Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Datenschutz und Informationsfreiheit

Bericht 2013

Berlin

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2013

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 **27. März 2013** vorgelegten Jahresbericht 2012 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2013 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2013“) 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.de

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Inhalt

Einleitung

Im November 2006 fand die Internationale Konferenz der Datenschutzbeauftragten in London unter dem Motto „Überwachungsgesellschaften“ statt. Der britische Informationsbeauftragte Richard Thomas beschrieb aus diesem Anlass die Gefahr, dass nicht nur seine Landsleute sich „schlafwandelnd“ auf dem Weg in eine Überwachungsgesellschaft befänden. Wie zutreffend diese Prognose war, ist spätestens mit den von Edward Snowden im Juni veranlassten Veröffentlichungen über die exzessiven Überwachungspraktiken der US-amerikanischen und britischen Geheimdienste offenkundig geworden.

Dass das Internet eine unsichere Infrastruktur ist, war schon vor den Snowden-Veröffentlichungen vielen Menschen klar. Unbekannt war dagegen, dass es systematisch als Plattform für eine weltweite, anlasslose Überwachung genutzt wird und dass darüber hinaus Geheimdienste auch demokratischer Staaten, die jedes Maß verloren haben, die gesamte Telekommunikation jederzeit beobachten. Das Erschreckende an diesem Befund ist nicht, dass die NSA und andere Geheimdienste gezielt Spionage betreiben und z.B. die Mobiltelefone der Bundeskanzlerin und ihres Amtsvorgängers abhören. „Zutiefst verstörend“ – wie es der ehemalige Präsident des Bundesnachrichtendienstes und des Bundesamtes für Verfassungsschutz, Hansjörg Geiger, formuliert hat – ist vielmehr die Totalität des Überwachungsanspruchs, die sich auch in Begriffen wie „Full Take“ oder „Mastering the Internet“ ausdrückt. Die National Security Agency (NSA) und das britische Government Communications Headquarter (GCHQ) sind nicht nur außer Kontrolle, es gibt Hinweise darauf, dass jedenfalls die NSA auch die Kontrolle über ihre eigenen Datenverarbeitungssysteme verloren hat. Sie haben durch den Einbau von Schwachstellen in die Infrastruktur die weltweite Informationssicherheit beschädigt, weil auch Kriminelle diese Schwachstellen nutzen können.

Welche Folgen die Snowden-Veröffentlichungen letztlich haben werden, ist noch nicht ganz abzusehen. Eines ist aber jetzt schon klar: Der Vertrauensverlust gegenüber staatlichen Institutionen, privaten Diensteanbietern, insbesondere amerikanischer Provenienz, aber auch gegenüber dem Internet insgesamt ist massiv. Eine weltweite Plattform, die lange Zeit als Erweiterung der indi-

viduellen Kommunikations- und Informationsfreiheit verstanden wurde, ist offenbar schon seit längerem zugleich zu einer weltweiten Überwachungsplattform geworden.

Obwohl der Bundespräsident bezogen auf Deutschland davor gewarnt hat, unser Land dürfe nicht zu einem „schlafwandelnden Riesen“ werden[1] – was auf das Thema der Londoner Konferenz von 2006 zurückverweist –, sind die Konsequenzen, die die Bundesregierung bisher aus dem NSA-Skandal gezogen hat, im Wesentlichen verbaler Natur. Die Bundeskanzlerin und der Bundesinnenminister haben das Vorgehen der US-Behörden kritisiert. Ob das praktische Folgen haben wird, ist fraglich.

Immerhin hat die Vollversammlung der Vereinten Nationen am 18. Dezember – also fast genau 30 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts – auch auf deutsche Initiative hin eine Resolution verabschiedet, die den weltweiten Schutz der Privatsphäre auch im digitalen Zeitalter einfordert.[2] Zwar ist diese Resolution rechtlich nicht bindend, das Thema wird aber auf der Tagesordnung der UNO bleiben und – so ist zu hoffen – in nicht allzu ferner Zukunft zu einer völkerrechtlich verbindlichen Konvention über den Schutz der Privatsphäre führen. Eine solche Konvention fordern die Datenschutzbeauftragten weltweit bereits seit Jahren. Der Weg zu einer internationalen Vereinbarung ist sicherlich lang, aber es ist wichtig, dass der erste Schritt getan wurde. Datenschutz war schon vor der Aufdeckung des Überwachungsexzesses der NSA und ihrer Kooperationspartner nicht nur ein nationales Thema. Jetzt ist endgültig klar: Der Datenschutz muss international garantiert werden.

Neben politischen und rechtlichen Maßnahmen zur Begrenzung und besseren Kontrolle der Überwachungspraktiken von Nachrichtendiensten und mit ihnen kooperierenden Wirtschaftsunternehmen muss jetzt verstärkt über technische Möglichkeiten des Selbstschutzes nicht nur diskutiert werden, sie müssen auch zum Einsatz kommen. Die Vertraulichkeit technisch vermittelter Kommunikation ist die entscheidende Voraussetzung dafür, dass Telekommunikationsdienste überhaupt noch unbefangen und angstfrei genutzt werden können. Es gibt zu denken, dass der Bundespräsident als „gelernter DDR-Bürger“ über Verwandte und Freunde berichtet, die „anfangen, sich am Telefon ähnlich zu verhalten, wie wir das früher in der DDR getan haben.“[3] Diesem „Chilling Effect“, dem Gefühl des Beobachtetwerdens, muss auch mit technischen Mitteln begegnet werden. Verschlüsselung bietet zwar keine absolute Sicherheit gegen die Ausspähung durch Nachrichtendienste, sie ist durch deren Aktivitäten aber keineswegs entwertet. Verschlüsselung ist vielmehr auch nach dem Berliner Datenschutzgesetz eine wesentliche Anforderung an den technischen Datenschutz. Dieser Anforderung genügen zwar zahlreiche Verfahren der Berliner Verwaltung, allerdings keineswegs alle. Hier besteht noch erheblicher Nachholbedarf. Denn es steht der Verwaltung nicht frei, Verschlüsselungsdienste zu nutzen oder dies zu unterlassen, sobald sie personenbezogene Daten verarbeitet.[4] Verschlüsselung ist nicht nur Pflicht, sie ist auch unverzichtbar. Darauf weisen wir anhand von drei konkreten Beispielen in diesem Bericht hin.[5] Eine Behörde oder ein Diensteanbieter kann nicht mit der Begründung unverschlüsselt Daten online erheben oder übermitteln, der Bürger oder Kunde habe auf die Verschlüsselung verzichtet. Der Schutz personenbezogener Daten vor unbefugter Kenntnisnahme durch technische Verfahren, die nach heutigem Kenntnisstand ausreichend sicher sind, gehört zum unabdingbaren Mindeststandard. Allerdings müssen den Menschen einfacher zu handhabende Werkzeuge des Selbstschutzes an die Hand gegeben werden, als sie bisher verfügbar sind. Hier sind der Staat, die Unternehmen und die Entwickler und Hersteller von Hard- und Software gefordert. Schon jetzt berichten deutsche Hersteller von Sicherheitssoftware über eine steigende Nachfrage als Konsequenz aus dem Überwachungsskandal.

Exzessive und aggressive Überwachung ist nur möglich unter exzessiver Geheimhaltung. Das hat die Internationale Konferenz der Informationsfreiheitsbeauftragten bei ihrer 8. Sitzung im September in Berlin[6] zu einer „Berliner Erklärung“ veranlasst, in der sie die Anwendbarkeit der Informationsfreiheitsgesetze auch auf die Nachrichtendienste betont.[7] Deren Kontrolle durch parlamentarische Gremien und Gerichte muss weltweit wie auch in Deutsch-

1 Rede zum Tag der Deutschen Einheit, siehe Frankfurter Allgemeine Zeitung vom 4. Oktober 2013
2 Dokumentenband 2013, S. 151
3 Interview mit der Frankfurter Allgemeinen Zeitung vom 24. Januar 2014
4 Siehe 1.1
5 Siehe 6.2, 12.1.3 und 14.2
6 Siehe 18.1
7 „Transparenz – der Treibstoff der Demokratie“, siehe Dokumentenband 2013, S. 198

land verbessert und wirksamer gestaltet werden. Aber allein die von Edward Snowden veröffentlichten Dokumente haben dazu beigetragen, dass sowohl in Europa als auch in den USA eine Debatte darüber begonnen hat, ob Geheimdienste bei der Sammlung von Informationen Grenzen unterliegen sollten und wie diese zu definieren sind. Schon das ist ein Fortschritt gegenüber der seit dem 11. September 2001 ins Uferlose gewachsenen heimlichen Überwachung der weltweiten Kommunikation.

In Sachen Informationsfreiheit tritt Europa im Übrigen auf der Stelle. Nachdem die Europäische Kommission schon 2008 einen Entwurf zur Novellierung der Verordnung über den Informationszugang bei EU-Institutionen vorgelegt hatte, der allerdings zu einer Absenkung des Transparenzniveaus geführt hätte, ist kein Fortschritt mehr erkennbar. Das Europäische Parlament hat sich für eine Verbesserung der Transparenz eingesetzt und in einer Entschließung vom 12. Juni die Blockadehaltung der Kommission und der Mehrheit der Mitgliedsstaaten scharf kritisiert, ohne dass dies zu Bewegung in den festgefahrenen Positionen geführt hätte. In Deutschland besteht immerhin die Hoffnung, dass in Baden-Württemberg und Niedersachsen Informationsfreiheitsgesetze verabschiedet und „die weißen Flecke“ auf der deutschen Transparenz-Landkarte weniger werden.

1 Digitale Verwaltung

1.1 Sicherheit im Berliner Landesnetz

Die weltweite Gefährdung der Informationssicherheit ist nicht völlig neu.[8] Allerdings hat sie durch die Enthüllungen über die Aktivitäten der NSA und anderer Geheimdienste eine neue, bedrohliche Qualität erhalten. Behörden werden wie Wirtschaftsunternehmen von diversen Angreifern immer massiver attackiert. In einem Interview gab der Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Michael Hange, an, dass es täglich 2.000 bis 3.000 Angriffe auf den Regierungsinformationsverbund Bonn-Berlin gibt, wobei ca. zehn Angriffe Sabotagecharakter aufweisen.[9] Das IT-Dienstleistungszentrum Berlin (ITDZ) registrierte 2012 ungefähr 1,1 Millionen Hacker-Attacken. Das ist jeder zehnte aus dem Internet kommende Kommunikationsversuch. Diese Zahlen untermauern eindrucksvoll, wie notwendig die Absicherung der öffentlichen Verwaltung ist. Ein wichtiger Aspekt der Sicherheit von Informationen ist die Verschlüsselung bei ihrer Übertragung. Verschlüsselung garantiert keine absolute Sicherheit vor Ausspähung und unbefugten Zugriffen Dritter. Aber sie ist nach wie vor ein essenzielles Mittel zur gebotenen Erhöhung der Datensicherheit. Vor diesem Hintergrund sollen im Folgenden die Rahmenbedingungen für die Sicherheit im Berliner Landesnetz umrissen werden.

Netzwerke

Das ITDZ bietet der öffentlichen Verwaltung des Landes Berlin IT-Dienstleistungen an, zu denen auch eine Netzinfrastruktur gehört. Dafür betreibt das ITDZ folgende Netze:

- Berliner Landesnetz Multi Service Network (BeLa MSN): Transportnetz für Daten- und Sprachübertragung

8 JB 2011, 1.2.2
9 FAZ vom 22. November 2013, S. 33

- Grenznetz:
  Zentraler Übergang vom Berliner Landesnetz in Fremdnetze, z.B. das Internet.[10] Hier befindet sich die sog. demilitarisierte Zone (DMZ), in der z.B. Webserver der Verwaltung platziert sind, die einen Zugriff aus dem Internet ermöglichen. Ein Durchgriff auf das eigentliche Berliner Landesnetz wird jedoch verhindert.
- Datacenter Local Area Network (DC-LAN):
  Netzwerk des High-Secure Data-Center (HSDC) für Anwendungen mit hohem Schutzbedarf. Auf dieses Netz kann nur aus dem Berliner Landesnetz heraus zugegriffen werden, eine direkte Verbindung zum Grenznetz besteht nicht.
- Kundennetze:
  Diese Netzwerke sind die lokalen Netzwerke einzelner Verwaltungen, die vom ITDZ erstellt und betrieben werden. Sie sind mit dem Berliner Landesnetz verbunden, über das sie via Grenznetz den Zugriff auf das Internet ermöglichen.

Für Verwaltungen, die keinen unmittelbaren Zugang zum Berliner Landesnetz haben, bietet das ITDZ spezielle Anbindungsmöglichkeiten an:

- BeLa Zugang DSL:
  Über einen DSL-Anschluss erfolgt eine gesicherte Verbindung zum Grenznetz, über das sowohl das BeLa MSN als auch das Internet erreicht werden können.
- Festverbindungen:
  Die Festverbindungen werden genutzt, wenn die Bandbreite des BeLa Zugangs DSL zu gering ist. Sie haben die gleiche Funktionalität wie das Netz BeLa Zugang DSL.

Verwaltungen, die nur einen Zugang zum Internet benötigen, können Berlin DSL nutzen. Dies ist ein Standard-DSL-Zugang zum Internet. Der Datenverkehr läuft nicht über das Grenznetz. Für die mobile Sprachkommunikation und den mobilen Zugang zum Landesnetz hat das ITDZ ebenfalls Angebote.

10 Fremdnetze sind alle IT-Netzstrukturen außerhalb des Geltungsbereiches der IT-Sicherheitsgrundsätze des Landes Berlin.

Die Verwaltungen sind nicht verpflichtet, die Netzwerkdienste des ITDZ zu nutzen. Wenn sie einen direkten Zugang zu Fremdnetzen und zudem einen Zugang zum BeLa MSN haben, sind sie zu ausreichenden Sicherheitsmaßnahmen verpflichtet. Diese müssen durch ein **behördenspezifisches IT-Sicherheitskonzept** gewährleistet werden.[11] Sonst drohen die vom ITDZ getroffenen Sicherheitsmaßnahmen unterlaufen zu werden.

BeLa MSN, DC-LAN, Grenznetz und Kundennetze werden vollständig vom ITDZ betrieben. Es wird dabei von Dienstleistern unterstützt. Für die Festverbindungen und die DSL-Angebote greift das ITDZ auf Infrastrukturen der Unternehmen Deutsche Telekom AG und Versatel Deutschland GmbH zurück. Die Angebote für mobile Sprach- und Datenkommunikation basieren zusätzlich auf der Infrastruktur der deutschen Vodafone GmbH.

Verschlüsselung

Die Sprachübertragung im BeLa MSN erfolgt verschlüsselt. Wird das Telefonieangebot des ITDZ (IPCentrex) genutzt, ist die Kommunikation bis zum Endgerät verschlüsselt. Endet die Zulieferung der Sprachkommunikation an einer Telefonanlage der Verwaltung, so liegt die weitere Verschlüsselung in deren Ermessen.

Es gibt keine generelle Verschlüsselung der Datenübertragung im Berliner Landesnetz, sondern nur für Teilmengen der Kommunikation. Das ITDZ verschlüsselt nur die Kommunikation zwischen denjenigen Behörden, die den Verschlüsselungsdienst in Auftrag geben und bezahlen. Eine Verschlüsselung kann sowohl verfahrensintern als auch auf Netzwerkebene realisiert werden. Es gibt bereits zahlreiche Verfahren, die eine Verschlüsselung nutzen (z.B. Integrierte Personalverwaltung IPV, ProFISKAL). Der Standardnetzzugang zum Berliner Landesnetz bietet die Möglichkeit, für ausgewählte Ziele die Kommunikation generell zu verschlüsseln. Auch wenn das Berliner Landesnetz durch das Grenznetz und andere technisch-organisatorische Maßnahmen vom Internet und anderen Fremdnetzen abgeschirmt wird, müssen alle Berliner Behörden, die personenbezogene Daten im BeLa MSN übermitteln, Verschlüsselung einsetzen. Dies gilt natürlich erst recht bei der Nutzung des offenen Internets.

11 Siehe dazu 1.5

Das ITDZ bietet Möglichkeiten für sichere Kommunikation an. Diese müssen aber auch genutzt werden. Die von jeder öffentlichen Verwaltung anzufertigenden IT-Sicherheitskonzepte zeigen die jeweilige Notwendigkeit für eine sichere Verschlüsselung auf und müssen umgesetzt werden.

1.2 De-Mail als Patentrezept?

Schon 2012 hatten wir über De-Mail und die damit einhergehenden Probleme berichtet.[12] Insbesondere die dort bereits angesprochene fehlende Ende-zu-Ende-Verschlüsselung stellt auch weiterhin ein massives Problem dar.

