, Urteil vom 1. Oktober 2014, Az.: 6 C 35.13
297 BVerwG, Urteil vom 27. November 2014, Az.: 7 C 19.12
298 Entschließung vom 17. Juni 2014: Das Urheberrecht dient nicht der Geheimhaltung!, Dokumentenband 2014, S. 147
299 Entschließung vom 17. Juni 2014: Keine Flucht vor der Informationsfreiheit ins Privatrecht!, Dokumentenband 2014, S. 148
300 Entschließung vom 17. Juni 2014: Informationsfreiheit nicht Privaten überlassen!, Dokumentenband 2014, S. 148

lage für die Beurteilung der Angemessenheit des staatlichen Eingriffshandelns ist.[301] Angesichts der eingeschränkten **Kontroll- und Beratungszuständigkeit** der Informationsfreiheitsbeauftragten des Bundes und der meisten Bundesländer trat die IFK für eine Erweiterung der Kompetenzen um das Umwelt- und das Verbraucherinformationsrecht ein.[302] Schließlich hat die IFK vor dem Hintergrund der Digitalen Agenda 2014-2017, der Digitalen Verwaltung 2020 und dem Nationalen Aktionsplan zur Umsetzung der G8 Open-Data-Charta die zügige Umsetzung dieser Regierungsprogramme gefordert, die u. a. die Einführung einer gesetzlichen Regelung für **Open Data** und die Schaffung von Open-Data-Ansprechpartnern in den Behörden vorsehen.[303]

Ein Meilenstein in puncto behördlicher Transparenz in Deutschland wurde mit dem Hamburger **Transparenzportal** gesetzt, das seit Oktober online ist.[304] Damit wurde der vom Hamburgischen Transparenzgesetz vorgesehene Zeitrahmen von zwei Jahren für die Einrichtung des Registers exakt eingehalten. Dort sind nun die meisten Dokumente der Stadtverwaltung für jedermann sichtbar bei gleichzeitiger Beachtung des Datenschutzes eingestellt. Das sollte für die Bundeshauptstadt das maßgebliche Beispiel sein.

14.3 Informationsfreiheit in Berlin

14.3.1 Gebühren für „Negativauskünfte“?

Wiederholt stellte sich die Frage, ob für „Negativauskünfte“ – also für die Auskunft, dass eine bestimmte Information nicht vorhanden ist – nach dem IFG Gebühren erhoben werden dürfen. Insbesondere ging es dabei um Auskünfte, dass im Baulastenverzeichnis für ein bestimmtes Grundstück keine Baulast ein-

301 Entschließung vom 9. Dezember 2014: Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!, Dokumentenband 2014, S. 149

302 Entschließung vom 9. Dezember 2014: Umfassende und effektive Informationsfreiheitsaufsicht unabdingbar!, Dokumentenband 2014, S. 150

303 Entschließung vom 9. Dezember 2014: Open Data muss in Deutschland Standard werden!, Dokumentenband 2014, S. 151

304 www.transparenz.hamburg.de

getragen ist,[305] sowie um Auskünfte, dass eine bestimmte Angelegenheit nicht überprüft bzw. bewertet wurde.

Zunächst ist die Aktenauskunft nach dem IFG gebührenpflichtig.[306] Eine „Negativauskunft" stellt jedoch keine Auskunft in diesem Sinne dar. Der Antrag auf Aktenauskunft hinsichtlich einer nicht vorhandenen Akte bzw. einer nicht vorhandenen Information ist nämlich bereits als unzulässig abzulehnen, da es am entsprechenden Antragsgegenstand mangelt und der Antrag insoweit „ins Leere" geht. Für die Ablehnung der Aktenauskunft wird dabei abweichend von dem Grundsatz, dass auch für die Ablehnung der Vornahme einer Amtshandlung eine anteilige Gebühr erhoben wird,[307] ausdrücklich keine Gebühr erhoben.[308]

Für die „Negativauskunft", dass eine bestimmte Information nicht vorhanden ist, darf somit nach dem IFG keine Gebühr erhoben werden. Soweit also im Baulastenverzeichnis für ein bestimmtes Grundstück keine Baulast eingetragen ist oder eine bestimmte Angelegenheit nicht geprüft bzw. bewertet wurde, ist die entsprechende Auskunft nicht gebührenpflichtig.

Für dieses Ergebnis sprechen insbesondere auch folgende Erwägungen: Wenn eine derartige „Negativauskunft" gebührenpflichtig wäre, würde es im Einzelfall vom Geschick der Antragstellerin oder des Antragstellers bei der Formulierung des Antrags abhängen, ob die erteilte „Negativauskunft" eine Gebührenfolge auslöst. So würde ein Antrag auf Aktenauskunft, ob für ein bestimmtes – baulastenfreies – Grundstück im Baulastenverzeichnis eine Baulast eingetragen ist, die Auskunft nach sich ziehen, dass keine Baulast eingetragen ist. Diese erteilte „Negativauskunft» wäre folglich als Aktenauskunft nach dem IFG gebührenpflichtig. Demgegenüber wäre ein entsprechender Antrag auf Aktenauskunft, **welche** Baulasten im Baulastenverzeichnis eingetragen sind, als unzulässig abzulehnen, da im Baulastenverzeichnis keine Eintragungen vorhanden sind, die begehrten Informationen folglich nicht vorliegen. Die „Negativauskunft" wäre in diesem Fall also gebührenfrei, obwohl im Ergebnis die gleiche Auskunft erteilt werden würde – nämlich dass keine Baulast eingetragen ist.

305 Siehe auch 2.6 sowie JB 2013, 18.3.3
306 § 16 Satz 1 IFG
307 § 6 Abs. 1 VGebO
308 Siehe Anmerkung zur Tarifstelle 1004 des Gebührenverzeichnisses zur VGebO

Unter Berücksichtigung von Sinn und Zweck des IFG[309] darf es jedoch nicht vom Geschick der Antragstellerin oder des Antragstellers bei der Formulierung des Antrags abhängen, ob die erteilte – im Ergebnis inhaltsgleiche – Auskunft eine Gebührenfolge nach sich zieht. Dies entspricht im Übrigen der Rechtslage nach dem Umweltinformationsgesetz.

„Negativauskünfte" aus Akten sind nicht gebührenpflichtig.

14.3.2 Interne Statistiken zum Bildungsurlaub

Der Verein Bildungswerk der Humanistischen Union in Nordrhein-Westfalen bat die Senatsverwaltung für Arbeit, Integration und Frauen um Berichtszahlen zum Bildungsurlaub im Land Berlin. Die Senatsverwaltung antwortete darauf zunächst, dass es sich um eine interne Statistik handle, die nicht veröffentlicht werde, und gab lediglich die Auskunft, dass ca. 1 % der Berliner versicherungspflichtigen Beschäftigten Bildungsurlaub genommen habe, von denen 60 % Frauen seien. Auf den Hinweis des Vereins, dass keine Ausschlussgründe nach dem IFG einschlägig seien, teilte die Senatsverwaltung mit, dass die statistischen Daten nicht zur Veröffentlichung bestimmt seien und überdies ein Interessenskonflikt bestehe, da der Verein zugleich ein Träger von Bildungsveranstaltungen sei, der gegenüber anderen Trägern der Weiterbildung nicht bevorzugt werden dürfe. Zwar übersandte die Senatsverwaltung ihm zwei Antworten auf Kleine Anfragen, jedoch nicht die begehrten Berichtszahlen. Weitere Nachfragen des Vereins blieben unbeantwortet.