Wenn eine Finanzbehörde Daten übermittelt, die dem Steuergeheimnis unterliegen, sind diese Daten mit einem geeigneten Verfahren zu verschlüsseln.[13] Die reine Transportverschlüsselung bei De-Mail stellt jedoch gerade kein geeignetes Verfahren dar, da die De-Mail-Nachricht bei beiden beteiligten De-Mail-Diensteanbietern automatisiert zur Kontrolle auf Schadsoftware entschlüsselt[14] und dadurch eine Kenntnisnahme des Inhalts der De-Mail-Nachricht ermöglicht wird. Um diesen Widerspruch aufzulösen, hat der Gesetzgeber zwischenzeitlich eine eigenwillige Lösung gefunden. So wurde die Abgabenordnung durch eine Regelung ergänzt, wonach die kurzzeitige automatisierte Entschlüsselung, die beim Versenden einer De-Mail-Nachricht durch den akkreditierten Diensteanbieter zur Überprüfung auf Schadsoftware und Weiterleitung an den Adressaten der De-Mail-Nachricht erfolgt, nicht gegen das Verschlüsselungsgebot verstößt.[15] Ferner sieht das Gesetz jetzt vor, dass dem Steuergeheimnis unterliegende Daten nicht unbefugt offenbart werden, wenn beim Versenden über De-Mail eine kurzzeitige automatisierte Entschlüsselung durch den akkreditierten Diensteanbieter zur Überprüfung auf Schadsoftware und Weiterleitung an den Adressaten der De-Mail-Nachricht stattfindet.[16] Dies erstaunt umso mehr, als der Gesetzgeber noch in der Begründung zum De-Mail-Gesetz

12 JB 2012, 1.1
13 § 87a Abs. 1 Satz 3 AO
14 § 3 Abs. 4 Nr. 4 De-Mail-Gesetz
15 § 87a Abs. 1 Satz 4 AO
16 § 30 Abs. 7 AO

eine Übermittlung von dem Steuergeheimnis unterliegenden Daten per De-Mail von der Behörde zum Steuerpflichtigen unter Berufung auf die fehlende Ende-zu-Ende-Verschlüsselung kategorisch ausgeschlossen hatte.[17]

Soweit es die Übermittlung von Sozialdaten betrifft, sind geeignete technisch-organisatorische Maßnahmen zu treffen, um zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[18] Eine Maßnahme in diesem Sinne ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.[19] Den Widerspruch zur fehlenden Ende-zu-Ende-Verschlüsselung bei De-Mail hat der Gesetzgeber zwischenzeitlich auf noch kreativere Weise gelöst: Es wurde kurzerhand eine Regelung in das Sozialgesetzbuch aufgenommen, wonach das Senden von Sozialdaten durch eine De-Mail-Nachricht an die jeweiligen De-Mail-Diensteanbieter zur kurzfristigen automatisierten Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zur Weiterleitung an den Adressaten der De-Mail-Nachricht schon kein Übermitteln darstellt.[20]

Es ist daher zu befürchten, dass der Gesetzgeber auch in anderen Fällen der Versendung besonders schutzbedürftiger Daten per De-Mail entsprechende Ausnahmen aufnehmen und dadurch die gesetzlich vorgeschriebenen Standards weiter aufweichen wird. De-Mail kann jedoch dem Anspruch, die Vertraulichkeit, Integrität und Authentizität der Nachrichten zu gewährleisten,[21] nur dann gerecht werden, wenn die Kommunikation generell durch eine Ende-zu-Ende-Verschlüsselung geschützt wird.

Gesundheits-, Sozial- und Steuerdaten sollten elektronisch nur mit Ende-zu-Ende-Verschlüsselung übermittelt werden.

17 BT-Drs. 17/3630, zu § 5 Abs. 3 De-Mail-Gesetz
18 § 78a Satz 1 SGB X i.V. m. Satz 2 Nr. 4 der Anlage zu § 78a SGB X
19 Satz 3 der Anlage zu § 78a SGB X
20 § 67 Abs. 6 Nr. 3 SGB X
21 § 5 Abs. 3 Satz 1 De-Mail-Gesetz

1.3 Nutzung der eID-Funktion des Personalausweises

Ein Personalausweisinhaber, der mindestens 16 Jahre alt ist, kann die eID-Funktion des neuen Personalausweises nutzen, also diesen dazu verwenden, seine Identität gegenüber öffentlichen und nicht-öffentlichen Stellen elektronisch nachzuweisen.[22] Neben Angaben über die Gültigkeit des Personalausweises können dabei u. a. Familien-, Geburts- und Vornamen, Doktorgrad, Anschrift, Tag und Ort der Geburt sowie die Angabe, ob ein bestimmtes Alter über- oder unterschritten wird oder ob ein Wohnort dem abgefragten Wohnort entspricht, übermittelt werden.[23]

Die Daten werden dabei nur übermittelt, wenn der Diensteanbieter[24] ein gültiges Berechtigungszertifikat[25] an den Personalausweisinhaber schickt und dieser in der Folge seine Geheimnummer eingibt.[26] Damit nachvollziehbar bleibt, welche Daten im Einzelnen an wen übermittelt werden, müssen dem Personalausweisinhaber, bevor er seine Geheimnummer eingibt, die Angaben zu Name, Anschrift und E-Mail-Adresse des Diensteanbieters, Kategorien der zu übermittelnden Daten, Zweck der Übermittlung, Hinweis auf die für den Diensteanbieter zuständige Datenschutzbehörde sowie letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats angezeigt werden.[27] Daneben ist die Übermittlung auf die im Berechtigungszertifikat genannten Datenkategorien beschränkt, wobei der Personalausweisinhaber die Übermittlung auch dieser Datenkategorien im Einzelfall ausschließen kann.[28] Berechtigungszertifikate in diesem Sinne sind elektronische Bescheinigungen, mit denen der berechtigte Diensteanbieter seine Identität dem Personalausweisinhaber nachweisen und die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis veranlassen kann.[29]

22 § 18 Abs. 1 Satz 1 PAuswG
23 § 18 Abs. 3 PAuswG
24 § 2 Abs. 3 PAuswG
25 § 2 Abs. 4 PAuswG
26 § 18 Abs. 4 Satz 1 PAuswG
27 § 18 Abs. 4 Satz 2 PAuswG
28 § 18 Abs. 5 PAuswG
29 § 2 Abs. 4 PAuswG

Für das Land Berlin ist geplant, ein **Bürgerkonto** als zentralen Identifizierungsdienst für die eID-Funktion des neuen Personalausweises einzurichten, das die Identifizierung für die jeweiligen Fachverfahren übernimmt, um so den Bürgerinnen und Bürgern die sichere elektronische Kommunikation mit der Verwaltung zu erleichtern. Hierbei besteht grundsätzlich die Möglichkeit, entweder ein temporäres oder ein permanentes Bürgerkonto einzurichten. Bei einem temporären Bürgerkonto werden die Daten des Personalausweisinhabers nur für die Dauer des Identifizierungsvorgangs gespeichert und nach Übermittlung an das Fachverfahren verworfen. Bei einem permanenten Bürgerkonto werden die Daten auch nach Abschluss des Identifizierungsvorgangs vorgehalten. Da das Bürgerkonto in diesem Fall durch ein weiteres Sicherheitsmerkmal wie etwa ein Passwort geschützt ist, ist auch ein Zugriff ohne den neuen Personalausweis möglich. In diesem Fall weisen die an das Fachverfahren übermittelten Daten jedoch einen geringeren Beweiswert auf, da gerade keine sichere Identifikation durch die eID-Funktion des neuen Personalausweises erfolgt.

Beim Einsatz eines Bürgerkontos verfügt nur dessen Betreiber über ein eigenes Berechtigungszertifikat, nicht jedoch die jeweiligen Fachverfahren. Das Bundesverwaltungsamt hat als Vergabestelle für Berechtigungszertifikate[30] klargestellt, dass für die Anerkennung als Diensteanbieter neben den gesetzlich normierten Voraussetzungen[31] in jedem Fall eine eigene datenschutzrechtliche Verantwortlichkeit des Diensteanbieters erforderlich ist. Daher kann anderen Stellen die Eigenschaft als Diensteanbieter nicht im Wege der Auftragsdatenverarbeitung verliehen werden, da der Auftragnehmer gerade keine eigene datenschutzrechtliche Verantwortung innehat, sondern diese vielmehr beim Auftraggeber verbleibt. In anderen Bundesländern wurde dieses Problem teilweise dadurch gelöst, dass der Identifizierungsdienst als gemeinsames Verfahren eingerichtet wird, bei dem alle beteiligten Stellen, also sowohl der Diensteanbieter als auch die jeweiligen Fachverfahren, selbst datenschutzrechtlich verantwortlich bleiben. Wir haben aus diesem Grund einen Vorschlag für eine Regelung über gemeinsame Verfahren zur Aufnahme in das Berliner Datenschutzgesetz erarbeitet.[32]

30 § 7 Abs. 4 PAuswG
31 § 2 Abs. 3 PAuswG
32 Siehe hierzu 1.7

Die Nutzung der elektronischen Identifizierungsfunktion des Personalausweises würde durch das geplante Bürgerkonto erleichtert. Einzelheiten bedürfen hier allerdings noch einer – auch gesetzlichen – Klärung.

1.4 EU-Verordnung über elektronische Identifizierung und Vertrauensdienste[33]

Die Europäische Kommission will durch eine Verordnung grenzüberschreitende und sichere elektronische Transaktionen in Europa ermöglichen. Sie soll dafür sorgen, dass Personen und Unternehmen mit ihren eigenen nationalen elektronischen Identifizierungssystemen (eID-Systemen) öffentliche Dienste in anderen EU-Ländern benutzen können. Außerdem soll ein Binnenmarkt für die grenzüberschreitende Verwendung elektronischer Signaturen und anderer Vertrauensdienste geschaffen werden.

Der gravierendste Mangel des Entwurfs ist das Fehlen eines Vertrauensdienstes, der die Vertraulichkeit der Kommunikation für E-Mail oder im Internet unterstützt. Das ist für die Wahrung der Privatsphäre und des Rechts auf informationelle Selbstbestimmung ein wesentlicher Punkt, der europaweit einheitlich geregelt werden sollte. Den Menschen und Unternehmen sollten einfach zu bedienende Verschlüsselungsverfahren zur Verfügung gestellt werden.

Viele europäische Länder verfügen bereits über ein eigenes eID-System. In Deutschland ist dieses auf dem neuen Personalausweis integriert und datenschutzgerecht ausgestaltet.[34] Dieses Verfahren erlaubt die gezielte Übermittlung erforderlicher Identitätsdaten über das Internet an den Diensteanbieter nach vorheriger Zustimmung des Betroffenen durch Freischaltung der entsprechenden Datenfelder. Auch können Betroffene sich bei einem Diensteanbieter unter einem Pseudonym identifizieren. Der Verordnungsentwurf der Kommission weist demgegenüber erhebliche Schwachpunkte bezüglich der eID auf. Es fehlt z.B. eine Regelung zum Datenschutz, in der für diesen Bereich Datenvermeidung, Datensparsamkeit und Pseudonymfunktionen verankert sind. Die deutsche Lösung könnte hier Vorbild sein.

33 COM(2012) 238 final
34 Siehe 1.3

Der Verordnungsentwurf definiert verschiedene elektronische Vertrauensdienste wie z.B. Signatur, Siegel, Zeitstempel, Dokumente, Zustelldienst und Website-Authentifizierung, die von qualifizierten Vertrauensdiensteanbietern angeboten werden, die für ihre jeweilige Tätigkeit zertifiziert sein müssen. Es sind positive Ansätze erkennbar, jedoch besteht auch hier noch Verbesserungsbedarf. So ersetzt der entsprechende Abschnitt der Verordnung die bisherige EU-Signaturrichtlinie,[35] sodass auch das deutsche Signaturgesetz bei Verabschiedung der Verordnung außer Kraft treten würde. Positiv ist lediglich die verbindliche Prüfung qualifizierter elektronischer Signaturen (QES) im Zeitpunkt der Erstellung. Dieses entspricht der Gültigkeit der manuellen Unterschrift ab dem Zeitpunkt der Unterzeichnung. Warum dies nicht auch für fortgeschrittene Signaturen festgelegt wird, ist unverständlich.

Der Kommissionsentwurf für eine Verordnung über elektronische Identifizierung und Vertrauensdienste ist nicht akzeptabel. Der europäische Gesetzgeber sollte sicherstellen, dass das in Deutschland geltende datenschutzgerechte Verfahren der elektronischen Identifizierung auch künftig europaweit genutzt werden kann.

1.5 Kontrolle von Sicherheitskonzepten

Bezirkliche IT-Sicherheitskonzepte

War die Sicherung der IT-Infrastruktur schon immer ein wichtiges Thema, so trifft dies für Gegenwart und Zukunft umso mehr zu.[36] Ein wichtiges Instrument ist der Betrieb eines Managementsystems für Informationssicherheit (Information Security Management System – ISMS),[37] um systematisch in einem ständigen Verbesserungsprozess die Sicherheit zu gewährleisten.

35 EU-Signaturrichtlinie 1999/93/EG
36 Siehe 1.1
37 BSI-Standard 100-1

Ein zentrales Element eines ISMS ist das IT-Sicherheitskonzept, das durch seine ständige Aktualisierung an geänderte Bedrohungen angepasst wird. In so einem Konzept werden der Ist-Zustand der IT-Infrastruktur und ihrer Sicherheit dem Soll-Zustand gegenübergestellt und etwaige Lücken planmäßig geschlossen. Dafür werden u. a. Risiken erhoben und Maßnahmen ermittelt, den Risiken adäquat zu begegnen. Der Senat hat dies erkannt und dazu bereits 2007 IT-Sicherheitsgrundsätze festgelegt.[38] Ihr Ziel ist, für die eingesetzten IT-Systeme und -Anwendungen einschließlich der baulichen und gebäudebezogenen Komponenten ein Sicherheitsniveau zu erreichen, das den sicheren Einsatz der Informationstechnik in der Berliner Verwaltung gewährleistet. Die Grundsätze sind von den am IT-Einsatz Beteiligten durch entsprechende Sicherheitskonzepte umzusetzen. In den IT-Sicherheitsgrundsätzen wird für jede Sicherheitsdomäne ein aktueller Grundschutz nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gefordert, wobei bei hohem bis sehr hohem Schutzbedarf eine ergänzende Risikoanalyse nach BSI Standard 100-3 durchzuführen ist. Für den normalen Schutzbedarf kann ein vereinfachtes Modellsicherheitskonzept genutzt werden.[39]

Die Berliner Verwaltung betreibt vielfältige Verfahren, um ihre Aufgaben erfüllen zu können. Um die Sicherheit dieser Verfahren zu gewährleisten, ist für jedes Verfahren ein **spezifisches Sicherheitskonzept** zu erstellen. Damit die zugrunde liegende IT-Infrastruktur nicht wiederholt einbezogen werden muss, ist für diese ein **behördliches IT-Sicherheitskonzept** erforderlich. Dieses bildet die IT-Sicherheitsbasis für alle weiteren Anwendungen und hat damit eine zentrale Bedeutung. Es ist nach den IT-Sicherheitsgrundsätzen Voraussetzung für die Nutzung der landeseinheitlichen IT-Infrastruktur, des Berliner Landesnetzes.

Bereits 2011 wurden Statistiken zu den behördlichen IT-Sicherheitskonzepten ausgewertet und ein deutliches Verbesserungspotenzial festgestellt.[40] Aufgrund ihrer Bedeutung werden IT-Sicherheitskonzepte der Berliner Verwaltung sukzessive von uns überprüft. Begonnen haben wir 2013 mit den Bezirksämtern.

38 Grundsätze zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsgrundsätze), vom Senat beschlossen am 11. Dezember 2007

39 „Modellhaftes IT-Sicherheitskonzept für die Behörden der Berliner Verwaltung“

40 JB 2011, 1.2.2

Bisherige Erkenntnisse

Ende 2012 haben wir die Bezirksämter darüber informiert, dass 2013 eine Prüfung der behördlichen IT-Sicherheitskonzepte beabsichtigt ist. Im März wurden alle Bezirksämter um Übersendung ihrer behördlichen IT-Sicherheitskonzepte gebeten. Bis Ende November sind fünf der zwölf Bezirksämter dieser Bitte nachgekommen. Mehr als die Hälfte aller Bezirksämter konnte also binnen eines Jahres kein (aktuelles) IT-Sicherheitskonzept übermitteln. Dabei wurde noch nicht berücksichtigt, ob die übermittelten IT-Sicherheitskonzepte den Anforderungen genügen. Einige Bezirke haben die Erstellung eines behördlichen Sicherheitskonzeptes erst in Auftrag gegeben.

Die Senatsverwaltung für Inneres und Sport erstellt jährlich den Bericht zur Informationssicherheit. In diesem werden Zulieferungen der Berliner Verwaltung in Form einer Abfrage berücksichtigt. Abgefragt werden u. a. das Vorhandensein eines IT-Sicherheitskonzepts, die Aktualität, die Fertigstellung einer neuen Fassung und die Maßnahmenumsetzung. Allein die Betrachtung der Zulieferungen zu den Berichten der Jahre 2011 und 2012 liefert erhellende Ergebnisse. Nur drei Bezirksämter, die unserer Bitte um Zusendung nicht nachkamen, gaben an, kein IT-Sicherheitskonzept zu haben. Ferner finden sich Angaben, dass die Konzepte „zurzeit erarbeitet“ werden, in einigen Fällen gekoppelt mit avisierten Terminen in 2012. Ein (aktuelles) Konzept ist 2013 jedoch trotzdem nicht vorhanden. Eine weitere Durchsicht ergibt, dass in einigen Bezirksämtern zum Teil keine Schulungen zur IT-Sicherheit durchgeführt werden (acht Bezirksämter), dass kein IT-Sicherheitsbeauftragter bestellt wurde (drei Bezirksämter), dass der Sicherheitsprozess nicht oder nur unvollständig implementiert ist (zehn Bezirksämter) und dass es an Ressourcen mangelt (neun Bezirksämter). Dies ist nur eine kleine Auswahl der gemeldeten Defizite.

Einige Bezirksämter nehmen die Sicherheit von Informationen ernst und versuchen auch in Zeiten knapper Mittel diese zu gewährleisten. Andere Bezirksämter haben weiterhin einen deutlichen Verbesserungsbedarf. Es wäre sinnvoll, wenn der Senat nicht nur einen Bericht zur Informationssicherheit erstellen, sondern auch die Umsetzung der Forderungen aus den IT-Sicherheitsgrundsätzen regelmäßig überprüfen würde. Dazu gehört die Prüfung der IT-Sicherheitskonzepte, zumal die Existenz eines behördlichen Sicherheitskonzeptes Grundlage für den Anschluss der Behörde an das Berliner Landesnetz ist.

Die Aktualität und der Umsetzungsgrad der IT-Sicherheitskonzepte könnte durch den Einsatz von speziellen Grundschutzanwendungen unterstützt und verbessert werden. Eine solche Anwendung ist z.B. das GSTool des BSI, dass unmittelbaren Bundes-, Landes- und Kommunalverwaltungen kostenlos zur Verfügung gestellt wird. Nachdem die komplette Neuentwicklung der nächsten Version dieser Anwendung gescheitert ist, unterstützt das BSI die aktuelle Version nach der gegenwärtigen Planung nur noch für einen kurzen Zeitraum. Weitere Unterstützung danach wird voraussichtlich kostenpflichtig vom Hersteller bezogen werden müssen. Wie beim 3. IT-Grundschutztag 2013 des BSI ebenfalls vorgetragen wurde, zieht dieses in Betracht, die am Markt befindliche Software zu evaluieren und mit dem Hersteller des Produkts der Wahl einen Rahmenvertrag zu schließen, der dann nur noch für die Bundesverwaltung gilt. Bei der problematischen Haushaltslage vieler Kommunen und insbesondere des Landes Berlin wird dies dem Einsatz von Grundschutzanwendungen abträglich sein. In Zeiten von diversen Initiativen zur IT-Sicherheit auf der bundespolitischen Ebene ist ein solches Vorgehen unverständlich und kontraproduktiv. Die Einbeziehung der Länder und Kommunen in den Rahmenvertrag für ein neues GSTool sollte deshalb ermöglicht werden. Der IT-Grundschutz soll in seiner Basis ebenfalls überarbeitet werden. Dies darf aber nicht zu einer Schwächung des bisherigen Vorgehens führen.