Ausschlussgründe nach dem IFG[310] sind bei rein statistischen Angaben zum Bildungsurlaub nicht einschlägig. Das IFG enthält insbesondere auch keinen Ausschlussgrund für interne Unterlagen. Vielmehr soll das Gesetz – in ausdrücklicher Abkehr vom Prinzip des Amtsgeheimnisses – durch ein umfassendes Informationsrecht das in Akten festgehaltene Wissen und Handeln öffentlicher

309 § 1 IFG
310 §§ 5 bis 12 IFG

Stellen unter Wahrung des Schutzes personenbezogener Daten unmittelbar der Allgemeinheit zugänglich machen, um über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen.[311] Ferner kann der Antrag auf Informationszugang von jedem Menschen sowie von juristischen Personen gestellt werden[312] und es kommt weder auf die Identität des Antragstellers noch auf den beabsichtigten Verwendungszweck an, sodass es auch unerheblich ist, ob der Verein gegenüber anderen Trägern der Weiterbildung – die im Übrigen selbst einen entsprechenden Antrag stellen könnten – bevorzugt würde. Wir wiesen die Senatsverwaltung zudem vorsorglich darauf hin, dass der Verein als gemeinnützig anerkannt und daher von der Gebührenzahlung befreit ist.[313]

Der Verein erhielt letztlich umfangreiche Jahresstatistiken zum Bildungsurlaub in Berlin für den Zeitraum 2009 bis April 2014. Da bestimmte Zahlen wegen laufender Nachmeldungen der Bildungsträger noch nicht vorlagen, wurde dem Verein eine Nachlieferung in Aussicht gestellt. Wegen der Gemeinnützigkeit wurden dem Verein keine Gebühren auferlegt.

Der Informationszugang nach dem IFG darf nicht abgelehnt werden, weil interne Informationen begehrt werden, sondern ist zu gewähren, wenn keine der im IFG – abschließend – geregelten Ausnahmen Anwendung findet.[314] Auch ist es unerheblich, wer den Antrag stellt und wofür die antragstellende Person die Informationen benötigt.

14.3.3 Zugang zu Schulinspektionsberichten

Ein Petent begehrte von der Senatsverwaltung für Bildung, Jugend und Wissenschaft Akteneinsicht in Schulinspektionsberichte. Die Senatsverwaltung teilte ihm mit, dass eine Akteneinsicht in die Berichte, in denen

311 § 1 IFG
312 § 3 Abs. 1 Satz 1 und 2 IFG
313 § 2 Abs. 1 Satz 1 Nr. 4 VGebO
314 § 4 Abs. 1 IFG

> die Schulinspektion jeder einzelnen inspizierten Schule Rückmeldungen zu den Inspektionsergebnissen liefert, nicht möglich sei. Der Akteninhalt beziehe sich auf den Prozess der Willensbildung innerhalb von und zwischen Behörden.[315] Schulinspektionsberichte lieferten Informationen über eine Vielzahl schulischer Gegebenheiten, die unbefangen und ohne die Besorgnis, sich zu blamieren oder blamiert zu werden, erfasst und bewertet würden. Mit einer unbefangenen Mitwirkung der Schulen sei nur dann zu rechnen, wenn die Schulevaluation vertraulich durchgeführt würde. Daher würden die schutzwürdigen Belange der Senatsverwaltung gegenüber dem Informationsinteresse der Bürgerinnen und Bürger überwiegen. Schließlich enthielten die Schulevaluationsberichte Informationen über Stärken und Schwächen der jeweiligen Schulleitungen sowie sonstiger Personengruppen, die als personenbezogene Daten schützenswert seien.[316]

Die Senatsverwaltung hatte den Informationszugang zu den Schulinspektionsberichten im Ergebnis zu Recht abgelehnt, hierfür jedoch nicht die zutreffende Rechtsgrundlage herangezogen.

Das Schulgesetz enthält eine Regelung, wonach die Schulaufsichtsbehörde regelmäßig einen nach Bezirken, Schularten und Bildungsgängen differenzierten Bildungsbericht über den Entwicklungsstand und die Qualität der Schulen veröffentlicht, in dem die Evaluationsergebnisse in angemessener Weise darzustellen sind.[317] Hierdurch wird ein eigenständiger Informationszugang zu den Schulinspektionsberichten im Wege einer Berichtspflicht eröffnet. Diese Berichtspflicht wurde durch die Verordnung über schulische Qualitätssicherung und Evaluation dahingehend konkretisiert,[318] dass einerseits eine Veröffentlichung der konkreten Schulinspektionsberichte nur durch die jeweilige Schule erfolgen darf,[319] andererseits die Schulaufsichtsbehörde nach Vorstellung des Inspektionsberichts der Schulkonferenz lediglich eine Zusammenfassung der wesentlichen Ergebnisse der Schulinspektion in einem Bericht veröffentlichen darf.[320]

315 § 10 Abs. 4 IFG
316 § 6 IFG
317 § 9 Abs. 5 SchulG
318 § 9 Abs. 6 SchulG
319 § 5 Abs. 3 SchulQualSiEvalVO
320 § 5 Abs. 4 SchulQualSiEvalVO

Wir konnten dem Petenten daher nur mitteilen, dass er nach dem IFG keinen Anspruch auf Informationszugang zu den Schulinspektionsberichten hat, da der insoweit speziellere Informationszugang nach dem Schulgesetz Vorrang hat.[321]

Die Anwendbarkeit des IFG ist ausgeschlossen, soweit in Vorschriften des Landes Berlin oder des Bundes speziellere Regelungen für den Informationszugang normiert sind. Die öffentliche Stelle muss daher in jedem Fall prüfen, ob das IFG überhaupt anwendbar ist.

14.3.4 Satzung der Westerwelle Foundation

Ein Journalist bat die Senatsverwaltung für Justiz und Verbraucherschutz um Akteneinsicht in alle dem dortigen Stiftungsregister vorliegenden Unterlagen zur Westerwelle Foundation Stiftung für internationale Verständigung. Daraufhin erhielt er zwar eine Kopie der Satzung, in der jedoch die Angaben über das Stiftungsvermögen geschwärzt waren. Auf Nachfrage erklärte ihm die Senatsverwaltung, dass es sich hierbei um schutzwürdige Betriebs- und Geschäftsgeheimnisse handeln würde.[322]

Nach der höchstrichterlichen Rechtsprechung sind als Betriebs- und Geschäftsgeheimnisse alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge zu verstehen, die nicht offenkundig, sondern nur einem begrenzen Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat.[323] Selbst bei Vorliegen von Betriebs- und Geschäftsgeheimnissen ist jedoch eine Interessenabwägung zwischen dem schutzwürdigen Interesse der Betroffenen an der Geheimhaltung und dem Informationsinteresse der Allgemeinheit vorzunehmen.[324] Wir baten die Senatsverwaltung daher um Stellungnahme, aus welchem Grund das Stiftungsvermögen für schützenswert erachtet wird, und wiesen zudem darauf hin, dass der Vorstand der Stiftung um eine entsprechende Zustimmung ersucht werden könnte.

321 Siehe auch JB 2008, 15.3
322 § 7 IFG
323 BVerfG, Beschluss vom 14. März 2006, 1 BvR 2087/03; BVerwG, Beschluss vom 4. Januar 2005, 6 B 59.04
324 § 7 Satz 1 i. V. m. § 1 IFG

Die Senatsverwaltung gab daher den Vorstandsmitgliedern der Stiftung, bei denen es sich zugleich um die Stifter handelte, Gelegenheit, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern.[325] Diese widersprachen dem Informationszugang, ohne hierfür eine Begründung zu liefern. Daraufhin kam die Senatsverwaltung im Rahmen der Interessenabwägung zum Ergebnis, dass der Offenbarung von personenbezogenen Daten[326] oder Betriebs- und Geschäftsgeheimnissen[327] keine schutzwürdigen Belange der Stiftung oder der Stifter entgegenstehen, und gewährte daher dem Journalisten die begehrte Akteneinsicht in die Stiftungsakte in vollem Umfang.

Die öffentliche Stelle hat zunächst selbst zu bestimmen, ob und inwieweit Aktenbestandteile schützenswerte Betriebs- oder Geschäftsgeheimnisse darstellen. Selbst bei Vorliegen solcher Geheimnisse hat die öffentliche Stelle in jedem Fall eine Abwägung zwischen dem schutzwürdigen Interesse der Betroffenen und dem Informationsinteresse der Allgemeinheit vorzunehmen.

14.3.5 Tauziehen um den Park am Gleisdreieck

Aus der Praxis

Ein Petent bat die Senatsverwaltung für Stadtentwicklung und Umwelt um Akteneinsicht in alle Unterlagen, aus denen sich ergibt, ab wann, mit welchem Zweck, aus welchen Mitteln und mit welchen Kosten die durch den West- und Ostpark des Gleisdreiecks führenden Straßen geplant und angelegt wurden bzw. werden und ob es darüber hinausgehende Planungen gebe. Die Senatsverwaltung teilte ihm daraufhin mit, dass es sich bei dem Park am Gleisdreieck um eine gewidmete Grünanlage handle, was jegliche Straßenplanungen ausschließe, man jedoch davon ausgehe, dass die Parkwege gemeint seien, für die die Grün Berlin Stiftung zuständig sei. Bei der Senatsverwaltung seien zu dem Themenkomplex keine Akten vorhanden.

325 § 14 Abs. 2 Satz 1 IFG
326 § 6 IFG
327 § 7 IFG

Da uns nicht nachvollziehbar schien, dass bei der Senatsverwaltung überhaupt keine Akten vorhanden sein sollen, stellten wir hierzu eigene Nachforschungen an. Diese ergaben, dass die Senatsverwaltung, vertreten durch die Grün Berlin Stiftung, die Bauherrin des Parks am Gleisdreieck ist. Auch stellte sich heraus, dass die Stiftung nach einer Antwort auf eine Kleine Anfrage[328] erst im Dezember 2012 errichtet wurde, der Baubeginn im Ost- und Westpark jedoch bereits im Juni 2008 bzw. August 2010 und die Eröffnung im September 2011 bzw. Mai 2013 erfolgten. Ferner stellte sich heraus, dass der zuständige Staatssekretär sowie eine Mitarbeiterin der Senatsverwaltung dem Aufsichtsrat der Grün Berlin GmbH angehören, die die Grün Berlin Stiftung errichtet hatte, und die Mitarbeiterin sich noch im Februar 2014 in einer Ausschusssitzung zum Thema „Bewirtschaftung im Gleisdreieckpark“ geäußert hatte. Demnach war davon auszugehen, dass bei der Senatsverwaltung zum Park am Gleisdreieck Unterlagen sowohl aus der Zeit vor als auch nach der Errichtung der Grün Berlin Stiftung vorhanden sein müssen.

Wir teilten der Senatsverwaltung unsere Erkenntnisse mit und wiesen darauf hin, dass es sich bei den gegenständlichen Informationen um Umweltinformationen[329] handeln dürfte, deren Einsichtnahme vor Ort gebührenfrei ist.[330]

Hiermit konfrontiert erklärte uns die Senatsverwaltung, dass der Antrag des Petenten nicht abgelehnt worden sei, sondern ihm nach entsprechender Interpretation seines Schreibens lediglich mitgeteilt worden sei, dass er zur Wegeplanung im Park am Gleisdreieck umfängliche Planungsunterlagen bei der Grün Berlin Stiftung erhalten könne. Auch sei der Petent nicht darauf verwiesen worden, dass bei der Senatsverwaltung keine Unterlagen vorlägen. Vielmehr habe ihm ein einfacherer Weg zur Informationserlangung aufgezeigt werden sollen.

Nach nochmaligem Schriftwechsel zwischen dem Petenten und der Senatsverwaltung gewährte sie ihm schließlich gebührenfrei Akteneinsicht.

328 Drs. 17/11785
329 § 18a Abs. 1 IFG i. V. m. § 2 Abs. 3 UIG
330 § 18a Abs. 4 Satz 2 Nr. 1 IFG

Gegenstand des Informationszugangsanspruchs nach dem IFG sind die bei der öffentlichen Stelle vorhandenen Akten[331], sodass ein entsprechender Antrag nicht mit der Begründung abgelehnt werden darf, dass die begehrten Informationen (auch) bei einer anderen Stelle vorhanden sind. Bei Unklarheiten über den Antragsgegenstand hat die öffentliche Stelle die Antragstellerin oder den Antragsteller entsprechend zu beraten und zu unterstützen.[332]

14.3.6 Viel Ärger um die Internationale Gartenbauausstellung

Eine Petentin bat das Bezirksamt Marzahn-Hellersdorf zunächst um Akteneinsicht in die Bebauungspläne für das Gelände „Kienberg, Wuhletal, Jelena-Santic-Friedenspark und Wiesenpark". Hierauf erhielt sie die Auskunft, dass dort zwei Bebauungspläne festgesetzt seien, die sie auf der Internetseite des Stadtentwicklungsamts einsehen könne, und sich zwei Bebauungspläne im Verfahren befänden, sodass den entsprechenden Akten nur sehr wenig zu entnehmen sei.

Daraufhin beantragte die Petentin Akteneinsicht in die entsprechenden Bauanträge für dieses Gelände. Das Bezirksamt teilte ihr mit, dass der Antrag zu allgemein gehalten sei und um Angaben zu den gewünschten Vorgängen, namentlich Straße, Hausnummer und Vorhabenbezeichnung, ergänzt werden müsse. Die Petentin erklärte dem Bezirksamt daraufhin, dass es im Wuhletal keine Straßen und Hausnummern gebe, übersandte jedoch eine Aufstellung der für sie relevanten Flurstücke sowie eine genauere Beschreibung der Begrenzung eines Parks durch verschiedene Straßen. Sie wies darauf hin, dass sie vor erfolgter Akteneinsicht keine Vorhabenbezeichnungen benennen könne, und äußerte Interesse an allen Baumaßnahmen auf dem Gelände. Das Bezirksamt lehnte den Antrag nun vollständig ab und führte zur Begründung aus, dass den Unterlagen nicht zu entnehmen sei, welche Akten die Petentin einsehen wolle, das Recht

331 § 3 Abs. 1 Satz 1 IFG
332 § 13 Abs. 1 Satz 3 IFG

auf Akteneinsicht sich jedoch nur auf Verwaltungsvorgänge beziehe, die unter einer Vorhabenbezeichnung, Straße und Hausnummer geführt werden.

Die Auffassung, das Recht auf Akteneinsicht beziehe sich nur auf Verwaltungsvorgänge, die unter einer Vorhabenbezeichnung, Straße und Hausnummer geführt werden, findet im IFG keine Stütze. Zwar soll im Antrag die betreffende Akte bezeichnet werden.[333] Die Antragstellerin ist jedoch durch die öffentliche Stelle zu beraten und zu unterstützen, wenn ihr Angaben zur hinreichenden Bestimmung einer Akte fehlen.[334] In diesem Zusammenhang wiesen wir das Bezirksamt darauf hin, dass anhand der von der Petentin übersandten Aufstellung sowie der weiteren Beschreibung ohne Weiteres ermittelt werden kann, um welche Vorgänge es sich handelt. Wir regten eine Neubescheidung des Antrags an und wiesen vorsorglich darauf hin, dass es sich bei den begehrten Informationen um Umweltinformationen[335] handelt, deren Einsichtnahme vor Ort gebührenfrei ist.[336]

Das Bezirksamt erklärte uns, dass der Petentin nicht die Akteneinsicht verwehrt werden solle, jedoch aus dem Schriftwechsel nicht hervorgegangen sei, welche Akte zur Verfügung gestellt werden solle. Da aus dem Antrag das eigentliche Begehren der Petentin nicht ersichtlich gewesen sei, sei dieser zurückgewiesen worden. Erst aufgrund unseres Schreibens sei klar geworden, dass die Petentin Akteneinsicht in Bauanträge zur Internationalen Gartenbauausstellung begehre. Das Bezirksamt teilte uns mit, dass dort bislang vier Bauanträge gestellt worden seien, die derzeit in Bearbeitung seien, weswegen Akteneinsicht nur nach dem Verwaltungsverfahrensgesetz des Bundes gewährt werde.[337] Die Petentin sei jedoch keine Beteiligte an diesen Verfahren, weshalb auch einem erneuten Antrag nicht stattgegeben werden würde.