Bäder-Betriebe

2012 hatten wir berichtet, dass uns mehrere Eingaben des Personalrats der Berliner Bäder-Betriebe (BBB) zu einer Kontrolle veranlasst haben.[41] Bereits die für die Prüfungsvorbereitung vorgelegten Dokumente waren ausnahmslos unvollständig, widersprüchlich und in den meisten Fällen inaktuell. Wir hatten die BBB aufgefordert, die festgestellten Mängel umgehend und nachhaltig beheben zu lassen. Hierzu wurde vereinbart, dass uns in regelmäßigen Abständen Zwischenberichte zur Verfügung gestellt werden.

Allerdings kam es bei der Abarbeitung der Mängel immer wieder zu Verzögerungen, da die Zusendung der Zwischenberichte der BBB nur sehr zögerlich erfolgte. Erst nach Androhung einer Beanstandung[42] wurde nach über einem Dreivierteljahr ein weiterer Zwischenbericht übergeben. Die zuletzt übermittelten Dokumente zeigten jedoch, dass weiterhin viele Unzulänglichkeiten vorhanden sind. So wird im Informationssicherheitsleitfaden auf noch fehlende (z.B. Bedrohungsanalyse), in Planung (z.B. IT-Notfallvorsorge), in Bearbeitung (z.B. IT-Security Policy) oder in Überarbeitung (z.B. Berechtigungskonzept SAP R/3) befindliche wichtige Dokumente verwiesen. In Zahlen heißt das, dass über die Hälfte der Dokumente zumindest nicht aktuell sind. Insbesondere die Erstellung eines Sicherheitskonzeptes zur Gewährleistung der informationstechnischen Sicherheit ist jedoch von elementarer Bedeutung. Die Aktualität dieser Dokumente ist unverzichtbar.

Die Erstellung, ständige Überprüfung und Umsetzung von IT-Sicherheitskonzepten sind auch in Zeiten knapper Haushaltsmittel unverzichtbar. Diese Aufgaben dürfen auch in den Bezirken nicht vernachlässigt werden. Die Berliner Bäder-Betriebe sind insoweit ein Negativ-Beispiel.

1.6 „MAERKER“ und „Straßensheriff“

Bei dem Projekt „Maerker“ handelt es sich um eine internetbasierte Plattform, auf der Bürgerinnen und Bürger Mängel (z.B. Schlaglöcher, illegale Müllentsorgung, defekte Straßenbeleuchtung) an die Verwaltung melden können. Aufbauend auf dem Erfolg des Originalprojektes in Brandenburg[43] soll nun auch in Berlin das „Online-Ordnungsamt“ für Mängelmeldungen eingeführt werden.[44]

Innerhalb von drei Werktagen werden die Anliegen geprüft, durch Redakteure der Webseite an die zuständigen Stellen weitergeben und nach deren Rückmeldung der aktuelle Bearbeitungsstand im Maerkerportal mithilfe eines Ampelsystems dokumentiert. Ziel des Projektes ist, eine bessere Kommunikation zwischen den Menschen und der Verwaltung zu erreichen, Probleme schneller zu lösen und somit auch die Bürgerzufriedenheit zu steigern. Nach den positiven Erfahrungen im Bezirk Lichtenberg, der das Verfahren testweise im Oktober 2011 einführte, wurde 2013 beschlossen, das System schrittweise in allen zwölf

41 JB 2012, 17.1
42 § 26 BlnDSG

43 http://maerker.brandenburg.de/
44 Mitteilung des Senats zur Kenntnisnahme vom 21. November 2013, Drs. 17/1331

Bezirken einzusetzen. Neben Lichtenberg setzen die Bezirke Marzahn-Hellersdorf und Tempelhof-Schöneberg das Verfahren bereits ein.

Wir haben das Angebot in seiner bisherigen Form geprüft. Positiv hervorzuheben ist, dass die Bürgerhinweise anonymisiert veröffentlicht werden. Personenbezogene Daten (z.B. Kfz-Kennzeichen) werden nicht online veröffentlicht. Lediglich die Daten des Hinweisgebers sowie der Hinweis selbst werden an die für die Bearbeitung zuständige Stelle innerhalb der jeweiligen Verwaltung weitergeleitet. Dort erhalten nur die zuständigen Beschäftigten Zugriff auf die Daten, sodass die Sicherheit und der Schutz der Daten stets gewährleistet sind.

In Brandenburg wurde inzwischen auch eine kostenlose mobile Applikation (App) für die Nutzung von „Maerker" mit iOS-Geräten veröffentlicht.[45] Eine Anpassung der bestehenden App oder Eigenentwicklung für den Einsatz im Berliner Raum ist geplant.

Zunehmend gibt es darüber hinaus auch Bestrebungen privater Anbieter, Internet-Angebote und Apps zu entwickeln, mit denen Menschen aktiv auf Missstände in ihrer Nachbarschaft oder generell im öffentlichen Raum aufmerksam machen können. Ein Unternehmen will die App „Straßensheriff" mit dem Ziel anbieten, einzelnen Verkehrsteilnehmern mithilfe ihrer Smartphones die Anzeige von Regelverstößen zu ermöglichen. In einem ersten Schritt sollen Verkehrsverstöße (z.B. auf Fahrrad- oder Gehwegen geparkte Fahrzeuge) auf einer Karte im Internet angezeigt werden. Darüber hinaus sollten auch Nachrichten an die betreffenden Autofahrer im Internet gepostet und schließlich die Ordnungsämter per E-Mail und Beweisfoto zur Verhängung von Bußgeldern aufgefordert werden können.

Wir haben das Unternehmen darauf hingewiesen, dass nur das Markieren von wahrgenommenen Verkehrsverstößen auf einer Karte im Netz ohne Personenbezug, d. h. auch ohne Angabe eines Kfz-Kennzeichens, datenschutzrechtlich unproblematisch ist. Darüber hinaus können Nutzer der App nach Anmeldung unter Pseudonym ihre Erlebnisse ebenfalls ohne Personenbezug online schildern. Dagegen dürfen Mitteilungen an Fahrzeughalter unter Verwendung von Kfz-Kennzeichen nur veröffentlicht werden, wenn die Adressaten vorher eingewilligt haben. Das Versenden von Anzeige-Mails mit „Beweisfotos" an das Ordnungsamt scheidet solange aus, wie die sichere und damit auch gerichtsverwertbare Übermittlung der personenbezogenen Daten nicht mittels Ende-zu-Ende-Verschlüsselung sichergestellt ist. Zudem müssen die Nutzer darauf hingewiesen werden, dass sie keinen Anspruch auf Verhängung eines Bußgeldes haben, in einem möglichen Verfahren als Zeuge vorgeladen werden können und bei einer Falschanzeige mit strafrechtlichen Konsequenzen rechnen müssen.

45 http://www.kommune21.de/meldung_13848_Maerker+als+App.html

Während das Portal MAERKER datenschutzrechtlich einwandfrei ist, musste der Anbieter der „Straßensheriff"-App sein Konzept modifizieren, um den Vorgaben des Datenschutzes zu entsprechen.

1.7 E-Government-Gesetzgebung im Bund und in Berlin

Anfang August ist das Gesetz zur Förderung der elektronischen Verwaltung (**E-Government-Gesetz des Bundes**) in Kraft getreten. Wir hatten bereits 2012 auf Mängel im Referentenentwurf hingewiesen – allerdings erfolgslos.[46] Es ist äußerst problematisch, dass keine Vorgaben für den Einsatz einer verbindlichen Ende-zu-Ende-Verschlüsselung beim Einsatz von De-Mail[47] getroffen wurden, sodass noch nicht einmal sensitive Daten wie Gesundheitsdaten verschlüsselt übertragen werden müssen. Der Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, verbindliche Veröffentlichungspflichten des Staates – systematisch korrekt – besser in das Informationsfreiheitsgesetz des Bundes aufzunehmen, wurde ebenfalls nicht aufgegriffen; das führt zu einer „Rechtszersplitterung". Die Vorschrift über die Anforderungen an das Bereitstellen von Daten[48] ist unter Open Data-Gesichtspunkten ohnehin wenig praktikabel: Im Kern wird lediglich geregelt, dass Daten grundsätzlich in maschinenlesbaren Formaten zu veröffentlichen sind – dies jedoch nur, wenn an den Daten ein Nutzungsinteresse, insbesondere ein Weiterverwendungs-

46 JB 2012, 1.1 (S. 13 ff.)
47 Siehe hierzu auch 1.2
48 § 12 Abs. 1 EGovG Bund

interesse im Sinne des Informationsweiterverwendungsgesetzes, zu erwarten ist. Weder werden konkrete zu veröffentlichende Datenarten benannt, noch enthält die Regelung überhaupt eine Verpflichtung, Daten zu veröffentlichen. Es bleibt daher auch weiterhin jeder Behörde selbst überlassen, welche Informationen sie im Internet veröffentlicht.

Auf Landesebene liegt nun auch ein Referentenentwurf eines Gesetzes über E-Government- und Organisationsfragen (**Berliner E-Government-Gesetz**) vor.[49] Wir haben der Senatsverwaltung für Inneres und Sport zwei Vorschläge für Regelungen über **Veröffentlichungspflichten** und **gemeinsame Verfahren** unterbreitet:

Die vorgeschlagene Regelung zu **Veröffentlichungspflichten** orientiert sich an den bisherigen Regelungen im IFG,[50] am Referentenentwurf des Berliner E-Government-Gesetzes, am E-Government-Gesetz des Bundes, am Hamburger Transparenzgesetz, am Bremer Informationsfreiheitsgesetz sowie an der Berliner Open Data-Strategie.[51] Um einer „Rechtszersplitterung" entgegenzuwirken, haben wir vorgeschlagen, die Veröffentlichungspflicht ins IFG und nicht ins Berliner E-Government-Gesetz aufzunehmen. Dies bietet sich schon deswegen an, weil das IFG bereits über einen Katalog von Ausschlussgründen verfügt, auf die im Rahmen der Veröffentlichung von Daten zurückgegriffen werden kann. Über die bereits bestehenden Veröffentlichungspflichten hinaus sollen künftig u. a. auch Beschlüsse und Protokolle von Senats-, Bezirksamts-, Parlaments- und Ausschusssitzungen nebst Anlagen, Pressemitteilungen, Berichte, Statistiken, Rundschreiben, Dienstanweisungen, Handlungsempfehlungen sowie Gutachten und Studien veröffentlicht werden, soweit keine der im IFG geregelten Ausnahmen[52] Anwendung findet. Die Daten wären dabei in maschinenlesbaren, offenen Formaten zu veröffentlichen und für einen Zeitraum von mindestens zehn Jahren nach der letzten Änderung für den Abruf bereitzuhalten. Auch würde erstmals ein subjektiver Anspruch auf Veröffentlichung geschaffen, sodass bei unterbliebener Veröffentlichung der Rechtsweg eröffnet wäre.

49 Stand: 13. Juni 2013; zu den Vorentwürfen siehe JB 2012, 1.1, und JB 2011, 1.2.1
50 § 17 IFG
51 JB 2012, 1.2
52 §§ 5 bis 12 IFG

Die vorgeschlagene Regelung zu **gemeinsamen Verfahren** soll eine Angleichung des BlnDSG an die Rechtslage im Bund (Bundesdatenschutzgesetz sowie E-Government-Gesetz des Bundes) und in Brandenburg (Brandenburgisches Datenschutzgesetz) bewirken. Zum einen wird die Einführung **automatisierter Abrufverfahren**[53] erleichtert, da keine explizite Rechtsgrundlage mehr erforderlich ist, sondern sich die Zulässigkeit vielmehr nach den schutzwürdigen Interessen der Betroffenen sowie den Aufgaben der beteiligten Stellen richtet. Zum anderen können unter den gleichen Voraussetzungen dann erstmals **gemeinsame Verfahren** eingeführt werden, die mehreren datenverarbeitenden Stellen die Verarbeitung personenbezogener Daten in oder aus einem gemeinsamen (vorhandenen!) Datenbestand ermöglichen. Die Schaffung neuer Datenbestände ist davon nicht erfasst; hierfür ist weiterhin eine eigene Rechtsgrundlage erforderlich. Eine Regelung über gemeinsame Verfahren ist u. a. deswegen erforderlich, weil für den Betrieb des Bürgerkontos als zentralem Identifizierungsdienst für die eID-Funktion des neuen Personalausweises[54] eine eigene datenschutzrechtliche Verantwortung des Diensteanbieters erforderlich ist, sodass eine Auftragsdatenverarbeitung durch ihn ausscheidet. Zudem können sich auch nicht-öffentliche Stellen an automatisierten Abrufverfahren sowie den neu geschaffenen gemeinsamen Verfahren beteiligen, was bislang unzulässig ist.[55]

Der Berliner Gesetzgeber sollte im Rahmen des E-Government-Gesetzes eine erweiterte Veröffentlichungspflicht in das Informationsfreiheitsgesetz aufnehmen und gemeinsame Verfahren datenschutzgerecht regeln.

1.8 Open Data-Portal des Landes

Berlin hat im September 2011 als erstes Bundesland ein eigenes Open Data-Portal[56] im Rahmen des E-Government-Projekts „ServiceStadtBerlin" gestar-

53 § 15 BlnDSG
54 Siehe 1.3
55 § 15 Abs. 3 BlnDSG
56 http://www.daten.berlin.de

tet.[57] Seitdem wurde das Portal weiter ausgebaut und im Juni mit einem neuen Design in den Regelbetrieb überführt.[58] Seit Oktober werden die amtlichen Geodaten der Berliner Vermessungsverwaltung entsprechend den Open Data-Prinzipien kostenfrei zur Verfügung gestellt. Die Daten, zu denen die in den Bezirken geführte automatisierte Liegenschaftskarte, topographische Landeskartenwerke, Luftbilder und daraus abgeleitete entzerrte digitale Orthofotos sowie Informationen über Bodenrichtwerte zählen, dürfen für jeden kommerziellen und nicht-kommerziellen Verwendungszweck umfassend genutzt werden. Aktuell stehen auf der Webseite rund 280 Datensätze aus mehr als 20 unterschiedlichen Kategorien bereit, die zur Informationsrecherche und Weiterverarbeitung (z.B. für die Entwicklung von Applikationen) von der Öffentlichkeit, Unternehmen, Forschungseinrichtungen und Medieninstituten kostenfrei genutzt werden können. Langfristig ist die Abstimmung und Integration der Berliner Datenangebote mit anderen Angeboten in Deutschland, im deutschsprachigen Raum und in Europa geplant. Dies soll innerhalb der nächsten drei bis fünf Jahre erfolgen. [59]

Bislang besteht noch keine gesetzliche Verpflichtung für öffentliche Stellen, Daten zu veröffentlichen und in das Open Data-Portal des Landes Berlin einzustellen. Wir haben daher einen Vorschlag für eine Gesetzesänderung unterbreitet, der entsprechende Veröffentlichungspflichten in das Informationsfreiheitsgesetz (IFG) aufnimmt.[60]

Sowohl inhaltlich als auch technisch wird der Ausbau des Berliner Open Data-Angebots durch die Open Data-Arbeitsgruppe begleitet, in der Mitglieder verschiedener Berliner Verwaltungen, insbesondere aus den Bereichen Geodaten, Verkehr, Umwelt, Verbraucherschutz, Gesundheit und Soziales, sowie des Amtes für Statistik Berlin-Brandenburg vertreten sind. Zur Wahrung der Belange des Datenschutzes beteiligen auch wir uns an dieser Arbeitsgruppe.

Die Fortentwicklung der Angebote des Berliner Open Data-Portals ist im Sinne der Informationsfreiheit und der Bürgerbeteiligung zu begrüßen.

57 JB 2011, 1.2.1; JB 2012, 1.2
58 http://www.berlin.de/sen/wtf/presse/archiv/20130613.1125.386031.html
59 Kurzfassung der Berliner Open Data-Strategie, S. 20
60 Siehe 1.7

2 Schwerpunkte

2.1 EU-Datenschutzreform

Bereits im letzten Jahr hatten wir über die Pläne der Europäischen Union zu einer Reform des europäischen Datenschutzes berichtet und zehn Vorschläge zur Verbesserung der geplanten Datenschutz-Grundverordnung vorgestellt.[61] Diese Forderungen wurden in der Konferenz der Datenschutzbeauftragten des Bundes und Länder sowie in der Art. 29-Datenschutzgruppe diskutiert und zum Teil in gemeinsame Positionspapiere eingearbeitet. Wir haben uns darüber hinaus direkt an die Berichterstatterinnen und Berichterstatter im federführenden Ausschuss für Bürgerrechte, Inneres und Justiz des Europäischen Parlaments gewandt und unsere Sicht in den Gesetzgebungsprozess eingebracht. Viele unserer Empfehlungen wurden aufgegriffen und sind in den Kompromissvorschlag eingeflossen, den der Ausschuss am 21. Oktober 2013 mit großer Mehrheit angenommen hat. Dieser muss allerdings noch mit dem Ministerrat und der Kommission verhandelt werden. Bei diesen Verhandlungen vertritt der federführende Ausschuss das Europäische Parlament.

Der Kompromissvorschlag des Europäischen Parlaments

Unsere Forderung, dass die Aufsichtsbehörden das Recht auf anlasslosen **Zugang zu Geschäfts- und Diensträumen** behalten, wurde vom Europäischen Parlament aufgegriffen.

Während der ursprüngliche Entwurf der Kommission noch eine Bestellpflicht der oder des **betrieblichen Datenschutzbeauftragten** nur für Unternehmen mit mindestens 250 Beschäftigten vorsah,[62] sieht der Kompromissvorschlag des Parlaments jetzt vor, dass Unternehmen, die im Jahr Daten von mehr als 5.000 Betroffenen oder besonders sensitive Daten verarbeiten, zu einer Bestellung verpflichtet sind. Statt einer Befristung ihrer Bestellung auf nur zwei Jahre wurde die Mindestamtszeit immerhin auf Vier Jahre erhöht. Zudem wurden

61 JB 2012, 2.2
62 Dadurch wären nur noch 0,3 % aller Unternehmen zu einer Bestellung des betrieblichen Datenschutzbeauftragten verpflichtet gewesen.

Anreize geschaffen, personenbezogene Daten zu pseudonymisieren bzw. zu verschlüsseln.

Auch wenn viele unserer Vorschläge umgesetzt wurden, konnten sich unsere Positionen nicht immer durchsetzen. So hatten wir spezielle Regelungen zur Datenverarbeitung durch **Auskunfteien** empfohlen, die bislang nicht aufgegriffen wurden. Während wir dafür eingetreten sind, dass die Verarbeitung personenbezogener Daten zum Zwecke der **Werbung** grundsätzlich nur nach der vorherigen Einwilligung der oder des Betroffenen zulässig ist, könnte der Vorschlag des Parlaments so fehlinterpretiert werden, dass Datenverarbeitung zum Zwecke der Werbung grundsätzlich zulässig ist, bis die oder der Betroffene aktiv widerspricht. Hier ist noch immer dringend eine Klarstellung erforderlich. Alles in allem stellt der Kompromissvorschlag des Parlaments jedoch eine **vernünftige Ausgangsposition** für die Verhandlungen mit dem Rat und der Kommission dar.

Positionen im Ministerrat

Damit die Datenschutz-Grundverordnung in Kraft treten kann, muss neben dem Parlament auch der Rat der EU zustimmen, in welchem die Justiz- und Innenminister der Mitgliedstaaten vertreten sind. Dort waren allerdings bis zum Redaktionsschluss noch viele Punkte hoch umstritten.

So ist im Entwurf der Kommission vorgesehen, dass jeder Betroffene das Recht erhält, sich bei seiner Datenschutzbehörde über Datenverarbeiter zu beschweren, die ihren Hauptsitz im europäischen Ausland haben. Damit wäre es möglich, sich bei unserer Behörde über eine Datenverarbeitung durch das Unternehmen Facebook zu beschweren, welches seinen Hauptsitz in Irland hat. Bislang mussten wir die Betroffenen an die dortige Datenschutzbehörde verweisen. Noch völlig umstritten ist aber, welche Befugnisse die Aufsichtsbehörden erhalten sollen, solchen Beschwerden grenzüberschreitend nachzugehen. Nach dem Vorschlag der Kommission sollen die Datenschutzbehörden verpflichtet werden, solche Beschwerden an die Datenschutzbehörde des Unternehmenssitzes weiterzuleiten und ggf. gemeinsam mit der dortigen Behörde Maßnahmen zu treffen. Andere Vorschläge gehen deutlich weiter und sehen vor, dass die Beschwerdebehörde selbst die Befugnisse erhalten soll, auch Datenschutzverstöße durch ausländische Unternehmen zu ermitteln.

Solche Vorschläge werden allerdings von der datenverarbeitenden Industrie abgelehnt, da die Unternehmen befürchten, sich an – möglicherweise unterschiedlich strenge – Vorgaben verschiedener Aufsichtsbehörden halten müssen.

Ungeachtet dessen bringt die Datenschutz-Grundverordnung für die Unternehmen Vorteile, da sie sich auf dem europäischen Markt nicht mehr an 28 unterschiedliche Datenschutzgesetze halten müssen, sondern an einen einheitlichen unmittelbar geltenden Rechtsakt. Zusätzlich erhalten die Unternehmen an ihrem Sitz eine für sie grundsätzlich zuständige Datenschutzbehörde als Ansprechpartner vor Ort (**sog. One-Stop-Shop**). Dasselbe sollte aber für die Bürgerinnen und Bürger gelten, die das Recht haben, in ihrer Datenschutzbehörde vor Ort eine kompetente Ansprechpartnerin vorzufinden, die auch mit den notwendigen Befugnissen ausgestattet ist, das Recht auf informationelle Selbstbestimmung auch in grenzüberschreitenden Zusammenhängen effektiv zu schützen.

Wie sich die Datenschutzbehörden untereinander abstimmen sollen, ist ebenfalls umstritten. Zwar besteht generell Einigkeit, dass ein „**Kohärenzverfahren**“ zwischen den europäischen Aufsichtsbehörden und ein **Europäischer Datenschutzausschuss** geschaffen werden sollen, der sich mit grenzüberschreitenden Fällen befasst. Dieser stellt das Nachfolgegremium der Art. 29-Datenschutzgruppe[63] dar, in dem die Datenschutzaufsichtsbehörden vertreten sind. Allerdings steckt auch hier der Teufel im Detail. Nach dem ursprünglichen Entwurf der Kommission war vorgesehen, dass der Datenschutzausschuss zwar mit Mehrheit entscheiden kann, diese Entscheidung aber unverbindlich ist. Die Europäische Kommission will sich das Recht vorbehalten, Entscheidungen der Datenschutzbehörden auszusetzen, wenn sie der Auffassung ist, dass die einheitliche Anwendung des Europarechts gefährdet ist. Diese Regelung stellt eine Beeinträchtigung der garantierten **Unabhängigkeit der Datenschutzbehörden** dar, die mehrheitlich im Rat und im Parlament abgelehnt wird. Die Kommission hat viele andere Aufgaben, die unter Umständen mit dem Datenschutz in Konflikt geraten könnten. Sinnvoller wäre es, wenn der Europäische Datenschutzausschuss selbst verbindlich über solche Fälle entscheiden könnte, da dort ausschließlich Behörden vertreten sind, die zum Schutz des Rechts auf informationelle Selbstbestimmung berufen sind.

63 Siehe 16.2

Einigkeit zeichnet sich allerdings in Bezug auf eine wichtige Regelung ab, die auch als Reaktion auf die **NSA-Affäre** im Rat und im Parlament vorgeschlagen wurde. Sie sieht vor, dass Unternehmen – bevor sie personenbezogene Daten an ausländische Behörden oder Gerichte übermitteln – die jeweilige Datenschutzbehörde um eine Genehmigung bitten müssen. Die Grundvoraussetzung für einen solchen Datentransfer ist, dass ein entsprechendes Rechtshilfeabkommen zwischen den involvierten Staaten abgeschlossen wurde. Auch die oder der Betroffene muss über die Datenübermittlung informiert werden. An diese Regelung sollen grundsätzlich alle Unternehmen gebunden sein, die Daten von in der EU ansässigen Bürgerinnen und Bürgern verarbeiten. Dies gilt auch für US-Unternehmen. Schwierigkeiten sind insbesondere zu erwarten, wenn die Unternehmen von der anfragenden Behörde oder dem Gericht nach ausländischem Recht zur Verschwiegenheit verpflichtet werden. Solche Gesetzeskonflikte müssen auf zwischenstaatlicher Ebene geklärt werden, damit ein angemessener Datenschutz auch effektiv gewährleistet werden kann. Vor dem Hintergrund unbegrenzter und anlassloser Überwachung der Internet-Kommunikation durch US-Behörden[64] stellt diese Regelung aber einen großen Schritt in die richtige Richtung dar.

Unverständlicherweise hat sich die Bundesregierung in der Ratsarbeitsgruppe bisher nicht mit besonderem Nachdruck für eine Einigung auf einen gemeinsamen Standpunkt zur Datenschutzreform eingesetzt. Deshalb sind die Chancen gesunken, noch vor der Neuwahl des Europäischen Parlaments im Mai 2014 ein hohes europäisches Datenschutzniveau festzulegen, das jetzt wichtiger denn je ist.

Die Reform des europäischen Datenschutzrechts ist jetzt dringend erforderlich, um die bisherigen Regelungen an die moderne Datenverarbeitung anzupassen. Es ist dafür Sorge zu tragen, dass die Vorschläge des Europäischen Parlaments bei den Verhandlungen mit dem Rat und der Kommission nicht aufgeweicht werden. Datenschutzbehörden benötigen die erforderliche Unabhängigkeit und Kompetenzen, um das Recht auf informationelle Selbstbestimmung effektiv schützen zu können.

64 Siehe 2.2 und 3.3

2.2 Vom sicheren zum unsicheren Hafen – Datenübermittlungen in die USA

Die rasant zunehmende globale Vernetzung steigert die Attraktivität des Cloud Computing.[65] Immer mehr Unternehmen wollen personenbezogene Daten von Kunden, Lieferanten oder Beschäftigten in eine Cloud auslagern, um so einen Fernzugriff Von überall zu ermöglichen und die Aufrechterhaltung einer kostenintensiven Infrastruktur zu vermeiden. Datenschutzrechtlich werden hier jedoch enge Grenzen gesteckt, zumal wenn die Daten nicht nur innerhalb des Europäischen Wirtschaftsraumes (EWR) verarbeitet, sondern in einen Drittstaat transferiert werden. Die Auswahl des Cloud-Anbieters und dessen Serverstandorte spielen bei der Beurteilung der Zulässigkeit der Datenspeicherung in der Cloud eine erhebliche Rolle. Die Unternehmen müssen daher die Verarbeitungsorte kennen, um einen Cloud-Dienst und die Anforderungen an den Datenschutz überhaupt bewerten zu können.

Viele große US-amerikanische Internetdienste- und Cloud-Anbieter wie Amazon, Facebook, Google oder Microsoft können oder wollen keine Garantie geben, dass die Daten Europa nicht verlassen. Ihr Geschäftsmodell basiert gerade darauf, dass ihre Cloud und die darin stattfindenden Datenverarbeitungen nicht an geografische Grenzen gebunden sind. Eine Datenübermittlung in einen Drittstaat darf jedoch nur nach einer zweistufigen Prüfung erfolgen:[66]

1. Die Datenübermittlung muss nach dem Bundesdatenschutzgesetz zulässig, also durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt sein.[67]
2. Es muss ein angemessenes Datenschutzniveau im Drittstaat bestehen, beim Empfänger im Drittstaat hergestellt werden oder ein Ausnahmetatbestand nach § 4c BDSG vorliegen.

65 JB 2011, 2.1

66 § 4 Abs. 1, §§ 4b, 4c BDSG; siehe Beschluss des Düsseldorfer Kreises vom 11./12. September 2013: Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen, Dokumentenband 2013, S. 28

67 Z.B. §§ 28 oder 32 BDSG

Erst wenn sichergestellt ist, dass die Datenübermittlung auf der 1. Stufe zulässig ist, stellt sich die Frage des angemessenen Datenschutzniveaus beim Datenempfänger im Drittland. Für bestimmte Länder hat die Europäische Kommission ein solches festgestellt. In anderen Fällen kann der Datenexporteur in der EU mit dem Empfänger in den USA die EU-Standardvertragsklauseln vereinbaren, die von der Kommission als angemessene Garantien hinsichtlich des Schutzes der Betroffenen anerkannt sind. Auch verbindliche Unternehmensregelungen (Binding Corporate Rules) können angemessene Garantien schaffen und den Datentransfer in den Drittstaat zwischen konzernangehörigen Unternehmen auf der 2. Stufe rechtfertigen. In diesem Fall müssen die Datentransfers Berliner Unternehmen durch uns genehmigt werden.[68]

Datenschutzniveau in den USA

Um den Datentransfer in die USA ohne allzu große Hemmnisse für die Handelsbeziehungen zwischen der EU und den USA zu ermöglichen, hat das US-Handelsministerium die sog. **Safe Harbor-Grundsätze** veröffentlicht, die von der Europäischen Kommission in einer förmlichen Entscheidung als angemessen anerkannt wurden.[69] Diese Angemessenheitsentscheidung betrifft nur solche US-Datenempfänger, die den Safe Harbor-Grundsätzen beigetreten sind, d. h. sich öffentlich verpflichtet haben, diese umzusetzen. Diese Organisationen werden in einer Liste geführt, die auf den Webseiten des US-Handelsministeriums veröffentlicht ist.[70] An andere Stellen, die dem „sicheren Hafen" nicht oder nicht mehr angehören, dürfen personenbezogene Daten aus der EU nur ausnahmsweise übermittelt werden, wenn ein Fall des § 4c BDSG vorliegt.

Bei Anerkennung der Safe Harbor-Grundsätze wurde zwar auf die **Zugriffsmöglichkeiten von US-Sicherheitsbehörden** auf Daten in den USA verwiesen. Zumindest der Europäischen Kommission war aber nicht bewusst, dass US-Behörden verstärkt nach den Terroranschlägen vom 11. September 2001 diese Zugriffsmöglichkeiten massiv ausgeweitet und von ihnen gemeinsam mit ausländischen Nachrichtendiensten auch außerhalb der USA flächendeckend und ohne konkrete Verdachtsmomente Gebrauch gemacht haben.

68 § 4c Abs. 2 Satz 1 BDSG
69 Entscheidung 2000/520/EG vom 26. Juli 2000, ABl. L 215 vom 25. August 2000, S. 7
70 safeharbor.export.gov/list.aspx

Vor dem Hintergrund der aktuellen Erkenntnisse im Zusammenhang mit den Aktivitäten des US-Geheimdienstes **National Security Agency (NSA)** muss die Datenschutzsituation in den USA deshalb grundsätzlich neu bewertet werden.

Die jetzt bekannt gewordenen Zugriffe von US-Behörden sind im Lichte des europäischen Datenschutzrechts nicht zu rechtfertigen, da die Grundsätze der Verhältnismäßigkeit sowie die fundamentalen Datenschutzprinzipien der Zweckbestimmung, der Erforderlichkeit und der Transparenz nicht ausreichend eingehalten werden. Selbst Zugriffe, die auf gesetzlichen Ermächtigungsgrundlagen nach US-Recht wie dem Foreign Intelligence Surveillance Act (FISA) beruhen sollen, halten einer solchen Überprüfung nicht stand. Die Betroffenen werden weder informiert noch stehen ihnen Auskunfts- oder Rechtsschutzmöglichkeiten zur Verfügung. Im Gegenteil: Die Unternehmen werden durch sog. „gag orders" verpflichtet, Zugriffe geheim zu halten. Auch scheint eine effektive Überprüfung der Notwendigkeit von Überwachungsmaßnahmen nicht gewährleistet, wie sich aus neuerdings veröffentlichten Entscheidungen des für Anordnungen nach dem FISA zuständigen Gerichts ergibt. Zudem hat die NSA offenbar mindestens partiell die Kontrolle über ihre eigene Datenverarbeitung verloren, wodurch es zu eindeutigen Verstößen gegen US-Recht gekommen ist.[71]

In erster Linie ist es Sache der **Bundesregierung** und der **Europäischen Kommission**, endlich Konsequenzen aus den bekannt gewordenen Überwachungsmaßnahmen zu ziehen und sich für den Datenschutz der Menschen in Europa effektiv einzusetzen.

Die **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder hat die Bundeskanzlerin bereits im Juli in einem Brief aufgefordert, plausibel darzulegen, wie der unbeschränkte Zugriff ausländischer Nachrichtendienste auf personenbezogene Daten der Menschen in Deutschland im Sinne der Datenschutzgrundsätze begrenzt wird. Das Bundeskanzleramt hat hierauf nur mit allgemeinen Ausführungen zu den Aktivitäten, die die Bundesregierung im Zusammenhang mit der neuen europäischen Datenschutz-Grundverordnung[72]

71 Siehe Einleitung
72 Siehe 2.1

entfaltet, geantwortet und den Brief der Datenschutzkonferenz an das Bundesministerium des Innern weitergegeben.

Bereits drei Jahre nach Inkrafttreten der Safe Harbor-Entscheidung hätte die Kommission sie evaluieren werden müssen. Erst im November – also mit zehnjähriger Verspätung – hat sie eine **Mitteilung zur Funktionsweise von Safe Harbor** veröffentlicht. [73] Darin stellt sie Defizite bei der Transparenz und der Durchsetzung des Arrangements fest. Der Massenzugriff Von Geheimdiensten auf personenbezogene Daten, die an Safe Harbor-Unternehmen transferiert wurden, würde zudem ergänzende, ernsthafte Fragen für die Aufrechterhaltung der Datenschutzrechte europäischer Bürger aufwerfen. Die Kommission gibt insgesamt **13 Empfehlungen zur Verbesserung des Safe Harbor-Programms**. Danach soll die Ausnahme, die in der Safe Harbor-Entscheidung für Zugriffe aus Gründen der nationalen Sicherheit vorgesehen ist, nur für Fälle gelten dürfen, in denen die Erforderlichkeit und Verhältnismäßigkeit strikt eingehalten werden. Bis zum Sommer 2014 sollen die US-Behörden diese Empfehlungen umsetzen. Sodann will die Kommission die Entscheidung erneut überprüfen. Was bis dahin im Hinblick auf die täglich in einer Vielzahl stattfindenden Datentransfers in die USA geschehen soll, bleibt unklar. Mit dieser Frage hat sich auch die Art. 29-Datenschutzgruppe, in der wir die Landesaufsichtsbehörden vertreten, befasst – bislang ohne Ergebnis.

Konsequenzen für unsere Tätigkeit

In dem Brief an die Bundeskanzlerin und in einer begleitenden Pressemitteilung hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder angekündigt, dass die Aufsichtsbehörden für den Datenschutz vorerst keine neuen Genehmigungen für Datenübermittlungen in Drittstaaten (z.B. auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche auf der Grundlage der Safe Harbor-Entscheidung und der EU-Standardvertragsklauseln erfolgten Datenübermittlungen auszusetzen sind. Dreh- und Angelpunkt dieser Prüfung ist die Frage, welche Beschränkungen der Datenschutzrechte über diejenigen hinausgehen, die im Sinne von Artikel 8 der Europäischen Menschenrechtskonvention in einer demokratischen Gesellschaft

73 Bisher nur in englischer Fassung verfügbar: Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847

notwendig sind. Die Europäische Kommission hat bei ihrer Anerkennung der Safe Harbor-Grundsätze 2000 den nationalen Aufsichtsbehörden ausdrücklich die Befugnis eingeräumt, transatlantische Datenübermittlungen auszusetzen, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden. [74] Wir haben damit begonnen, in Fällen, in denen uns Drittstaatentransfers bekannt sind, die verantwortlichen Stellen um Stellungnahme zu bitten, welche Maßnahmen ergriffen werden, um Massenzugriffe durch die NSA auf Daten in den USA zu verhindern. Dabei geht es uns insbesondere darum, mit den Unternehmen in einen Dialog zu treten, Strategien und Maßnahmen zu erörtern, die angesichts der Gefahr eines Datenzugriffs verfolgt und ergriffen werden können, sowie einen Austausch über mögliche Lösungswege zu erreichen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dies bei einer Podiumsdiskussion in der Industrie- und Handelskammer zum Thema „Schadet die NSA Ihrem Business?“ am 4. Dezember erläutert.