Auch diese Rechtsauffassung des Bezirksamts war unzutreffend. Die Akteneinsicht für Verfahrensbeteiligte ist zum einen nicht nach dem Verwaltungsverfahrensgesetz des Bundes,[338] sondern nach dem Verwaltungsverfahrensgesetz

333 § 13 Abs. 1 Satz 2 IFG
334 § 13 Abs. 1 Satz 3 IFG
335 § 18a Abs. 1 IFG i. V. m. § 2 Abs. 3 UIG
336 § 18a Abs. 4 Satz 2 Nr. 1 IFG
337 § 29 VwVfG
338 § 29 VwVfG

des Landes Berlin[339] zu gewähren. Zum anderen richtet sich die Akteneinsicht bei laufenden Verfahren für Nichtbeteiligte nach dem IFG.[340] Außerdem enthält das IFG keinen Ausschlussgrund, um die Akteneinsicht in laufende Vorgänge pauschal zu verweigern, sondern lediglich im Hinblick auf Entwürfe zu Entscheidungen und Arbeiten zu ihrer unmittelbaren Vorbereitung.[341] Für den Fall, dass die begehrte Akteneinsicht auch weiterhin ohne Prüfung der Ausschlussgründe nach dem IFG abgelehnt werden sollte, drohten wir eine Beanstandung an.[342]

Das Bezirksamt gab nach insgesamt mehr als vier Monaten dem Antrag endlich statt und gewährte gebührenfreie Akteneinsicht in die begehrten Vorgänge.

Öffentliche Stellen dürfen Anträge auf Informationszugang weder pauschal mit der Begründung ablehnen, dass diese zu allgemein gehalten seien, noch zwingend die Angabe von Aktenzeichen, Vorhabenbezeichnungen o. Ä. verlangen. Sofern der antragstellenden Person Angaben zur hinreichenden Bestimmung einer Akte fehlen, hat die Behörde die Person zu beraten und zu unterstützen[343], etwa durch Übersendung einer Aufstellung der in Frage kommenden Akten.

14.3.7 Ungewöhnliche Handhabung des Gesetzes im Bezirksamt Pankow

Aus der Praxis

Eine Petentin bat das Bezirksamt Pankow einerseits um Auskunft, ob eine Baugenehmigung zu einer Grundrissänderung ihrer Wohnung erteilt wurde, andererseits um Akteneinsicht in die zugehörige Bauakte. In dem vereinbarten Termin wurde der Petentin zwar ein Grundriss vorgelegt, von dem sie jedoch keine Kopie erhielt. Darüber hinaus wurde ihr mitgeteilt, dass wegen der Akteneinsicht zunächst der Eigentümer um Erlaubnis gefragt werden müsse.

339 § 1 Abs. 1 i. V. m. § 4a VwVfG Bln
340 § 4a Abs. 4 VwVfG Bln; siehe 2.6
341 § 10 Abs. 1 IFG
342 § 26 BlnDSG
343 § 13 Abs. 1 Satz 3 IFG

Wir erklärten dem Bezirksamt die Rechtslage im Hinblick auf Akteneinsichten in Bauakten[344] und wiesen darauf hin, dass die Einsicht in die Bauakte nicht von der Zustimmung des Eigentümers abhängt. Außerdem sind auf Verlangen grundsätzlich Fotokopien herauszugeben,[345] wenn der Überlassung nicht im Einzelfall Urheberrechte entgegenstehen (was jedoch bei Grundrissen und Planungsunterlagen zu reinen Zweckbauten regelmäßig nicht der Fall ist, da es an der hierfür nach dem Urheberrecht nötigen Schöpfungshöhe mangelt) und der angehörte Betroffene nicht die Zustimmung verweigert.[346] Wir wiesen in diesem Zusammenhang darauf hin, dass selbst bei verweigerter Zustimmung zumindest die Einsichtnahme ermöglicht werden muss.[347]

Das Bezirksamt erklärte daraufhin, man habe den Antrag der Petentin dahingehend verstanden, dass diese nur Akteneinsicht in den Aktenteil bezüglich ihrer eigenen Wohnung begehre. Erst im Akteneinsichtstermin habe die Petentin den Antrag auf die Gesamtakte ausgeweitet, die jedoch nicht zur Einsichtnahme vorbereitet worden sei. Ein Antrag auf Akteneinsicht in die vollständigen Bauantragsunterlagen sei nicht gestellt worden und das Bezirksamt werde ohne neuen Antrag auf Akteneinsicht auch nicht tätig werden.

Wir wiesen das Bezirksamt darauf hin, dass die Petentin jedenfalls während des Termins zur Akteneinsicht vor Ort einen Antrag hinsichtlich der gesamten Bauakte gestellt hat, und erklärten, dass dieser auch mündlich gestellt werden kann[348] und hierüber unverzüglich zu entscheiden ist.[349] Um weitere Verzögerungen bei der Bearbeitung zu vermeiden, empfahlen wir der Petentin gleichwohl, den Antrag vorsorglich noch einmal schriftlich zu stellen.

Auf den neuen schriftlichen Antrag hin erklärte das Bezirksamt der Petentin nunmehr, der **Bauherr** habe wegen der Akteneinsicht in die gesamte Bauakte zunächst um Kontaktaufnahme der Petentin bei ihm gebeten. Die Begründung hierzu erschöpfte sich in dem Hinweis, dass der **Eigentümer** den Schutz von

344 Zu den Einzelheiten siehe 2.6
345 § 13 Abs. 5 Satz 1 IFG
346 § 13 Abs. 5 Satz 2 IFG
347 § 13 Abs. 5 Satz 4 IFG
348 § 13 Abs. 1 Satz 1 IFG
349 § 14 Abs. 1 Satz 1 IFG

Betriebs- und Geschäftsgeheimnissen genieße.[350] Die Petentin wurde zudem gebeten, das Bezirksamt zu informieren, falls eine Einsichtnahme im Bezirksamt weiterhin nötig sei.

Von der Zustimmung des Bauherrn ist die Akteneinsicht aber ebenso wenig abhängig wie von der des Eigentümers. Bei der Prüfung von Betriebs- oder Geschäftsgeheimnissen[351] ist eine Anhörung der Betroffenen nur dann erforderlich ist, wenn die Behörde tatsächlich beabsichtigt, schutzwürdige Betriebs- oder Geschäftsgeheimnisse zu offenbaren.[352] Außerdem trifft in keinem Fall die Petentin die Pflicht, sich wegen des Umfangs der Akteneinsicht, wegen des Ersuchens um Zustimmung zur Offenbarung von Betriebs- oder Geschäftsgeheimnissen oder aus sonstigen Gründen mit den Betroffenen in Verbindung zu setzen. Dies ist vielmehr Sache der Behörde. Wir forderten das Bezirksamt daher auf, nunmehr unverzüglich[353] unter Beachtung dieser Ausführungen über den Antrag der Petentin zu entscheiden. Nach weiterer längerer Korrespondenz und nach mehr als einem halben Jahr ist der Petentin ein Termin zur Akteneinsicht angeboten worden.

Der Informationszugang nach dem IFG ist einerseits nicht von der Zustimmung der Betroffenen abhängig, andererseits ist eine im Einzelfall erforderliche Anhörung Betroffener von der öffentlichen Stelle vorzunehmen, nicht von der Antragstellerin oder dem Antragsteller. Im Übrigen lässt der vom Bezirksamt an den Tag gelegte Umgang mit dem IFG nur den Schluss zu, dass dort ein erheblicher Fortbildungsbedarf besteht.[354]

350 § 7 IFG
351 Zu den Einzelheiten siehe 14.3.4
352 § 14 Abs. 2 Satz 1 IFG
353 § 14 Abs. 1 Satz 1 IFG
354 Siehe 14.4 sowie JB 2013, 18.3.1

14.4 Fortbildungen an der Verwaltungsakademie und bei öffentlichen Stellen

Wegen des weiterhin großen Interesses setzten wir unsere im letzten Jahr begonnene Fortbildungsreihe[355] zum IFG bei der Verwaltungsakademie (VAk) Berlin fort. Durch die konstruktiven Hinweise der Teilnehmenden konnte die Fortbildung dabei fortlaufend verbessert und noch zielgerichteter auf die praktischen Bedürfnisse der Anwenderinnen und Anwender zugeschnitten werden.

Auf Wunsch des Landesverwaltungsamts boten wir zudem erstmals eine In-House-Fortbildung für die dortige Leitungsebene an. Zum einen wurden die Grundlagen des IFG inklusive der wichtigsten Ausschlussgründe und Verfahrensvorschriften dargestellt, zum anderen wurden die vorab vom Landesverwaltungsamt mitgeteilten Fragen und Anwendungsprobleme praxisnah beantwortet. Das Landesverwaltungsamt hat daher bereits Interesse an zukünftigen In-House-Fortbildungen für Mitarbeiterinnen und Mitarbeiter bekundet, die mit der Bearbeitung von Anträgen nach dem IFG befasst sind.

Für die Zukunft sind daher auch weiterhin Fortbildungen bei der VAk Berlin sowie bei entsprechendem Bedarf auch vor Ort bei öffentlichen Stellen geplant.

355 JB 2013, 18.3.1

15 Wo wir den Menschen sonst noch helfen konnten ...

Einem Petenten wurde von einem Vollstreckungsbeamten des Finanzamtes ein **Termin zur Vollstreckung** zugestellt. Auf dem Umschlag befand sich ein großer **roter Aufkleber**, der dem Petenten androhte, dass die Haustür gewaltsam und kostenpflichtig geöffnet wird, wenn er zum angekündigten Termin nicht angetroffen wird. Durch den ungewöhnlichen roten Aufkleber war für jeden Dritten – wie z. B. Nachbarn – sofort zu erkennen, dass gegen den Petenten Vollstreckungsmaßnahmen liefen. Nach den Verfahrensvorschriften ist dieser Hinweis gemeinsam mit der letzten Zahlungsaufforderung und der Terminankündigung verschlossen zu hinterlassen,[356] um zu vermeiden, dass Dritte hiervon Kenntnis erlangen. Dies gilt auch dann, wenn er für den Schuldner als optisch hervorgehobene Warnung vor einer finanziellen Belastung dienen soll. Wir konnten erreichen, dass die **Senatsverwaltung für Finanzen** bei den Finanzämtern die Einhaltung der Verfahrensvorschriften anmahnte und der Aufkleber künftig nicht mehr auf den Umschlag geklebt wird.

Ein Bürger teilte uns mit, dass ein **Finanzamt** im Jahr 2008 eine Pfändungs- und Einziehungsverfügung gegen einen anderen, namensgleichen Steuerschuldner erlassen habe, die jedoch an seinen Arbeitgeber gegangen sei. Die Angelegenheit konnte mit dem Finanzamt geklärt werden. Umso verärgerter war der Bürger, dass seine Konten bei der Sparkasse gesperrt wurden, nachdem ein anderes Finanzamt im Jahr 2013 eine weitere Pfändungs- und Einziehungsverfügung gegen den namensgleichen Steuerschuldner erlassen hatte. Auf Nachfrage wurde dem Bürger vom Finanzamt mitgeteilt, dass bei der Kontodatenrecherche zur Person des Steuerpflichtigen nur nach Name und Geburtsdatum gesucht worden sei. Dies habe zu der für den Bürger nachteiligen **Verwechslung** geführt. Wir konnten erreichen, dass ein dauerhafter Sichtvermerk zu den Steuerakten des Bürgers genommen wurde, der auf die wiederholten Personenverwechslungen hinweist. Zusätzlich wurde dem Finanzamt aufgegeben, sich bei zukünftigen Vollstreckungsmaßnahmen in diesem Fall anhand von zusätzlichen Daten wie Geburtsort und Anschrift und ggf. weiterer Ermittlun-

356 Abschnitt 29 Abs. 1 VollzA

gen über die Identität des Vollstreckungsschuldners zu versichern. Es ist davon auszugehen, dass damit eine erneute Personenverwechslung ausgeschlossen ist.

Wir erhielten wieder mehrere Beschwerden, dass **Personalausweiskopien in Arztpraxen** angefertigt werden.[357] Wir haben die betreffenden Ärzte darauf hingewiesen, dass sowohl das Anfertigen von Personalausweiskopien als auch die Ablage in der Patientenakte unzulässig ist. Zu Abrechnungszwecken und zur Kontrolle der Identität des Patienten genügt die Vorlage des Personalausweises. Die Arztpraxen sind unserer Aufforderung gefolgt, die vorhandenen Personalausweiskopien zu vernichten und zukünftig auf das Anfertigen solcher Kopien zu verzichten. Auf diese Weise konnten wir den Petenten zu ihrem Recht auf Löschung der unzulässig gespeicherten Personalausweiskopien verhelfen.

Ein Bürger wies uns darauf hin, dass ihm durch einen Irrtum der Post eine Postkarte, die von einer Arztpraxis an eine Patientin gerichtet war, zugestellt worden sei. Auf der Rückseite der **Postkarte** sei die Patientin aufgefordert worden, der Praxis mitzuteilen, wie sie sich in Bezug auf den neuen Zahnersatz entschieden habe, und einen neuen Termin zwecks Weiterbehandlung zu vereinbaren. Hierbei handelte es sich um **Patientendaten**, die der ärztlichen Schweigepflicht unterliegen. Bei einem Versand dieser Daten per Postkarte besteht die Gefahr, dass Unbefugte diese Patientendaten lesen. Wir konnten erreichen, dass die Arztpraxis zukünftig Terminerinnerungen sowie behandlungsrelevante Nachfragen in einem verschlossenen Umschlag an ihre Patienten versendet.

Ein Bürger bat um Unterstützung, da er unmittelbar nach einer Übernachtung in einem **Schlaflabor** ein schriftliches **Angebot eines Anbieters medizinischer Hilfsmittel** erhalten habe, ohne vorher Kontakt zu seinem Arzt gehabt zu haben und bevor ihm die ärztliche Verordnung zuging. Die Übermittlung seiner Kontaktdaten sowie der Kopie der ärztlichen Verordnung an das Sanitätshaus ist ohne sein Wissen und ohne Einwilligung erfolgt. Das verantwortliche Schlaflabor räumte den Datenschutzverstoß ein und versicherte, dass aufgrund interner Vorgaben Einverständniserklärungen der Patienten für die Übermittlung dieser Daten an einen Leistungserbringer eingeholt würden und es sich um einen Einzelfall gehandelt habe. Aufgrund unserer Intervention hat das

357 Siehe schon JB 2013, 8.7

Schlaflabor für die Löschung der in diesem Zusammenhang übermittelten Daten bei dem Hilfsmittelvertrieb gesorgt. Auch wurden alle Beschäftigten des Schlaflabors von der Geschäftsführung noch einmal darauf hingewiesen, dass vor der Versendung von Patientendaten oder einer Verordnung überprüft werden muss, ob eine unterschriebene Einverständniserklärung des Patienten zur Übermittlung der für seine Versorgung notwendigen Daten an einen Hilfsmittelerbringer vorliegt.