Behörden und Unternehmen sind angesichts der bekannt gewordenen flächendeckenden Überwachung des weltweiten Datenverkehrs auf **Vertrauenswürdige Cloud-Dienste** angewiesen. Sowohl die Bundesregierung als auch die Europäische Kommission verfolgen deshalb Strategien, um solche Dienste (Trusted Cloud) zu fördern. Bei europäischen Cloud-Diensten besteht allerdings das zusätzliche Problem, dass zumindest auch der britische Geheimdienst GCHQ sich an den unverhältnismäßigen Überwachungspraktiken der NSA beteiligt. Solange dies nicht abgestellt wird, wären deutsche Cloud-Dienste zu bevorzugen. Es ist deshalb besonders zu begrüßen, dass die **Berlin Partner für Wirtschaft und Technologie GmbH** unserem bereits 2012 gegebenen Rat gefolgt ist: Sie hat ihr US-basiertes Kundenmanagement-System Ende 2013 abgeschaltet und verarbeitet ihre Kundendaten nun in Berlin. Ein Verbot der Nutzung anderer europäischer Cloud-Dienste würde allerdings an europarechtliche Grenzen stoßen.

Die Nutzung der Cloud-Angebote von US-Firmen wie z.B. **Microsoft Office 365** wirft demgegenüber zahlreiche noch ungeklärte Fragen auf. So hat das Bundesamt für Sicherheit in der Informationstechnik der Bundesverwaltung schon vor der Aufdeckung des NSA-Skandals von Office 365 abgeraten. In

74 Art. 3 Abs. 1 der Entscheidung 2000/520/EG vom 26. Juli 2000, ABl. L 215 vom 25. August 2000, S. 7

jedem Fall stellt sich auch die grundsätzliche Frage, ob ein Unternehmen in den USA als Auftragnehmer eines deutschen Auftraggebers weisungsgebunden nach § 11 BDSG arbeiten kann, wenn es von einer staatlichen Stelle gezwungen werden kann, sämtliche für die Auftraggeber gespeicherten Daten an diese Stelle zu übermitteln und den Auftraggeber hierüber aufgrund einer „gag order" weder vorher noch nachher zu informieren. In einzelnen Nutzungsszenarien kann der Einsatz von **Ende-zu-Ende-Verschlüsselung** und **Pseudonymisierung** eine Verbesserung des Sicherheits- und Datenschutznivaus erbringen. Hier ist jedoch eine Einzelfallprüfung notwendig.

Das zwischen Europa und den USA geschlossene Safe Harbor-Abkommen hat mit der Aufdeckung der unkontrollierten Aktivitäten der NSA seine Geschäftsgrundlage verloren und muss grundlegend überarbeitet werden. Letztlich kann Rechtssicherheit im grenzüberschreitenden Datenverkehr nur durch verbindliche internationale Vereinbarungen über Mindeststandards zum Datenschutz hergestellt werden.

2.3 Datenverarbeitung im forensischen Bereich eines Wirtschaftsprüfungsunternehmens

Als erste Aufsichtsbehörde in Deutschland haben wir den forensischen Bereich eines Wirtschaftsprüfungsunternehmens geprüft. Dieser Bereich bietet viele Dienstleistungen an: Er unterstützt Unternehmen bei der Untersuchung von wirtschaftskriminellen Taten und Handlungen in und gegen Institutionen des Mandanten, wie etwa Unterschlagungen in der Buchhaltung, Diebstahl von Waren oder die Begehung von Untreuehandlungen von Beschäftigten, die kollusiv mit Lieferanten zusammenarbeiten. Unternehmen wenden sich auch an die forensische Abteilung, um **Straftaten oder Compliance-Verstöße** zu verhindern. Hier analysiert das Wirtschaftsprüfungsunternehmen, ob bestimmte Verfahrensprozesse verändert und optimiert werden können. Leitende Beschäftigte werden vor ihrer Einstellung überprüft, auch neue Lieferanten vor der ersten Lieferung. Der forensische Bereich unterstützt Unternehmen außerdem bei Datenlecks, sichert und bereitet Daten für ihre Kunden auf, etwa um sie in ein Gerichtsverfahren einzubringen.

Um ihre Arbeit durchführen zu können, benötigen die Prüfer viele Informationen von ihren Mandanten, häufig auch personenbezogene Daten von Beschäftigten, Lieferanten und Kunden. Dies ist datenschutzrechtlich nicht zu beanstanden, allerdings müssen sowohl das auftraggebende Unternehmen als auch das Wirtschaftsprüfungsunternehmen bestimmte datenschutzrechtliche Standards beachten. Unsere Kontrolle hat ergeben, dass insoweit ein nicht unerheblicher **Verbesserungsbedarf** besteht. Die nachfolgenden Hinweise, die aufgrund festgestellter Mängel entwickelt worden sind, sollen sowohl Wirtschaftsprüfungsunternehmen als auch ihre Mandanten dabei unterstützen, Sonderuntersuchungen datenschutzkonform durchzuführen bzw. durchführen zu lassen.

Bei einem neuen Projekt ist zuerst zu prüfen, ob der Auftrag als Auftragsdatenverarbeitung ausgeführt werden kann. Die forensische Sicherung firmeneigener Daten oder eine Beweismittelsicherung im Zusammenhang mit einem in den USA anhängigen Gerichtsverfahren kann z.B. in der Regel als Auftragsdatenverarbeitung durchgeführt werden. Ist eine solche möglich, sollte eine Datenübermittlung unterbleiben, da diese dann nicht erforderlich ist.[75] Bei mehrstufigen Aufträgen ist es möglich, dass Teilbereiche als Auftragsdatenverarbeitung durchgeführt werden und erst im Anschluss an den Auftrag Daten übermittelt werden.

Übermittelt ein Kunde personenbezogene Daten an die Wirtschaftsprüfungsgesellschaft, ist die Frage, ob der Kunde die personenbezogenen Daten rechtmäßig verarbeitet, auch für die Wirtschaftsprüfungsgesellschaft von Bedeutung, da diese verantwortliche Stelle wird und die Datenverarbeitung nur dann rechtmäßig sein kann, wenn auch der Auftraggeber rechtmäßig in den Besitz der Daten gelangt ist. Dies führt zwar nicht zu der Verpflichtung, eine vollständige Rechtmäßigkeitsprüfung bei dem Kunden vor Übermittlung der Daten vorzunehmen, wohl aber zu der Notwendigkeit, eine Plausibilitätsprüfung durchzuführen. Dies hat die Wirtschaftsprüfungsgesellschaft bei zwei Muttergesellschaften, die Daten der Tochtergesellschaften übermittelt haben, unterlassen. Aufgrund des fehlenden Konzernprivilegs bestand hier der Verdacht, dass die Muttergesellschaften nicht rechtmäßig in den Besitz der personenbezogenen

75 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Daten gelangt waren bzw. als Auftragsdatenverarbeiter der Konzerntöchter diese Daten weisungswidrig an Dritte übermittelt hatten.

Bei einer forensischen Untersuchung dürfen nur die Daten erhoben werden, die für die Durchführung des Auftrags erforderlich sind.[76] Der forensische Bereich ist also verpflichtet, Verfahren zu entwickeln, die es ermöglichen, nur die Daten zu erheben, die zur Durchführung des Auftrags benötigt werden. Er ist nicht berechtigt, von Kunden angebotene Daten ohne Prüfung der Erforderlichkeit zu erheben. Erforderlich können allerdings auch Datensätze sein, bei denen eine Anfangswahrscheinlichkeit für eine Erforderlichkeit spricht, auch wenn diese sich später nicht bestätigt. Derartige Daten sollten möglichst zügig an den Auftraggeber zurückgegeben werden. Vermieden werden sollte aber ein Verfahren, in dem der forensische Bereich zunächst vorsorglich alle greifbaren Daten wie ein Staubsauger aufnimmt, um dann zu prüfen, ob und wie diese nutzbar gemacht werden können.

In der Regel benötigt das Wirtschaftsprüfungsunternehmen zur Durchführung des Auftrags Klarnamen. Kann ein Auftrag aber mit pseudonymen oder sogar anonymen Daten erledigt werden, sollten keine Klardaten erhoben und verarbeitet werden. So ist etwa bei einem **präventiven Screening** zur Durchführung einer Risikoanalyse in Bezug auf wettbewerbs- und kartellrechtliche Compliance zu prüfen, ob zunächst ein pseudonymer oder sogar anonymer Datenabgleich möglich und ausreichend ist.

Das Bundesdatenschutzgesetz hat den Grundsatz der Direkterhebung konstituiert.[77] Danach stellt die **Erhebung beim Betroffenen** die Regel dar. Nur in Ausnahmefällen, insbesondere wenn der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, kann von diesem Grundsatz abgewichen werden. Es ist zu empfehlen, die Gründe schriftlich zu fixieren, die zu einem Verzicht auf eine Direkterhebung geführt haben. Der Grundsatz der Direkterhebung wird jedenfalls nicht dadurch außer Kraft gesetzt, dass der Kunde dem Wirtschaftsprüfungsunternehmen die Direkterhebung untersagt.

76 § 28 Abs. 1 Satz 1 Nr. 2 und § 3a BDSG
77 § 4 Abs. 2 BDSG

Soweit die Datenverarbeitung bei dem Wirtschaftsprüfungsunternehmen auf die Einwilligung der Beschäftigten gestützt wird, ist zu hinterfragen, ob diese freiwillig in die Datenverarbeitung eingewilligt haben. Bei einem präventiven Screening zur Risikoanalyse war dies nicht der Fall. Auch wurde nicht beachtet, dass die Einwilligung eines Beschäftigten keine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten seiner Ehefrau darstellt.

Bei der Nutzung von Backups, die zu Datensicherungszwecken vorgehalten werden, ist die besondere **Zweckbindung** zu beachten.[78] Die Daten dürfen nur noch zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verwendet werden. Wenn ein Wirtschaftsprüfungsunternehmen Nutzungsspuren einsehen kann, obwohl diese Daten bereits gelöscht waren, spricht dies für einen Verstoß gegen § 31 BDSG. Bei der Wertung, ob gelöschte E-Mails wieder hergestellt werden dürfen, sollte auch beachtet werden, dass der Schutzbereich des § 88 TKG bei erhaltenen E-Mails deshalb eingeschränkt wird, da der Betroffene die Möglichkeit zur Löschung hat. Diese Möglichkeit ist ihm als Arbeitnehmer aber gerade genommen, wenn aufgrund von Backups gelöschte Daten wiederhergestellt werden können.

Das geprüfte Wirtschaftsprüfungsunternehmen verzichtete grundsätzlich darauf, **Betroffene** zu **benachrichtigen**.[79] Nach dem Bundesdatenschutzgesetz ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Die Betroffenen erhielten die Information, dass ihre personenbezogenen Daten von dem Wirtschaftsprüfungsunternehmen verarbeitet werden, nur dann, wenn sie im Rahmen von Ermittlungen – etwa bei Befragungen – hierüber informiert wurden oder der Mandant die entsprechenden Informationen selbst an den Betroffenen gegeben hatte.

Bei der Auslegung des § 33 BDSG ist zu beachten, dass diese Norm eine zur Sicherung des Rechts auf informationelle Selbstbestimmung erforderliche verfahrensrechtliche Schutzbestimmung darstellt. Ein Betroffener kann seine weitergehenden Rechte auf Auskunft, Berichtigung, Löschung und Sperrung

78 § 31 BDSG
79 § 33 Abs. 1 Satz 1 BDSG

seiner Daten nur ausüben, wenn er Kenntnis davon hat, dass personenbezogene Daten zu seiner Person bei einer bestimmten verantwortlichen Stelle gespeichert sind. Insofern konkretisiert die Benachrichtigungspflicht das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung. Der Gesetzgeber hat deshalb die Benachrichtigungspflicht der verantwortlichen Stelle nur in Ausnahmefällen suspendiert.[80] Eine Benachrichtigung ist etwa nicht erforderlich, wenn der Betroffene Kenntnis von der Datenverarbeitung bei dem Wirtschaftsprüfungsunternehmen hat oder wenn die Benachrichtigung die Ermittlungsarbeit gefährden würde. Das Wirtschaftsprüfungsunternehmen kann sich nicht pauschal auf seine Schweigepflicht berufen. Vielmehr müssen konkrete Tatsachen vorliegen, die ein rechtliches Geheimhaltungsinteresse begründen.[81]

Auch die forensische Abteilung eines Wirtschaftsprüfungsunternehmens ist an Compliance-Regeln gebunden. „Compliance" erstreckt sich auch auf die Einhaltung des Bundesdatenschutzgesetzes.

2.4 Das intelligente Haus

Mit der Verbesserung der Lebensqualität verändern sich auch die Bedürfnisse und Ansprüche der Menschen in ihrem privaten Wohnbereich. Die fortschreitende Digitalisierung des Lebens führt dazu, dass auch die Haustechnik zunehmend „intelligenter" bzw. „smarter" wird.

Unter dem Begriff **„Smart Home"**, der als Oberbegriff für technische Verfahren und Systeme in Wohnräumen dient, fällt sowohl die Vernetzung von elektrischen Einrichtungen (z.B. Lampen, Jalousien, Heizung) und von Haushaltsgeräten (z.B. Herd, Kühlschrank, Waschmaschine) als auch die Vernetzung von Komponenten der Unterhaltungselektronik (z.B. Radio, Fernsehen, Internet, Smartphone) und die damit verbundene zentrale Speicherung und Nutzung von Video- und Audio-Inhalten.

80 § 33 Abs. 2 Satz 1 Nr. 1 – 9 BDSG
81 § 33 Abs. 2 Satz 1 Nr. 3 BDSG

Bei intelligenter Gebäudetechnik denkt man zunächst an futuristische Filme: Kühlschränke, die Roboter zum Einkaufen schicken, Wasserhähne mit automatischer Temperaturregulierung, halbdurchlässige Badezimmerspiegel, die den Wetterbericht aus dem Internet präsentieren, oder greifarmgeführte Zahnbürsten, die auf die individuellen Bedürfnisse der Nutzenden zugeschnitten sind. Dies alles wird gesteuert von einem zentralen Computer, der die morgendliche Hygiene im Schlaf erledigt und die Bewohner erst fertig gekleidet am bereits gedeckten Frühstückstisch weckt.

Das klingt noch nach Zukunftsmusik, allerdings sind die Weichen für diese Entwicklung bereits gestellt. Unter dem Begriff **„Hausautomation"** werden mittlerweile sämtliche Überwachungs-, Steuerungs-, Regelungs- und Optimierungseinrichtungen im privaten Wohnraum zusammengefasst. Zur Hausautomation zählen z.B. Stromausfallmelder für Kühltruhe und Klimaanlage oder Wasserstandsensoren für den Keller. Insbesondere bezieht sich der Begriff auf die Steuerung der direkt mit dem Haus verbundenen Einrichtungen wie der Alarmanlage, der Beleuchtung, der Jalousien und der Heizung. Die Schalter im Haus können aber auch so programmiert werden, dass sie jedes Endgerät individuell steuern.

Wenn z.B. die Bewohner das Haus verlassen, teilen sie ihrem Haus über einen zentralen Schalter an der Eingangstür mit, dass es nun allein ist. Daraufhin schaltet das System erst einmal alle überflüssigen Elektrogeräte ab und beginnt vollautomatisch, potentiellen Einbrechern die Anwesenheit der Hausbewohner vorzuspielen: In vordefinierten Zeitintervallen schaltet sich die Hausbeleuchtung an und aus, und die Jalousien heben und senken sich. Sollten sich Einbrecher davon nicht abschrecken lassen, werden Sensoren an den Fenstern oder Bewegungsmelder an der Hausfassade aktiviert, wodurch die abwesenden Bewohner über ihr Smartphone eine Alarmmeldung erhalten. Die Nutzung des Systems auf diese Art und Weise könnte als **„elektronische Diebstahlsprophylaxe"** bezeichnet werden.

Das Smartphone kann aber nicht nur Alarmmeldungen empfangen, sondern auch aktiv zur **Fernsteuerung der Hausautomation** genutzt werden. Genannt sei das Einschalten der Heizung via Smartphone eine Stunde vor der Heimkehr, sodass die bis dahin kalte Wohnung bei der Ankunft bereits angenehm warm ist, ohne dass während der Abwesenheit Energie

verschwendet worden wäre. Diese Fernsteuerbarkeit wäre auch via Internet oder über das Telefonnetz denkbar.

Über die Schaffung einer angenehmen Wohnzimmeratmosphäre (z.B. der Steuerung des Lichteinfalls über Jalousien) hinaus bietet die Unterhaltungselektronik für den Privatgebrauch noch weitere Annehmlichkeiten. Zu den typischen Beispielen vernetzter Unterhaltungselektronik gehört die **zentrale Speicherung von Medien** wie Fotos, Musik und Filmen, die über entsprechende Serversysteme in jedem Zimmer des Hauses abrufbar sind. Die Übertragung der Daten erfolgt in der Regel drahtlos über ein WLAN-Netz, kann aber auch kabelgebunden realisiert werden.

Die alltäglichen Abläufe im Haushalt sowie die Nutzung der Haushaltsgeräte können mittels Automatisierung ebenfalls optimiert werden. Unter Haushaltsgeräte-Automation versteht man etwa die **Vernetzung, Fernsteuerung und Programmierung von Elektrohaushaltsgeräten** wie Herd, Kühlschrank, Waschmaschine oder Kaffeeautomat, wenn etwa der zum Frühstück automatisch aufgebrühte Kaffee und die aufgebackenen Brötchen zur gleichen Zeit fertig sein sollen.