Eine Bürgerin beschwerte sich darüber, dass ein **Jugendamt** ihre Sozialdaten an einen freien Träger der Jugendhilfe weitergegeben habe, um ihr Unterstützung bei der **Vaterschaftsfeststellung** und der Geltendmachung von Unterhaltsansprüchen anbieten zu können. Eine Einwilligung hatte das Jugendamt hierfür nicht eingeholt. Es stellte sich heraus, dass die Übertragung der Aufgabe an den freien Träger und damit auch die Datenübermittlung rechtmäßig war. Allerdings konnten wir erreichen, dass die Betroffenen künftig darüber aufgeklärt werden, warum ihre Daten an den freien Träger weitergegeben werden.

Aufgrund unserer Bemühungen gibt das Sozialamt Friedrichshain-Kreuzberg bei **Bescheinigungen über den Bezug von Sozialhilfe** die Höhe der gewährten Sozialleistung nicht mehr an. Solche Bescheinigungen sind z. B. bei der gesetzlichen Krankenkasse vorzulegen. Die Bescheinigung wird nur auf ausdrücklichen Wunsch der oder des Betroffenen mit dem Betrag versehen.

Wir haben erreicht, dass das **Sozialamt Lichtenberg** einen Vordruck, der bislang bei einem Erstantrag auf Hilfe zur Überwindung besonderer sozialer Schwierigkeiten ausgefüllt werden musste, nicht mehr verwendet. Der Vordruck sah eine **Entbindung von der Schweigepflicht** für die Mitarbeiterinnen und Mitarbeiter der Fachstelle Wohnungssicherung und Wohnungsversorgung sowie für die beteiligten Stellen und Einzelpersonen vor. Weitere konkretisierende Informationen, etwa zur Notwendigkeit einer Schweigepflichtentbindung, enthielt der Vordruck nicht. Das Sozialamt hat uns mitgeteilt, dass der Vordruck angesichts des Verfahrensablaufes gar nicht benötigt werde.

Ein ehemaliger **Trainer eines Fußballvereins** beschwerte sich darüber, dass das ihm gegenüber ausgesprochene **Platzverbot** in einem für eine Vielzahl von Personen zugänglichen Schaukasten ausgehängt worden ist. Wir haben dem Verein mitgeteilt, dass ein Platzverbot lediglich denjenigen bekannt zu

geben ist, die auch mit der Durchsetzung betraut sind, und ihn aufgefordert, den Aushang zu entfernen.

Eine Petentin begehrte von der **Senatsverwaltung für Stadtentwicklung und Umwelt** Einsicht in alle Unterlagen zu einer **Pilotanlage im Osthafen** und konnte daraufhin die zugehörige wasserrechtliche Zulassungsakte einsehen. Auf Nachfrage teilte die Senatsverwaltung ihr zunächst mit, dass darüber hinaus keine Unterlagen zu der Pilotanlage vorhanden seien. Die Petentin teilte uns aber mit, dass sie über verlässliche Informationen verfüge, dass die Senatsverwaltung ihr nicht alle vorhandenen Unterlagen vorgelegt habe, und schickte uns ein in dieser Angelegenheit an sie gerichtetes Schreiben des zuständigen Staatssekretärs. Dieses Schreiben übersandten wir der Senatsverwaltung mit der Bitte um Prüfung, welche weiteren Unterlagen der Petentin zur Verfügung gestellt werden können. Kurz darauf erhielt die Petentin von der Senatsverwaltung die Mitteilung, dass sie die übrigen vorhandenen Unterlagen einsehen könne.

Eine Petentin begehrte von der **Ärztekammer** verschiedene **Auskünfte zu Anzeigen** ihres Vaters gegen sie behandelnde Ärzte, da sie wegen entsprechender Anzeigen in der Vergangenheit bereits mehrfach ihren Arzt habe wechseln müssen. Die Ärztekammer lehnte die Auskunft aus datenschutzrechtlichen Gründen ab.[358] Wir teilten der Ärztekammer mit, dass die Petentin jedenfalls einen Anspruch auf die Auskunft hat, ob und weswegen ihr Vater einen bestimmten Arzt angezeigt hat sowie ob er darüber hinaus noch weitere Ärzte angezeigt hat, da der Offenbarung dieser Angaben in der Regel keine schutzwürdigen Belange der Betroffenen entgegenstehen.[359] Die Ärztekammer blieb zwar bei ihrer Auffassung, teilte der Petentin aber mit, dass Daten über Beschwerdeverfahren nach fünf Jahren gelöscht werden, wenn diese nicht mehr benötigt werden, und ihr Vater jedenfalls seitdem keine Beschwerden gegen irgendwelche Ärzte erhoben hat.

Der Verein Bundesverband für freie Kammern bat die **Psychotherapeutenkammer Berlin** um Auskunft über die Gesamteinnahmen, die Gesamtausgaben, die Zuführung zu den Rücklagen sowie die Entnahme aus den Rücklagen im Jahr 2012 sowie die Höhe der gesamten Rücklagen, des gesamten Vermö-

358 § 5a BlnKAG
359 § 6 Abs. 2 Satz 1 Nr. 1 a) und b) IFG

gens sowie die Anzahl der Mitglieder zum 31. Dezember 2012. Die Psychotherapeutenkammer erklärte daraufhin, dass dies kein Akteneinsichtsgesuch im Sinne des IFG sei. Vielmehr würden Einzelauskünfte erbeten, für deren Beantwortung es im Kammergesetz Berlin keine Rechtsgrundlage gebe. Wir teilten der Psychotherapeutenkammer mit, dass sie als Körperschaft des öffentlichen Rechts dem IFG unterliegt[360] und danach ein **Anspruch auf Auskunft** über den Inhalt der von der öffentlichen Stelle geführten Akten besteht, der auch **von juristischen Personen** geltend gemacht werden kann.[361] Die Psychotherapeutenkammer erteilte dem Verein daraufhin die gewünschte Auskunft.

360 § 2 Abs. 1 Satz 1 IFG
361 § 3 Abs. 1 Satz 1 und 2 IFG

16 Aus der Dienststelle

16.1 Entwicklungen

Seit 2005 hat sich die Zahl der Eingaben sowohl im Bereich Datenschutz als auch in der Informationsfreiheit deutlich erhöht. Zugleich hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit seine Prüftätigkeit von Amts wegen erheblich ausgeweitet, was zur verstärkten Verhängung von Bußgeldern und Anordnungen nach § 38 Bundesdatenschutzgesetz geführt hat. Die begrenzten personellen Ressourcen der Dienststelle führen allerdings dazu, dass solche Prüfungen gegenwärtig nicht im erforderlichen Umfang durchgeführt werden können und die Beantwortung der Fragen von Petenten, Abgeordneten sowie öffentlichen und privaten Datenverarbeitern immer mehr Zeit in Anspruch nimmt.

16.2 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Zu begrüßen ist, dass der zu Beginn der 17. Legislaturperiode neu geschaffene Ausschuss „Digitale Verwaltung, Datenschutz und Informationsfreiheit" nun zugunsten von mehr Transparenz die Sitzungen per Audio-Live-Stream ins Internet überträgt, sofern keine beteiligte Person dem widerspricht. Hierauf wird mit der Einladung hingewiesen. Eindeutig weniger Transparenz bietet jedoch das im Vergleich zum Vorgängerausschuss[362] geänderte Ausschussverfahren. Dort war es üblich, dass bei der Behandlung der Stellungnahmen des Senats zu den Jahresberichten die Beschlussvorschläge des Berliner Beauftragten für Datenschutz und Informationsfreiheit für mögliche Beschlüsse des Abgeordnetenhauses in die Ausschussprotokolle aufgenommen wurden. Auch die Art und Weise, wie der Unterausschuss damit umging – nämlich ob sie abgelehnt oder modifiziert oder gänzlich übernommen wurden –, wurde in der

362 Unterausschuss „Datenschutz und Informationsfreiheit" des Ausschusses für Inneres, Sicherheit und Ordnung im Abgeordnetenhaus von Berlin

Sitzung entschieden und war deshalb in den Protokollen nachlesbar. Dies war in dem neuen Ausschuss zunächst nicht mehr der Fall, weil die konkreten Vorschläge des Berliner Beauftragten für Datenschutz und Informationsfreiheit für Außenstehende nicht anhand der Protokolle nachvollzogen werden konnten. Stattdessen entscheiden die Sprecher der Fraktionen außerhalb der Sitzungen, wie sie mit den Vorschlägen des Berliner Beauftragten umgehen. Diese werden nun lediglich den Beschlussprotokollen als Anlage beigefügt.

16.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 27./28. März und am 8./9. Oktober in Hamburg unter dem Vorsitz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[363] Für 2015 hat der Hessische Datenschutzbeauftragte den Vorsitz in der Konferenz übernommen.

Der **Düsseldorfer Kreis**, in dem unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit die **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich** zusammenarbeiten, fasste Entschließungen zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt werden, sowie zur Unzulässigkeit von Dashcams und zur Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“.[364]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 17. Juni und am 9. Dezember ebenfalls in Hamburg unter dem Vorsitz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und fasste mehrere Entschließungen zu aktuellen Fragen des Informationszugangs und der Transparenz.[365] 2015 wird der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern den Vorsitz in dieser Konferenz übernehmen.

363 Dokumentenband 2014, S. 9 ff.
364 Dokumentenband 2014, S. 38 ff.
365 Dokumentenband 2014, S. 147 ff.

Die **Arbeitsgruppe nach Artikel 29 der Europäischen Datenschutzrichtlinie**, in der Berlin traditionell die Bundesländer vertritt, wird seit Beginn des Berichtszeitraums von der Präsidentin der französischen Datenschutzkommission geleitet. Die Arbeitsgruppe, die nach dem Entwurf für eine Europäische Datenschutz-Grundverordnung nach deren Inkrafttreten die Aufgaben des Europäischen Datenschutzausschusses übernehmen wird, beschloss drei ausführliche Stellungnahmen zu den Konsequenzen aus den Veröffentlichungen über die exzessiven Überwachungsmaßnahmen von Geheimdiensten sowie Stellungnahmen zu den wegweisenden Entscheidungen des Europäischen Gerichtshofs zur Vorratsdatenspeicherung und zum „Recht auf Vergessen". Darüber hinaus hat die Gruppe Stellungnahmen zu zentralen Regelungen der geltenden Datenschutzrichtlinie, zu Anonymisierungstechniken und zu praktischen Fragen des grenzüberschreitenden Datenverkehrs beschlossen, die zum Teil in unserem Dokumentenband abgedruckt sind.[366]

Auf Einladung der Datenschutzbeauftragten von Mauritius fand die **36. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre** vom 13.-16. Oktober statt, die sich mit zentralen Fragen des Datenschutzes in der globalen Informationsgesellschaft befasste. Die Konferenz äußerte sich in einer Entschließung zu den notwendigen Konsequenzen aus der entgrenzten Überwachung durch Geheimdienste.[367] Außerdem griff die Konferenz in einer weiteren Entschließung das Thema „Big Data" auf, das bereits die **Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group")** bei ihrer Sitzung in Skopje am 5./6. Mai zum Gegenstand eines Arbeitspapiers gemacht hatte. Diese Arbeitsgruppe tagte erneut am 14./15. Oktober in Berlin und verabschiedete ein weiteres Arbeitspapier zu den Datenschutzrisiken des Einsatzes privater Endgeräte in Unternehmensnetzen.[368]

Auf Einladung der schottischen Beauftragten für die Informationsfreiheit tagte am **5. November die 4. Europäische Konferenz der Informationsfreiheitsbeauftragten** in Edinburgh. Dabei wurden Möglichkeiten zur Intensivierung der Zusammenarbeit auf europäischer Ebene diskutiert. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat im Auftrag seiner euro-

366 Dokumentenband 2014, S. 55 ff.
367 Dokumentenband 2014, S. 109 ff.
368 Dokumentenband 2014, S. 117 ff.

päischen Kollegen die Europäische Kommission gebeten, den Aufbau einer geschützten Webplattform für die Mitglieder dieser Konferenz zu fördern, zu der auch zahlreiche osteuropäische Länder gehören, die den Beitritt zur Europäischen Union anstreben.

Das vom Europäischen Datenschutzbeauftragten ins Leben gerufene **Internet Privacy Engineering Network (IPEN)** veranstaltete am 26. September im Abgeordnetenhaus einen Workshop, den wir inhaltlich und organisatorisch mitgestaltet haben. IPEN bringt Teilnehmer aus Datenschutzbehörden, Hochschulen, der Open Source Community, der industriellen Software-Entwicklung sowie Einzelpersonen zusammen, die sich für technische Lösungen von Problemen des Datenschutzes einsetzen.[369]

Am 8. Dezember fand im Rahmen der **UNESCO** eine von der französischen Datenschutzkommission vorbereitete Konferenz statt, bei der europäische und internationale Experten, darunter auch ein Mitglied des Ausschusses für Verfassungsschutz des Abgeordnetenhauses und der Berliner Beauftragte für Datenschutz und Informationsfreiheit, über den Schutz der Privatsphäre im Zeitalter globaler Überwachung und terroristischer Bedrohung diskutierten. Die Konferenz wurde vom französischen Premierminister mit einer Rede eröffnet.

Erneut erhielten wir Besuch von mehreren ausländischen Delegationen, die sich in unserer Dienststelle über praktische Fragen der Datenschutzkontrolle und des Informationszugangs informierten. Dazu gehörten zwei Delegationen aus der Volksrepublik China, ein Vertreter der Datenschutzbeauftragten der Ukraine, eine Vertreterin des nationalen Zentrums für Datenschutz der Republik Moldau und zwei Hochschullehrerinnen aus der Türkei.

16.4 Öffentlichkeitsarbeit

Am 28. Januar fand auf Einladung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema „Big Data für Bond 2.0 – Für eine menschenrechtliche Einhegung der Nachrichtendienste in Zeiten von Big

369 Hintergrundinformationen unter https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/IPEN

Data“ eine zentrale Veranstaltung im Abgeordnetenhaus aus Anlass des 8. Europäischen Datenschutztages statt.

Am 17. Mai nahmen wir am gemeinsamen „Tag der offenen Tür“ des Abgeordnetenhauses und des Bundesrates teil und präsentierten dort einen Informationsstand.

Am 5. November wurde im FEZ Berlin ein Schülerfachforum für Medienkompetenz „Check your Web“ durchgeführt. Wir gestalteten an diesem Projekttag den Workshop „Das Datenschutzbrettspiel“ und stellten zusätzlich einen Infostand zur Verfügung. Mit einem im Rahmen eines Projektes an der Verwaltungsakademie entwickelten Brettspiel „Datenschutzhelden. Nimm dich in Acht vor den Spionen!“ wurden die Schülerinnen und Schüler spielerisch mit dem Thema Datenschutz vertraut und auf den vorsichtigen Umgang mit persönlichen Daten aufmerksam gemacht.

Die sechswöchige Veranstaltung der Zentral- und Landesbibliothek, der Themenraum „Gesellschaft unter Beobachtung?“, die am 9. Dezember in der Zentral- und Landesbibliothek begann, haben wir als einer der Kooperationspartner mit unseren Publikationen unterstützt.

Außerdem bieten wir im Rahmen der Vorlesungsreihe der KinderUni Lichtenberg (KUL) und der mobilen Lichtenberger KinderUni „KUL *unterwegs*“ regelmäßige Vorlesungen zum Thema „Soziale Netzwerke und Datenschutz“ für Kinder ab acht Jahren an.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat schließlich wie in den vorangegangenen Jahren am Oberstufenzentrum Handel I mit Schülerinnen und Schülern über aktuelle Fragen des Datenschutzes diskutiert. An dieser Schule macht der Lehrer Thomas Lingens datenschutzrechtliche Themen immer wieder in vorbildlicher Weise zum Gegenstand seines Unterrichts.