Eng verwandt mit der Hausautomation ist das sogenannte „**Smart Metering**“.[82] Gemeint ist ein System, das über einen intelligenten Zähler verfügt, der den tatsächlichen Verbrauch von Strom, Wasser oder Gas und die tatsächliche Nutzungszeit misst. Ziel ist es, dem Endverbraucher von der Tageszeit abhängige und möglichst niedrigere Energiekosten anzubieten. Zugleich soll Smart Metering für den Endverbraucher die Transparenz in Bezug auf den Energie- und Ressourcenverbrauch erhöhen und ihm helfen, verbrauchssenkende Maßnahmen zu ergreifen.

Ein Blick in die Zukunft

Neben dieser Vielzahl von positiven technischen Entwicklungen, die den Alltag der Menschen erleichtern sollen, gibt es allerdings auch kritische Anmerkungen. Das folgende Szenario wurde in vergleichbarer Form auf der Internationalen Funkausstellung 2013 in Berlin von einem bekannten Konzern für

82 Zuletzt JB 2012, 11.1

Unterhaltungselektronik vorgestellt und ist ein gutes Beispiel für **die möglichen Gefahren** dieser Entwicklung.

Ein Bekannter eines fiktiven Ehepaars meldet unerwartet über das Telefon sein Kommen an und gibt seinen aktuellen Standort bekannt. Über eine Steuerungssoftware auf dem heimatlichen Tablet-PC wird der wahrscheinliche Zeitpunkt seines Eintreffens ermittelt. Anhand der über Sensoren erfassten Lebensmittelvorräte im Kühlschrank und der vorhandenen Dekorationselemente unterbreitet das System Rezept- und Tischdekorationsvorschläge, die in der zur Verfügung stehenden Zeit realisierbar sind, und gibt entsprechende Umsetzungsanweisungen.

Auf den ersten Blick offenbaren sich bei diesem Szenario viele Vorteile, aber es eröffnen sich auch Risiken. Für die Erfassung der Daten, die erforderlich wären, müssten sich Sensoren im Kühlschrank und zumindest partiell auch in Schränken, in denen Dekorationselemente gelagert werden, befinden. Die erfassten Daten würden zur Ermittlung der Vorschläge an einen oder sogar mehrere Anbieter in das Internet übertragen werden. Viele Online-Angebote sind häufig kostenfrei und werden über Werbung oder die Vermarktung der gelieferten Nutzerdaten finanziert. Ein entsprechender Anbieter würde die Daten des Paares weitergeben. Eine Einwilligung durch die betroffenen Nutzer wird in der Regel bereitwillig erteilt.

Dieses Beispiel wäre auch auf den **Gesundheitssektor** erweiterbar. Derzeit befinden sich vernetzbare Fitnessgeräte in der Entwicklung, die in Verbindung mit dem Smartphone zu einem digitalen Gesundheitsmanager werden, bei dem Blutzucker, Temperatur, Gewicht, Blutdruck und Puls einfach und schnell erfasst, ausgewertet und gespeichert werden können. Würde man die einzelnen Mosaiksteine der genehmigten Datenübermittlung mit anderen Daten zusammenführen, ergäbe das ein erschreckend klares Gesamtbild des Einzelnen.

Die Datensammellust der Industrie ist aber nicht das einzige Risiko. Auch Haushaltsgeräte werden intelligente Geräte wie z.B. Herd oder Spülmaschine; diese können über das Smartphone mit Internet-Verbindung ferngesteuert werden. Damit wären sie dem **Risiko eines Angriffs aus dem Internet** ausgesetzt. Potentielle Fehler in der Gerätesoftware könnten durch Angreifer ausgenutzt werden und erheblichen Schaden verursachen. Wird der Herd von

außen angeschaltet, könnte das einen Brand verursachen. Dieses Problem hat auch die Industrie erkannt und eine entsprechende Sicherung installiert, die eine Bestätigung des Einschaltvorgangs am Gerät erfordert. Dennoch verbleiben Restrisiken, wie das Beispiel eines aus der Ferne abgeschalteten Kühlschranks verdeutlicht. Durch die verdorbenen Lebensmittel würde ein Vermögensschaden entstehen.

Big Brother im Haus?

Bereits 2011 berichteten wir von den möglichen Gefahren, die vernetzte Unterhaltungselektronik birgt.[83] Die Kopplung von Smartphones oder Tablet-PCs mit Unterhaltungselektronik verläuft langsamer als ursprünglich angenommen. Noch sind diese Geräte kein adäquater Ersatz für die Fernbedienung. Dennoch schreitet diese Entwicklung voran. Die Kopplung erzeugt ein zusätzliches Risiko, das durch potentielle Schadsoftware auf den Geräten entstehen kann. Der Einstieg in diesen Trend sollte gut überlegt sein.

Die eigenen vier Wände, die im Allgemeinen als geschützter Raum angesehen werden, könnten einer möglichen Überwachung durch die in Smart-TVs eingebauten Kameras und Mikrofone unterworfen werden. Das Thema hat vor dem Hintergrund der bekannt gewordenen Überwachungen durch die Geheimdienste[84] eine zusätzliche Dynamik erhalten. Einige Hersteller sind sich dieses Problems bewusst. In vielen, allerdings nicht in allen Geräten gibt es softwareunabhängige Möglichkeiten, die potenziellen Überwachungshelfer durch manuelle Schalter abzuschalten. An dieser Stelle kann das Einkaufsverhalten der Kunden helfen, diesen Prozess voranzubringen. Das Beispiel einer kürzlich erschienenen **Spielekonsole** zeigt den bereits jetzt vorhandenen Einfluss. Ursprünglich sollte diese Konsole nur mit einem Kamera- und Mikrofonmodul nutzbar sein, um eine Gesten- und Sprachsteuerung zu ermöglichen. Dies würde eine permanente Bereitschaft der Sensoren zur Aktivierung der Konsole bedeuten. Der anhaltend starke Kundenprotest änderte letztendlich die Strategie des Herstellers.

Die Hersteller entwickeln nicht nur zum Wohle des Kunden. Dies zeigen jüngst bekannt gewordene Fälle, in denen Hersteller von **Smart-TVs** im Verdacht standen, dass deren Geräte ungefragt Informationen über das Fernsehverhalten der Nutzenden übermitteln würden. Ein entsprechender Verdacht wurde im November von einem Hersteller bestätigt.

Weiterhin steht seit einer Studie der Technischen Universität Darmstadt auch der künftige Fernseh-Standard HbbTV in Verdacht, dass HbbTV-Applikationen das Nutzungsverhalten der Kunden verfolgen und an Programmveranstalter bzw. Hersteller von Smart-TV-Geräten weiterleiten.[85] HbbTV verknüpft die bisher über den DVB-Standard ausgestrahlten Fernsehprogramme mit Internet-Diensten, wie z.B. die Mediatheken diverser Fernsehsender. Auch das inzwischen an Bedeutung gewonnene IP-TV überträgt funktionsbedingt Nutzungsdaten an die jeweiligen Anbieter. Wir befinden uns am Anfang eines Übergangs des Mediums Fernsehen von der Ein-Weg-Übertragung zu einem Zwei-Wege-System, in dem Daten der Zuschauerin oder des Zuschauers erfasst werden können. Es muss in der Hand der einzelnen Person liegen, ob ihr **Medienkonsum** beobachtet werden darf. Der Datenschutz muss immanenter Bestandteil dieser neuen Technologien sein. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder mehrfach hingewiesen.[86]

Sicherung des Heimnetzwerks

In den meisten Fällen ist die Zentrale der heimischen Vernetzung der **Router**. Dieser bildet den Übergangspunkt vom heimischen Netzwerk zum Internet. Nach der Einrichtung des Geräts rückt dieses meist erst im Störungsfalle zurück in den Fokus. Aber auch Router benötigen eine gewisse Wartung, sie sind nicht immer frei von Fehlern. Ein Problem ist das Fehlen einer automatischen Update-Funktion. Erst im Sommer 2013 wurden erhebliche Sicherheitslücken in diversen Routern unterschiedlicher Hersteller bekannt. Darunter waren viele Geräte, die von großen Internet-Providern im Paket mit ihren Anschlüssen verkauft wurden. Ein Provider reagierte mit der Durchführung von Sicherheitsüberprüfungen für noch nicht ausgelieferte Gerätetypen. Obwohl diese Probleme im umfänglichen Maße publiziert wurden, ist damit zu

83 JB 2011, 12.6
84 Siehe 2.2 und 3.3

85 http://media.cased.de.s3.amazonaws.com/files/2013_CASED_HbbTV.pdf; entsprechende Feststellungen hat die niederländische Datenschutzbehörde bei TV-Geräten von Philips gemacht.
86 Zuletzt Entschließung vom 28./29. September 2011: Anonymes elektronisches Bezahlen muss möglich bleiben!, Dokumentenband 2011, S. 26

rechnen, dass viele Geräte trotzdem keinem Update unterzogen wurden. Wie der PC oder das Notebook benötigt der Router eine regelmäßige Wartung.

Einige Geräte bieten auch die Möglichkeit, den Internet-Zugang für Geräte zu kontrollieren. Die Option ist in der Regel nur sinnvoll, wenn Geräte im heimischen Netzwerk kommunizieren dürfen, aber der Internet-Zugang verwehrt werden soll. Ein fallweiser Zugang ist theoretisch realisierbar, aber nur umständlich zu steuern, da eine Anmeldung am Router erforderlich wird. Die Realisierung einer benutzerfreundlichen Kontrollinstanz, bei der die Anwender entscheiden, welcher Internet-Verkehr erwünscht ist, wird in Zukunft eine große Herausforderung für die Hersteller dieser Geräte darstellen.

Die voranschreitende Vernetzung der eigenen vier Wände erfasst immer mehr persönliche, bisher als sicher geltende Daten. Die Freiheit des Einzelnen, über diese zu bestimmen, muss bereits bei der Entwicklung dieser Technologien im Mittelpunkt stehen.

3 Inneres und Sport

3.1 Falsch verstandene Zuständigkeit

Einem beim Landeskriminalamt (LKA) im Bereich Sexualstraftaten tätigen Polizisten fiel ein auf der Straße geparktes, beschädigtes Kraftfahrzeug auf. Er vermutete einen Unfallschaden oder gar einen strafrechtlichen Hintergrund und führte eine Fahndungsabfrage zu dem Fahrzeug durch. Diese verlief negativ. Als der PKW ein paar Wochen später weiterhin im selben Zustand dort parkte, nahm der Polizist im Polizeilichen Informationssystem eine Halter- und Fahndungsabfrage vor. Anschließend bat er die Kontaktbereichsbeamtin, den Halter über den Zustand seines Fahrzeuges zu informieren. Da ihm die Kontaktbereichsbeamtin kein Ergebnis zurückgemeldet hatte, rief er an und erfuhr, dass der Halter sich selbst um sein Kraftfahrzeug kümmern wollte. Da das Auto weiterhin unverändert auf öffentlichem Straßenland abgestellt war, hat der LKA-Mitarbeiter den Halter unter Verwendung seines dienstlichen Briefkopfes offiziell angeschrieben. Die Daten erhielt er durch eine erneute Abfrage. Erst nach dem empörten Rückruf des Halters informierte der LKA-Mitarbeiter die zuständige Fachdienststelle für Verkehrsangelegenheiten und machte den Fall aktenkundig.

Der Polizeipräsident kam zu dem Ergebnis, dass der LKA-Mitarbeiter die Abfrage nicht für private Zwecke durchgeführt habe. Er habe in einem gesamtpolizeilichen Auftrag gehandelt, also strafbare und ordnungswidrige Handlungen zu erforschen und zu bekämpfen (Repression) sowie Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren (Prävention). Der Beamte habe durch seine Feststellungen und durchgeführten Tätigkeiten sowohl der vom beschädigten PKW ausgehenden Verletzungsgefahr entgegenwirken als auch den Verdacht auf Straftaten im Zusammenhang mit dem PKW bzw. zum Nachteil des Fahrzeugeigentümers verhindern wollen. Es handele sich dabei um die Wahrnehmung von Aufgaben der Gefahrenabwehr, wie sie jedem Polizeibeamten allgemein zugewiesen seien. Die Halterabfragen seien für die Aufgabenerfüllung erforderlich gewesen.

Bei der rechtlichen Bewertung ist zu unterscheiden zwischen den ersten und den weitergehenden Ermittlungen des Polizisten. Die Verifizierung des Sachverhaltes nebst ersten Ermittlungen hierzu kann noch seiner Aufgabe zur Gefahrenabwehr im Sinne eines gesamtpolizeilichen Auftrags zugeschrieben werden. Die Polizei kann personenbezogene Daten in einer von ihr automatisiert geführten Datei abfragen und mit deren Inhalt abgleichen, wenn Tatsachen die Annahme rechtfertigen, dass dies für die Erfüllung einer bestimmten ordnungsbehördlichen oder polizeilichen Aufgabe im Rahmen der Zweckbestimmung dieser Datei erforderlich ist.[87]

Spätestens dann ist im zweiten Schritt der Vorgang an die zuständige Stelle zur weiteren Bearbeitung abzugeben. Der Polizeipräsident hat insoweit einen dienstrechtlichen Verstoß des Polizisten gegen interne Handlungsanweisungen eingeräumt. Der Beamte hat sich im Übereifer über die festgelegte Aufgabenverteilung hinweggesetzt.

Jeder Polizist darf nach dem ASOG nur rechtmäßig erhobene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit das zur Erfüllung seiner Aufgaben oder zur Vorgangsverwaltung erforderlich ist.[88] Der zweite Zugriff des Beamten auf polizeiliche Datenbanken zur erneuten Identitätsfeststellung, um den Halter anzuschreiben, war unzulässig, weil er für diese Aufgabe nach der internen Geschäftsverteilung nicht zuständig war.

Polizeibedienstete dürfen die im Polizeilichen Informationssystem gespeicherten Daten nur im Rahmen der ihnen durch Geschäftsverteilung zugewiesenen Aufgaben im erforderlichen Umfang abrufen.

3.2 Internet-Wache

Auf dem Portal der Internet-Wache der Polizei kann jeder eine Online-Strafanzeige erstatten oder mit einer einfachen Sachverhaltsschilderung der Polizei einen Vorgang zur Kenntnis geben. Bei der Erstattung einer Strafanzeige ist die Angabe von Name und Anschrift erforderlich. Die Sachverhaltsschilderung dagegen kann ohne Angaben eigener personenbezogener Daten abgeschickt werden. Nun sollte aber keiner glauben, dass die Identität des Absenders nicht festgestellt werden kann.

Ein Petent hatte sich anstelle eines Briefes ohne Angabe seines Namens entschlossen, der Polizei bestimmte Informationen aus dem Bereich der organisierten Kriminalität über den Weg der Sachverhaltsdarstellung online zur Kenntnis zu bringen. Dabei wollte er bewusst keine weiteren Angaben zur Person machen, weil er Gewalt- und Racheakte fürchtete. Er schrieb ausdrücklich, dass seine Angaben anonym zu behandeln seien.

Tatsächlich hielt die Polizei den Sachverhalt für so bedeutend, dass sie Maßnahmen treffen wollte, die richterlich angeordnet werden müssen. Der Richter verfügte vor einer Entscheidung über den Antrag, dass Informationen über die Nutzerkennung der IP-Adresse des anonymen Hinweisgebers ermittelt werden sollen, um über dessen Identität weitere Informationen zu erhalten. So wurde der Petent ausfindig gemacht, und sein Name stand nun in den Ermittlungsakten. Im Falle einer Akteneinsicht wäre dem Verteidiger des Beschuldigten die Identität des Anzeigenden bekannt geworden.

Die Staatsanwaltschaft vertritt den Standpunkt, ein Informant sei zugleich Zeuge, insofern ein wichtiges Beweismittel. Die Ermittlung aller be- und entlastenden Umstände sei originäre Aufgabe der Staatsanwaltschaft.[89] Zu diesen Ermittlungen gehöre die Namhaftmachung von bisher unbekannten Zeugen. Auf deren entgegenstehenden Willen komme es dabei grundsätzlich nicht an.[90]

Sofern Zeugen begründet geltend machen, anonym bleiben zu müssen, da ansonsten eine Gefährdung vorliegt, werden die entsprechenden Daten in der Handakte geführt, die dem Verteidiger und dem Beschuldigten nicht zugänglich ist. Akteneinsicht wird dann nur in einer entsprechend teilgeschwärzten Akte gewährt. Der Umfang der Schwärzung hängt dabei vom Grad der Gefährdung ab, da auch der Beschuldigte im Rahmen eines fairen Verfahrens die

87 § 28 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG)
88 § 42 Abs. 1 ASOG
89 § 160 StPO
90 § 48 StPO

Möglichkeit haben muss, sich gegen Tatvorwürfe konkret verteidigen und mit den gegen ihn erhobenen Beweisen auseinandersetzen zu können.[91]

Das Verfahren wurde nach § 170 Abs. 2 StPO eingestellt. Die Beschuldigten haben keine Kenntnis vom Verfahren erhalten. Eine Datenweitergabe ist nicht erfolgt. Im Falle einer möglicherweise noch erfolgenden Akteneinsicht obliegt es der Staatsanwaltschaft, mögliche schutzwürdige Akteninhalte vorher zu entfernen. Eine grundsätzliche Löschung der Daten aus der Akte ist aufgrund der Notwendigkeit der Aktenwahrheit nicht möglich.

Der Polizei haben wir empfohlen, auf dem Portal der Internet-Wache einen deutlichen Hinweis darauf anzubringen, dass die Vertraulichkeit und Anonymität trotz des äußeren Anscheins nicht gewährleistet werden kann. Die scheinbar anonyme Eingabe in das Portal Internet-Wache der Polizei ist ohnehin nur pseudonym, da durch die IP-Adresse rückverfolgt werden kann, von welchem Rechner aus die Eingabe getätigt wurde. Das bisherige E-Mail-basierte System wird demnächst durch ein mehrschichtiges und hoch verfügbares Softwaresystem abgelöst. Im Rahmen dieses Projektes wird ein entsprechender Hinweis auf den Umfang der Vertraulichkeit der Angaben entwickelt und bei der Einführung der neuen Internet-Wache veröffentlicht.

Wer anonym bleiben will, sollte sich mit einem konventionellen Brief ohne Absenderangaben an die Ermittlungsbehörden wenden. Auch ohne Angaben zur eigenen Person muss eine an die Internet-Wache gerichtete Sachverhaltsdarstellung nicht anonym bleiben.

3.3 PRISM beim Verfassungsschutz?

Im Juni berichtete die Presse aufgrund der Enthüllungen von Edward Snowden erstmals über das Programm PRISM, mit dem der Auslandsgeheimdienst der USA (National Security Agency – NSA) weltweit flächendeckend Meta- und Inhaltsdaten insbesondere im Internet erfasst. Deutschland ist eines der Hauptziele der NSA. Ebenfalls meldete die Presse, dass deutsche Dienste an der Überwachung der deutschen Bevölkerung beteiligt sind. Nach eigenen Angaben sammeln die USA auf Grundlage einer richterlichen Anordnung im Rahmen von PRISM Kommunikationsdaten Verdächtiger in den Bereichen Terrorismus, organisierte Kriminalität und zur Gewährleistung der nationalen Sicherheit.[92] PRISM ist auf die globale Kommunikation ausgelegt und betrifft primär Daten von nicht-amerikanischen Telekommunikationsteilnehmern.[93]

Aufgrund der möglichen außenpolitischen Relevanz sind die Kontaktaufnahme zu ausländischen Nachrichtendiensten und ausländischen Stellen und mögliche Datenübermittlungen an diese eine Bundesangelegenheit. Informationen, die aus dem Ausland übermittelt werden, erreichen den Berliner Verfassungsschutz ausschließlich durch die Übermittlung der zuständigen Bundesbehörden (z.B. Bundesamt für Verfassungsschutz). Diese enthalten keine Angaben über die Art und Weise der Kenntniserlangung, sodass auch eine Bezugnahme auf PRISM als mögliche Ursprungsquelle nicht erfolgt. Eine selbständige Übermittlung von Informationen durch den Berliner Verfassungsschutz an ausländische Nachrichtendienste findet nach dessen Angaben nicht statt.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert die Bundesbehörden, die mit nachrichtendienstlichen Befugnissen ausgestattet sind.[94] Allerdings hat er bekannt gegeben, dass das Bundesministerium des Innern seine Fragen zur Einbeziehung deutscher Behörden in PRISM und zu dem britischen Geheimdienstprojekt „TEMPORA“ sowie der Nutzung des Spähanalysewerkzeuges „XKeyscore“ mit dem unzutreffenden Verweis auf die Zuständigkeit der vierköpfigen G10-Kommission des Deutschen Bundestages nicht beantwortet hat.[95] Die Kontrolle der Nachrichtendienste muss dringend intensiviert werden. Der Austausch von Erkenntnissen zwischen den Nachrichtendiensten darf nicht dazu führen, dass der verfassungsrechtliche Schutz der eigenen Bevölkerung unterlaufen wird und die Bürgerinnen und Bürger schutzlos den Geheimdiensten anderer Länder ausgeliefert sind. Eine freie Kommunikation ist so nicht mehr gewährleistet, das Internet wird zu einer weltweiten Überwachungsplattform.

91 Art. 6 Europäische Menschenrechtskonvention (EMRK)

92 Rechtsgrundlage ist Section 702 Foreign Intelligence Surveillance Act (FISA).
93 Siehe Einleitung und 2.2
94 § 24 Abs. 1 BDSG
95 Pressemitteilung des BfDI vom 11. Juli 2013

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Verbesserungen bei der Kontrolle der Nachrichtendienste gefordert.[96] Völkerrechtliche Abkommen dürfen nur abgeschlossen werden, wenn ein umfassender Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert werden. Zu prüfen ist auch der Aufbau alternativer, möglichst dezentral gehaltener Netzstrukturen.

Mit grenzenloser Überwachung im Geheimen wird lediglich die Illusion einer absoluten Sicherheit gewährt, während real die Freiheitsrechte sabotiert werden. Neben einer besseren Kontrolle der Nachrichtendienste müssen internationale Regelungen zur Begrenzung staatlicher Datensammelwut und Spionage geschaffen werden.

3.4 Sieben Jahre Warten – und kein Ende in Sicht

Seit 2003 beobachteten Vertrauensleute des Verfassungsschutzes und des Bundesamts für Verfassungsschutz die „Initiative für ein Berliner Sozialforum“ (BSF). Ein an diesem Forum teilnehmender Sozialwissenschaftler beantragte 2006 beim Verfassungsschutz Auskunft über die zu seiner Person gespeicherten Informationen. Die Behörde teilte dem Sozialwissenschaftler nur mit, dass zu seiner Person im Rahmen der Beobachtung linksextremistischer Bestrebungen Informationen in Unterlagen und der amtsinternen Datei gespeichert seien. Einsicht in die Unterlagen könne ihm „aus Gründen des Schutzes der Arbeitsweise, Nachrichtenzugänge und schutzwürdigen Interessen Dritter“ nicht erteilt werden. Daraufhin erhob der Betroffene Klage, um weitergehende Auskünfte und Akteneinsicht zu erhalten. Im Berufungsverfahren wies das Oberverwaltungsgericht (OVG) Berlin-Brandenburg 2011 die Klage ab. Maßgebend hierfür waren prozessuale Gründe, die das Gericht zuungunsten des Betroffenen berücksichtigte. Der Betroffene hatte nämlich versäumt, einen Antrag auf Einleitung eines sog. In-camera-Verfahrens zu stellen.[97] In einem solchen Verfahren prüft das OVG nach Vorlage der Akten, ob die geltend gemachten Geheimhaltungsgründe tatsächlich vorliegen. Das Bundesverwaltungsgericht hob diese Entscheidung auf und verwies die Klage an das OVG zurück.[98] Es bestehe keine Obliegenheit des Betroffenen, ein solches In-camera-Verfahren zu beantragen. Nun muss das OVG erneut entscheiden, ob der Verfassungsschutz dem Betroffenen Auskunft und Akteneinsicht gewähren muss.[99]

Es ist zu hoffen, das über den 2006 beim Verfassungsschutz gestellten Antrag auf Akteneinsicht und Auskunft bald abschließend inhaltlich entschieden wird.

3.5 Übersichtsaufnahmen bei Versammlungen

Das Verwaltungsgericht Berlin hat 2010 festgestellt, dass die Beobachtung einer Versammlung durch die Polizei mittels einer Kamera und die Übertragung der Bilder in die Einsatzleitstelle ohne Einwilligung der an der Versammlung Teilnehmenden einen Eingriff in die Versammlungsfreiheit und das Recht auf informationelle Selbstbestimmung darstellen.[100] Dafür bedarf es einer gesetzlichen Grundlage.[101]

Damit bestätigte das Verwaltungsgericht unseren schon früher vertretenen Standpunkt.[102] Mit dem Gesetz über Aufnahmen und Aufzeichnungen von Bild und Ton bei Versammlungen unter freiem Himmel und Aufzügen hat das Abgeordnetenhaus nun eine Rechtsgrundlage dafür geschaffen.[103] In der Anhörung im Ausschuss für Inneres, Sicherheit und Ordnung haben wir dar-

96 Entschließung vom 5. September 2013: Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen, Dokumentenband 2013, S. 18 siehe auch den Bericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an den Deutschen Bundestag zu Abhöraktivitäten US-amerikanischer Nachrichtendienste in Deutschland vom 15. November 2013, BT-Drs. 18/59

97 § 99 Abs. 2 VwGO
98 Entscheidung vom 30. Oktober 2013 – BVerwG 6 C 22.12
99 §§ 31 und 32 Gesetz über den Verfassungsschutz in Berlin
100 Entscheidung vom 5. Juli 2010 – VG 1 K 905.09
101 §§ 12 a, 19 a
102 JB 2009, 3.5
103 GVBl., S. 103

auf hingewiesen, dass die Anwendung der Vorschriften überprüfbar sein muss.[104] Um die notwendige Transparenz herzustellen, sollte kein heimlicher Wechsel zwischen den Ermächtigungsgrundlagen möglich sein. Deshalb sollten unterschiedliche Techniken (Kamerasysteme) eingesetzt werden, die entweder die nicht gespeicherten Übersichtsaufnahmen oder speicherbare Aufnahmen von Einzelpersonen machen. Letztere sind nur zulässig bei solchen Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie die öffentliche Sicherheit oder Ordnung erheblich gefährden.

Grundrechtseingriffe sind nur aufgrund gesetzlicher Regelungen zulässig; die Kontrolle ihrer Rechtmäßigkeit muss technisch-organisatorisch unterstützt werden.

3.6 Meldedatenabgleich beim Zensus

Aus der Praxis

Beim Mikrozensus 2011 stellte sich heraus, dass in Berlin etwa 180.000 Menschen weniger leben als im Melderegister gespeichert sind. Der Bezirk Charlottenburg-Wilmersdorf war davon am stärksten betroffen. Die Einwohnerdaten sind für Behördenentscheidungen (z.B. die Zuschneidung von Wahlkreisen oder Einschulungsbereichen) unerlässlich. Deshalb wollte sich der Stadtrat die Grunddaten von 1.000 nach dem Zufallsprinzip ausgewählten Einwohnerinnen und Einwohnern des Bezirks vom Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) übermitteln lassen. Diese sollten dann von Bezirksamtsbediensteten besucht werden, um festzustellen, ob sie noch unter der im Melderegister gespeicherten Adresse leben.

Die Meldebehörde darf einer anderen Behörde oder sonstigen öffentlichen Stelle für eine Gruppenauskunft aus dem Melderegister bestimmte Daten von namentlich nicht bezeichneten Einwohnern übermitteln, soweit dies zur Erfüllung von in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist.[105] Weder die Voraussetzung der Zuständigkeit noch die Erforderlichkeit ist erfüllt. Es ist weder Aufgabe des LABO noch des Bezirksamtes, statistische Erhebungen des Amts für Statistik Berlin-Brandenburg zu überprüfen.

Auch ist im vorliegenden Fall die Datenübermittlung für den beabsichtigten Zweck der Kontrolle des Zensus nicht erforderlich. Die geplante Stichprobe und die Besuche bei den Bürgern sind keine mathematisch taugliche Methode, um eine womöglich nicht ordnungsgemäße Durchführung des Zensus zu belegen. Um die Umgehung der Prinzipien Objektivität, Neutralität und wissenschaftliche Unabhängigkeit nachzuweisen, ist diese willkürlich geplante Methode der stichprobenartigen Untersuchung ungeeignet.

Eine Überprüfung der Meldeverhältnisse von Amts wegen wäre zwar grundsätzlich zulässig, würde aber konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit des Melderegisters hinsichtlich einzelner oder einer Vielzahl namentlich bekannter Einwohnerinnen und Einwohner voraussetzen.[106] Die zufällige Auswahl von 1.000 im Bezirk wohnhaften Personen erfüllt diese Voraussetzungen nicht.

Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil festgestellt, dass eine Kombination der Volkszählung für statistische Zwecke mit einem Melderegisterabgleich wegen des Eingriffs in das Recht auf informationelle Selbstbestimmung[107] verfassungswidrig ist.[108] Ein solcher Abgleich und erst recht Besuche als Konsequenz eines unwillkommenen Zensusergebnisses und ohne konkrete Anhaltspunkte für Verletzungen der Meldepflicht würden daher gegen das Grundgesetz verstoßen.

Das Land Berlin hat mittlerweile Widerspruch gegen die Feststellung der Einwohnerzahl durch das Statistische Bundesamt eingelegt.

Es ist nicht Aufgabe der Bezirksämter, die Validität amtlicher statistischer Erhebungen – noch dazu mit untauglichen Mitteln – zu überprüfen.

104 Sitzung vom 4. März 2013, siehe Wortprotokoll 17/24
105 § 25 Abs. 1 MeldeG
106 § 3a Abs. 2 MeldeG
107 Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG
108 Entscheidung vom 15. Dezember 1983, siehe BVerfGE 65, 1

3.7 ODIS

Das Verfahren ODIS ist ein Teilprojekt der Online-Datenbank des Standesamts I in Berlin. Dabei handelt es sich um ein bundesweit bereitgestelltes und einsehbares Zentralverzeichnis aller Auslandspersonenstandsfälle, auf das alle Standesämter im Bundesgebiet zugreifen können. Wir haben das Projekt bis zur Produktivsetzung begleitet.

Ein Hinweis des Landesbeauftragten für Datenschutz Baden-Württemberg veranlasste uns nunmehr zu einer Kontrolle. Während der Kontrollmaßnahme wurden Abweichungen zu den uns vorliegenden Sicherheits- und Betriebskonzepten in zwei Punkten festgestellt.

Für die Auswertungsdateien wurden zu weitgehende Zugriffsrechte vergeben. Administratoren in den dezentralen Standesämtern war es möglich, Einblick auf Aktivitäten außerhalb ihres Zuständigkeitsbereichs zu erhalten.

Die technischen Vorgaben bei der Auswahl von Passwörtern durch die Benutzer waren unzureichend, so dass unsichere Passwörter gewählt werden konnten. Datenschutzkonforme Systeme überprüfen die regelgerechte Bildung von Passwörtern und weisen diese bei Abweichung ab. Die Mindestlänge sollte dabei acht Zeichen, mindestens aber sechs betragen und aus einem alphanumerischen Zeichenmix mit mindestens einem Sonderzeichen gebildet werden. Ein Wechsel ist zyklisch ca. alle 90 Tage vorzuschreiben, und die Wiederverwendung eines bereits benutzten Passworts sollte erst nach mindestens fünf Wechseln wieder ermöglicht werden.[109]

Die verfahrensverantwortliche Stelle im LABO nahm die Hinweise auf und hat uns über die Behebung der festgestellten Mängel informiert.

Je stärker Verzeichnisse – etwa im Bereich der Standesämter – bundesweit zentralisiert werden, desto wichtiger wird die korrekte Vergabe von Zugriffsrechten und die Passwortsicherheit.

109 Ausführliche Hinweise sind unserem Ratgeber Nr. 3 – Empfehlungen für die Vergabe von Passwörtern zu entnehmen, siehe http://www.datenschutz-berlin.de/attachments/522/Ratgeber_Nr3_2008.pdf?1222349975

3.8 Ausländische Eltern fußballbegeisterter Kinder

Der Berliner Fußballverband (BFV) verlangt bei der Erstanmeldung oder einem Vereinswechsel junger minderjähriger Spieler mit Migrationshintergrund unter Berufung auf das Reglement des Weltfußballverbandes (FIFA) bezüglich Status und Transfer von Spielern von den Eltern die Vorlage der Arbeitsverträge, Arbeitserlaubnisse, Identitäts- und Nationalitätsnachweise oder Meldebescheinigungen, um nachprüfen zu können, ob sie sich nicht allein wegen einer Fußballkariere des Kindes in Deutschland aufhalten.

Der BFV hat auf Missbrauchsfälle in der Vergangenheit insbesondere bei interkontinentalen Transfers von Spielern hingewiesen. Um Betrug, Geldwäsche oder Menschenhandel vorzubeugen, habe die FIFA ein komplexes System entwickelt, das derartige Fälle ausschließen soll. Gerade im Bereich des Jugendfußballs wolle man bei Wechseln aus Südamerika und Afrika Missbrauch und Ausbeutung verhindern. So seien Jugendliche und ihre Eltern zum Teil mit finanziellen Versprechungen nach Europa gelockt worden. Wenn sie die Erwartungen an die sportlichen Leistungen nicht erfüllen könnten, seien sie ohne Unterstützung sich selbst überlassen worden.

Die FIFA-Regularien werden beim Wechsel oder Beitritt in einen Verein aus dem Profibereich angewendet (obere vier Spielklassen). Die Vorlage der Dokumente dient dem Nachweis, dass nicht der finanzielle Unterhalt der Familie der Beweggrund des Beitritts oder Wechsels ist.

Bei den FIFA-Vorschriften handelt es sich um Satzungsrecht, das gegenüber gesetzlichen Regelungen nachrangig ist. Das BDSG erlaubt das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.[110] Der Schutz Minderjähriger ist ein berechtigtes Interesse auch eines Sportverbandes. Dieses rechtfertigt aber keine unbegrenzte und damit unverhältnismäßige

110 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Datenerhebung und weitere -verarbeitung. Sie muss im Einzelfall erforderlich sein. Gerade in Berlin mit zahlreichen Jugendlichen mit Migrationshintergrund wirken die Vorlagepflichten befremdend. Es geht um Jugendliche, die überwiegend hier geboren sind und Fußball spielen wollen.

In der Ausländerbehörde werden wichtige, insbesondere den Aufenthaltsstatus betreffende Fragen geklärt. Nicht hinreichend deutlich wird, warum ein Sportverband Kindern wegen ihrer Herkunft Hürden beim Zugang zu den Vereinen aufbaut, wenn die dafür verantwortlichen staatlichen Stellen keine Einwände gegen einen Aufenthalt in Deutschland haben. Bei allem Verständnis für das Ziel „Minderjährigenschutz“ geht dieses Verlangen zur Offenbarung von Einzelheiten aus dem Privatleben zu weit.

Nach einem Gespräch mit Vertretern der FIFA und des DFB hält die FIFA die Vorlage der Dokumente durch die Eltern nicht mehr bei jedem Vereinsbeitritt eines Jugendlichen für erforderlich. Wir haben angeregt, die Intensität der Prüfungen an das Missbrauchsrisiko anzupassen. Außerdem sollte grundsätzlich eine Versicherung der Eltern ausreichen, dass ein Vereins- oder Wohnortwechsel nicht vor dem Hintergrund einer Fußballkariere erfolgt. Bei konkreten Anhaltspunkten für einen Missbrauch kann dann abgestuft ein Überprüfungsverfahren eingeleitet werden.

Die Zulässigkeit und der Umfang der Datenerhebung und -speicherung beim Fußballverein oder dem Verband sind am BDSG zu messen. Die FIFA-Vorschriften sind als Satzungsrecht nachrangig.

3.9 Zoff bei „Union“ – Anteilseigner im Handelsregister

Die „An der Alten Försterei“ Stadionbetriebs AG hat bei einer Kapitalerhöhung mit Zeichnungsscheinen gearbeitet, die personenbezogene Daten wie z.B. E-Mail-Adressen, Geburtsdaten, Anschriften, Personalausweis- und Telefonnummern, aber auch Bankkontodaten der Zeichner enthielten. Die Scheine wurden als Zweitschriften beim Registergericht eingereicht und dadurch über das elektronische Handelsregister öffentlich zugänglich.