Berlin, den 25. März 2015

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Anhang

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 2. Oktober 2014 im Abgeordnetenhaus von Berlin zum Jahresbericht 2013

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren,

Sie befassen sich heute mit dem Jahresbericht 2013 des Berliner Beauftragten für Datenschutz und Informationsfreiheit und der Stellungnahme des Senats hierzu.

Die Einzelheiten des Berichts werden im Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit zu beraten sein, der im zurückliegenden Jahr sehr konstruktiv die anstehenden Themen diskutiert hat. Dafür danke ich dem Ausschuss und insbesondere seinem Vorsitzenden, dem Abgeordneten Fabio Reinhardt. Allerdings würde ich mir wünschen, dass die Positionen, auf die sich der Ausschuss verständigt, als Beschlussempfehlungen schneller das Plenum erreichen. In diesem Zusammenhang begrüße ich es, dass das Abgeordnetenhaus einen Beschluss zum **Schutz der Vertraulichkeit des Inhalts elektronischer Kommunikation mit öffentlichen Stellen** gefasst hat.

Dieses Thema zieht sich auch durch den aktuellen Jahresbericht des Datenschutzbeauftragten. In Zeiten wachsender Unsicherheit und Verletzlichkeit von Kommunikationsinfrastrukturen ist es von zentraler Bedeutung, dass Berlin seinen Bürgerinnen und Bürgern vertrauenswürdige Mitteilungswege anbietet und diese auch für die Kommunikation zwischen Behörden nutzt. Ende-zu-Ende-Verschlüsselung muss zum Standard werden. Die vom Bundesgesetzgeber vorgesehene und teilweise vorgeschriebene De-Mail bietet zwar mehr Vertraulichkeit als die unverschlüsselte Kommunikation. Die De-Mail ist allerdings ungeeignet für die Übermittlung von Gesundheits- und anderen vergleichbar sensitiven Daten. Verschlüsselung reicht aber nicht aus, um den zunehmenden Angriffe durch Kriminelle, aber auch Nachrichtendienste auf

die Datenverarbeitung des Landes Berlin zu begegnen. Dabei geht es um die generelle **Erhöhung der Widerstandsfähigkeit (Resilienz) der IT-Systeme** gegen flächendeckende Attacken, die in Zukunft mit Sicherheit noch zunehmen werden. Zur Resignation besteht dabei kein Anlass. Wir befinden uns in einem Wettlauf. Um ein Wort von Bertolt Brecht abzuwandeln: Wer an diesem Wettlauf teilnimmt, kann verlieren. Wer nicht teilnimmt, hat schon verloren.

Es gibt durchaus auch positive Entwicklungen: Mehrere große US-Unternehmen aus der IT-Branche haben angekündigt, Rechenzentren nach Europa zu verlagern, um das Vertrauen der europäischen Kunden zurückzugewinnen. Ob dies gelingen kann, ist noch offen. Umso wichtiger ist es aber, dass Berliner Schulen nicht **Cloud-Dienste** amerikanischer Unternehmen nutzen, die dazu führen, dass die Daten von Berliner Schülern, Eltern und Lehrern auf Servern in den USA liegen, wo der Datenschutz nicht den nötigen Stellenwert hat.

Erst in der vergangenen Woche hat in diesem Haus ein Workshop von Experten des vom Europäischen Datenschutzbeauftragten ins Leben gerufenen **Netzwerks für technische Internet-Sicherheit (IPEN)** stattgefunden. Dieses Netzwerk erarbeitet Handlungsanweisungen, wie die Entwickler von Hard- und Software, aber auch Start-up-Gründer den Datenschutz möglichst früh in ihre Überlegungen einbeziehen können. Das ist für die lebendige Berliner Start-up-Szene von erheblicher Bedeutung, die ohnehin ihre Geschäftsmodelle an europäischen Maßstäben von Datenschutz und Transparenz ausrichten muss, um wirtschaftlich Erfolg zu haben. Dabei geht es um mehr als Datensicherheit: Es geht auch um **datensparsame Geschäftsideen** als Alternativen zu den großen US-Unternehmen, deren invasive Werbestrategien zunehmend als übergriffig empfunden werden.

Meine Damen und Herren,

Berlin hat sowohl national als auch international einen guten Namen in Sachen Datenschutz. In Sachen **Informationsfreiheit** besteht noch ein gewisser Nachholbedarf, selbst wenn Berlin bereits 1999 als zweites Bundesland in Deutschland ein Informationsfreiheitsgesetz verabschiedet hat. Auch hier geht die Entwicklung allerdings weiter, wie das Beispiel des Hamburger Transparenzgesetzes zeigt. Seit gestern ist das Hamburger **Transparenzportal** online, in das

die meisten Dokumente der dortigen Verwaltung für jedermann sichtbar bei gleichzeitiger Beachtung des Datenschutzes eingestellt werden. Das sollte für die Bundeshauptstadt das maßgebliche Beispiel sein.

Herzlichen Dank für Ihre Aufmerksamkeit!

Stichwortverzeichnis

A

B

C

D

E

F

G

I

J

K / L

M

N

O

P

R

S

T

U

V

W

Y

Z

Veröffentlichungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte:
Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über seine Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Der Tätigkeitsbericht wird von uns auch als Broschüre für die Bürgerinnen und Bürger veröffentlicht.

Dokumente zu Datenschutz und Informationsfreiheit:
Diese Schriftenreihe erscheint jährlich als Anlage zu unserem Tätigkeitsbericht. Sie enthält die bedeutsamen Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen des genannten Jahres.

Berliner Informationsgesetzbuch (BlnInfGB):
In dieser Textsammlung werden von uns die wichtigsten Regelungen zum Datenschutz und zur Informationsfreiheit für das Land Berlin herausgegeben.

Ratgeber und Faltblätter zum Datenschutz:
In diesen Publikationen haben wir praktische Informationen zu einzelnen Fragen im Alltag zusammengestellt. Damit wollen wir die Menschen in die Lage versetzen, ihre Datenschutzrechte bzw. ihr Recht auf Informationszugang eigenständig wahrzunehmen.

Welche Broschüren wir im Einzelnen veröffentlicht haben, können Sie einer Übersicht auf unserer Website www.datenschutz-berlin.de entnehmen. Den überwiegenden Teil unserer Broschüren haben wir dort für Sie auch zum Download bereitgestellt. Eine Bestellung per Post ist gegen Einsendung eines an Sie selbst adressierten und mit 1,00 Euro frankierten DIN-A5-Umschlages möglich.

www.datenschutz-berlin.de

E-Government • Zentrales Service-Konto Berlin • Konsequenzen aus dem anhaltenden NSA-Skandal? • Entwicklungen beim Cloud Computing – das Beispiel Office 365 • Gemeinsame Terrorabwehrzentren • Schutz von Mandatsgeheimnissen in Ermittlungsverfahren gegen Abgeordnete • Online-Lernplattformen • Informationszugang bei der Bauaufsicht – Prüfung von Amts wegen • Stadtweite Veranstaltungsdatenbank • Elektronisches Doping beim Schach • Fahndung bei Facebook • Übergabe des Sprachlerntagebuchs an Schulen • Online-Einwilligung in SCHUFA-Erklärung • Scoring-Urteil des Bundesgerichtshofs: Gesetzgeber ist gefordert • Keine Werbeanrufe unter dem Deckmantel von Zufriedenheitsabfragen • Gibt es ein Recht auf Vergessen? • Diebstahl von Laptops im Zahnärztlichen Dienst • Schutz der Privatsphäre bei SmartTV • Real World Tracking • Gebühren für Negativauskünfte?