Die Stadionbetriebs AG berief sich zunächst darauf, dass der Zeichnungsschein zugleich eine Einwilligungserklärung in die Datenverarbeitung enthalten habe. Diese war aber nicht hinreichend bestimmt und informierte nur unzureichend. Die Zeichnenden konnten aus ihr nicht schließen, dass die zum Teil sensitiven personenbezogenen Daten im Handelsregister veröffentlicht werden.

Die Übermittlung der Überschussdaten an das Registergericht kann auch nicht auf eine Rechtsvorschrift gestützt werden. Das Aktiengesetz legt lediglich fest, dass formale Vorgaben zur Aktie und die Kapitalgesellschaft auf dem Zeichnungsschein erfasst werden. Von weitreichender Erfassung personenbezogener Daten der Zeichnenden ist nicht die Rede.

Mangels wirksamer Einwilligung und Erlaubnisnorm war die Datenübermittlung rechtswidrig. Darüber hinaus ist die Stadionbetriebs AG ihrer Informationspflicht bei unrechtmäßiger Übermittlung von Daten (hier: Bankdaten) nicht nachgekommen.[111] Inzwischen sind die personenbezogenen Zeichnungsscheine der Anteilseigner nicht mehr öffentlich abrufbar.

Eine Einwilligungserklärung ist nur dann wirksam, wenn sie hinreichend bestimmt ist und die bzw. der Betroffene über die weitere Datenverarbeitung informiert wird. Das gilt insbesondere dann, wenn die Daten veröffentlicht werden sollen.

111 § 42a BDSG

4 Verkehr

4.1 Neue Technologien im Auto

Aus der Praxis

Der technische Fortschritt nimmt auch im Automobilbereich stetig zu. Mit den Verbesserungen für die Verkehrssicherheit und erhöhtem Komfort für die Nutzer moderner Fahrzeuge gehen mitunter auch Datenschutzrisiken einher, da einige der neuen Technologien zunehmend Daten über die fahrende Person erfassen und dadurch z.B. die Erstellung von Bewegungs- oder Nutzungsprofilen begünstigen.

So mussten wir feststellen, dass Autovermieter mitunter ihre vermieteten Fahrzeuge per GPS überwachten, ohne jedoch die Kunden vorab hierüber zu informieren und deren Einwilligung einzuholen.[112] Auch das ab Oktober 2015 in Europa verpflichtend für alle neuen Pkw-Modelle und leichte Nutzfahrzeuge vorgeschriebene Notrufsystem „eCall" nutzt Techniken zur Positionsbestimmung. Das System ermöglicht, bei einem Unfall das Fahrzeug automatisch zu lokalisieren und mit der fahrenden Person über eine Funkeinheit zu kommunizieren, die im Auto mit einem Ortungssystem verbaut ist. Das „eCall"-System soll aufgrund der Empfehlungen der Art. 29-Datenschutzgruppe so ausgestaltet werden, dass die mit entsprechenden Bordgeräten ausgestatteten Fahrzeuge im Normalbetrieb „nicht verfolgbar" sind. Bei Auslösung eines Notrufs beim Unfall soll lediglich ein Mindestdatensatz an die Notrufabfragestelle geschickt werden.[113] Allerdings hat es der Innenausschuss des Europaparlaments Anfang 2014 bedauerlicherweise abgelehnt, den Betroffenen die Möglichkeit zur fallweisen Abschaltung zu geben.

Durch den Einsatz kooperativer Systeme, bei denen eine Vielzahl von Fahrzeugen miteinander und mit einer Verkehrsleitzentrale kommuniziert, kann der Fahrer frühzeitig vor Staus gewarnt werden, das Navigationssystem berechnet umgehend eine geeignete Alternativroute, das Bordsystem warnt vor möglichen Gefahren auf der Strecke und sucht auf Wunsch den nächsten freien Park-

112 Siehe http://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-gps-ortung-von-mietwagen.html

113 Erwägungsgrund (9) der delegierten Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012, ABl. L 91 vom 3. April 2013, S. 1 ff.

platz. Erste Einsätze dieser sog. Car-to-X-Kommunikation in der Serienproduktion von Ober- und Mittelklassewagen deutscher Hersteller sind ebenfalls ab 2015 geplant. Mit Hilfe von Smartphones lässt sich inzwischen bei einigen Fahrzeugmodellen nicht nur die Navigation per Sprache steuern. Selbst die Abstimmung der Fahrwerksdämpfung oder das autonome Suchen eines Stellplatzes inklusive des Parkvorgangs lassen sich über entsprechende Anwendungen bereits realisieren. Soweit hierfür überhaupt personenbezogene Daten im Fahrzeug gespeichert werden müssen, dürfen sie nicht ohne Zustimmung des Fahrers ausgelesen werden können.

Im Sinne der Verbesserung der Verkehrssicherheit für schnellere Hilfe bei Unfällen, zur Verringerung von Staus und für den erhöhten Komfort der Kunden sind viele der neuen Technologien im Automobilbereich durchaus begrüßenswert. Jedoch müssen die möglichen Risiken für den Datenschutz begrenzt werden. Eine permanente Überwachung des Fahrzeugstandorts ermöglicht die Erstellung von Bewegungsprofilen. Datenvermeidung, Datensparsamkeit wie auch ein Mindestmaß an Transparenz sind deshalb bei der Entwicklung solcher Systeme zu berücksichtigen.

4.2 „Pay as you drive" – der Versicherer fährt mit

Aus der Praxis

Nachdem es in anderen Ländern wie Großbritannien, Italien und den USA bereits seit einiger Zeit Versicherungsangebote für Autofahrer gibt, welche mit Hilfe eines Telematiksystems den Fahrstil überwachen und aufbauend darauf die Prämie für die Kfz-Versicherung kalkulieren, sollen entsprechende Angebote ab 2014 auch in Deutschland auf den Markt kommen.

Die Systeme zeichnen neben allgemeinen Fahrtdaten (z.B. genaue Anzahl gefahrener Kilometer im Jahr) permanent das Verhalten der fahrenden Person im Verkehr auf, z.B. ob oftmals stark beschleunigt oder abrupt abgebremst wird, wie hoch die Durchschnittsgeschwindigkeit ist, wie das Lenkverhalten aussieht und ob Kurven langsam oder rasant durchfahren werden. Nach Auskunft eines Unternehmens aus der Versicherungsbranche „könnten Informationen zu Zeit

und Ort der Fahrt“ ebenso von Interesse sein. Aufgrund neuerer Fahrassistenzsysteme (wie z.B. der Messung des Abstands zu einem vorausfahrenden Fahrzeug oder der Beobachtung der Spurhaltung des Wagens) sind auch weitere Anpassungen des Systems denkbar, die eine noch umfassendere Beobachtung des Fahrverhaltens zuließen. Die gewonnenen Daten der Verkehrstelematik werden dazu genutzt, ein Risikoprofil der Autofahrerin bzw. des Autofahrers zu erstellen und anhand dessen eine genauere Prämienberechnung für die Kfz-Versicherung vornehmen zu können. Hierbei haben sich zwei verschiedene Systeme zur Erstellung der entsprechenden Verhaltensprofile etabliert. Entweder werden die Daten direkt im Fahrzeug durch ein entsprechendes Zusatzgerät erfasst und an den Versicherer übertragen oder die gemessenen Rohdaten können an einen Dienstleister übermittelt werden, der die Aufbereitung der Profile übernimmt und diese an die Versicherung weiterleitet. Bei entsprechend sicherer Ausgestaltung der Technik ist es möglich, diese so zu konzipieren, dass der Versicherer selbst keinen Zugriff auf die Rohdaten hat, sondern nur aggregierte Daten erhält. In der Praxis lässt sich dies von den Nutzenden jedoch nicht kontrollieren, sodass ein Risiko hinsichtlich des Umgangs mit den personenbezogenen Daten bestehen bleibt.

Anbieter der Technik sowie Vertreter der Versicherungsbranche argumentieren oft damit, dass sich laut statistischen Untersuchungen die Fahrer bei Telematiktarifen vorsichtiger im Verkehr bewegen würden, da ihnen bewusst ist, dass ihr Fahrstil überwacht und somit eine defensivere Fahrweise belohnt wird. Gleichzeitig würde dies bei vielen Nutzenden auch zu günstigeren Versicherungsprämien aufgrund sinkender Unfallzahlen führen. All dies geht jedoch stets mit einer Gefahr für die Beeinträchtigung der Privatsphäre der Nutzer solcher Tarife einher, da hier sehr umfassende personenbeziehbare Daten gewonnen werden, deren sorgfältiger Schutz nicht immer eindeutig überprüft werden kann.

Anhand der gewonnenen Daten lassen sich umfangreiche Bewegungs- und Nutzungsprofile erstellen, welche abhängig vom Fahrstil auch zu steigenden Versicherungsprämien führen können. Darüber hinaus muss darauf geachtet werden, welche Stellen Zugriff auf die gewonnenen Daten erhalten und ob hier der Schutz der personenbezogenen Daten stets in vollem Umfang gewahrt ist.

4.3 Fahrzeugkameras im Straßenverkehr

4.3.1 Videoüberwachung durch Autovermieter

Aus der Praxis

Wir wurden auf einen Autovermieter hingewiesen, der in seinen Mietwagen kleine versteckte Kameras installiert hatte. Eine Prüfung vor Ort hat ergeben, dass der Fahrzeuginnenraum nicht überwacht wurde. Die Kameras sollten aber ohne Wissen der Kunden die Straße vor und hinter dem Fahrzeug filmen. Das Unternehmen versprach sich davon, Fälle von Versicherungsbetrug aufklären zu können. Auch für Taxigewerbe hat die Versicherungsbranche den Einsatz solcher Kameras angeregt.

Der Einsatz solcher Fahrzeugkameras ist grundsätzlich unzulässig. Das Bundesverfassungsgericht hat bereits 1983 festgestellt, dass mit dem Grundgesetz eine Gesellschafts- und Rechtsordnung unvereinbar wäre, in der der Bürger nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß (Recht auf informationelle Selbstbestimmung).[114] Dieses Recht umfasst die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung zu werden. Daher sieht das Bundesdatenschutzgesetz vor, dass Videoüberwachung transparent erfolgen muss, damit die oder der Betroffene die Möglichkeit hat, der Überwachung auszuweichen bzw. Auskunfts- oder Löschungsrechte geltend zu machen.

Die **heimliche Videoüberwachung** ist grundsätzlich unzulässig. Sie ist in der Regel staatlichen Organen zur Abwehr schwerwiegender Gefahren oder zur Strafverfolgung vorbehalten. Deshalb sind Videoüberwachungsanlagen normalerweise mit einem entsprechenden Hinweis zu versehen.[115] Diese Hinweispflicht ist an einem fahrenden Auto kaum zu realisieren. Jeder Passant müsste damit rechnen, dass ein entsprechend ausgestattetes Fahrzeug um die Ecke biegt und solche Videoaufnahmen anfertigt. Zwar kann es immer vorkommen, dass Passanten auch ungewollt – z.B. von Touristen mit Smartphones oder Videokameras – gefilmt oder fotografiert werden. Dabei handelt es sich

114 „Volkszählungsurteil“ vom 15. Dezember 1983, siehe BVerfGE 65,1 ff.
115 § 6 b Abs. 2 BDSG

aber in der Regel um eine Datenverarbeitung zu persönlichen und familiären Zwecken, die nicht unserer Kontrolle unterliegt. Es hat aber eine andere Qualität, wenn Unternehmen wie Autovermietungen, Versicherungen oder Taxigewerbe[116] diese Daten zu geschäftlichen Zwecken erheben oder verarbeiten.

Außenkameras an Fahrzeugen sind nicht mit den Vorgaben des Bundesdatenschutzgesetzes vereinbar.

4.3.2 Dashcams in Fahrzeugen

Wir sind darauf aufmerksam geworden, dass immer mehr Autofahrerinnen und Autofahrer sog. Dashcams in ihren Fahrzeugen installieren. Darunter sind kleine Videokameras zu verstehen, die üblicherweise auf dem Armaturenbrett angebracht werden und das öffentliche Straßenland filmen.

Wir stehen dieser Praxis sehr kritisch gegenüber, da in einer freiheitlichen Gesellschaft grundsätzlich die Möglichkeit bestehen muss, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt gefilmt zu werden.[117] Wenn diese Aufnahmen allerdings von Privatpersonen zu persönlichen oder familiären Zwecken erfolgen, wird eine solche Videoüberwachung nicht vom Anwendungsbereich des Bundesdatenschutzgesetzes umfasst. In solchen Fällen fehlt uns die Handhabe, derartige Filmaufnahmen zu verhindern. Den Betroffenen bleibt allerdings die Möglichkeit, sich zivilrechtlich zu wehren, wenn z.B. das Recht am eigenen Bild[118] verletzt wurde.[119]

Dienen die Aufnahmen allerdings nicht ausschließlich privaten oder familiären Zwecken, können wir eine unzulässige Videoaufzeichnung im Einzelfall

116 Siehe Beschluss des Düsseldorfer Kreises vom 26./27. Februar 2013: Videoüberwachung in und an Taxis, Dokumentenband 2013, S. 26 In diesem Beschluss bekräftigen die Datenschutzaufsichtsbehörden auch ihre Auffassung zur Videoüberwachung in Taxis.

117 Siehe auch 4.3.1

118 § 22 Kunsturhebergesetz

119 § 1004 Abs. 1 analog, § 823 Abs. 1 BGB

unterbinden und ggf. Bußgelder verhängen. Nach höchstrichterlicher Rechtsprechung verlässt eine Datenverarbeitung z.B. dann den persönlichen und familiären Bereich, wenn personenbezogene Daten für jedermann zugänglich in das Internet eingestellt werden (sog. Internetpranger).[120] Dasselbe gilt, wenn die Aufzeichnungen als mögliches Beweismittel angefertigt werden, um sie für eine spätere Rechtsverfolgung gegenüber der betroffenen Person zu verwenden.

Wir empfehlen Autofahrerinnen und -fahrern, aus Rücksicht auf die Privatsphäre der anderen Verkehrsteilnehmenden auf den Einsatz solcher Dashcams zu verzichten. Videoaufnahmen, die nicht ausschließlich zu persönlichen und familiären Zwecken angefertigt werden, müssen sich an den strengen Vorgaben des Bundesdatenschutzgesetzes messen lassen und sind in der Regel unzulässig.

4.4 Veröffentlichung von Kundendaten im Arbeitsstättennachweis

Im November 2012 wurde der Handwerkerparkausweis eingeführt, der Handwerker dazu berechtigt, ihr Fahrzeug gebührenfrei in Parkraumbewirtschaftungszonen abzustellen. Mit dem Handwerkerparkausweis muss ein sog. Arbeitsstättennachweis für jedermann sichtbar hinter der Windschutzscheibe ausgelegt werden. Dieser musste ursprünglich den Namen des Handwerkers, seine Telefonnummer, den Namen des Kunden und seine Adresse mit genauer Bezeichnung der Etage enthalten. Gegen die Veröffentlichung der Arbeitnehmer- und Kundendaten hatten mehrere Berliner Handwerksbetriebe berechtigte Bedenken. Wir sind deshalb an die zuständige Senatsverwaltung für Stadtentwicklung und Umwelt herangetreten. Daraufhin wurde der Arbeitsstättennachweis auf die Angabe der Kundenadresse und einer Telefonnummer des Handwerksbetriebs reduziert.

120 Urteil des Europäischen Gerichtshofs vom 6. November 2003 – EuGH C 101/01 (Rs. Lindqvist)

Damit wurden allerdings nicht alle unsere Bedenken ausgeräumt. Aus der genauen Angabe der Adresse und der Etage kann jedermann mit Hilfe des Klingelschildes ablesen, bei welchem Kunden sich der Handwerker befindet. Dies kann in manchen Fällen unbedenklich, in anderen aber für die Betroffenen unangenehm sein, z.B. wenn ein Kammerjäger bestellt wurde. Das BDSG sieht vor, dass in einem solchen Fall eine Abwägung zwischen dem berechtigten Interesse an der Veröffentlichung und dem Interesse des Betroffenen an der Geheimhaltung vorgenommen werden muss.[121] Dem Handwerksbetrieb wird damit aufgebürdet, im Einzelfall entscheiden zu müssen, ob das Interesse an einem einsatzortnahen Parkplatz gegenüber dem Recht des Kunden auf informationelle Selbstbestimmung überwiegt.

Wir haben die Senatsverwaltung eindringlich darauf aufmerksam gemacht, dass wir dies nicht für eine praxistaugliche Vorgehensweise halten. Wir konnten sie aber nicht davon überzeugen, auf die Angabe der Kundenadresse und der Etage zu verzichten. Die Senatsverwaltung hält die genaue Kundenadresse für notwendig, damit das Ordnungsamt vor Ort überprüfen kann, ob dort tatsächlich ein Handwerker arbeitet oder ob der Handwerkerparkausweis missbraucht wird. Wir können dem nicht zustimmen. Das Ordnungsamt könnte z.B. den Standort des Fahrzeugs notieren und sich von dem Handwerksbetrieb im Nachhinein den Vertrag bzw. das Protokoll der Handwerksleistung vorlegen lassen, um die Parkberechtigung zu kontrollieren. Zur Kontrolle ist es also nicht erforderlich, dass jeder beliebige Dritte diese Daten einsehen kann. Außerdem ist das Ordnungsamt ohnehin nicht dazu berechtigt, die Wohnungen der Kunden zu betreten, um festzustellen, ob dort tatsächlich Bauarbeiten durchgeführt werden.

Wir raten deshalb Handwerksbetrieben, im Zweifel die jeweiligen Kunden um ihr Einverständnis zur Auslage ihrer Daten zu bitten. So können sich Handwerksbetriebe rechtlich absichern und Beschwerden ihrer Kundschaft vermeiden.

Die Senatsverwaltung sollte zukünftig auf die Eintragung von Kundendaten im Arbeitsstättennachweis verzichten. Die Angabe ist nicht erforderlich und bringt die betroffenen Handwerksbetriebe in unnötige rechtliche Schwierigkeiten.

121 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

4.5 Deutsche Bahn AG und bahn.bonus-Programm

Um den Bahnkunden auf ihre individuellen Bedürfnisse zugeschnittene Angebote machen zu können, hatte die Deutsche Bahn AG (DB AG) die Bedingungen für Teilnehmende am sog. bahn.bonus-Programm geändert; sie bat die Alt- und Neukunden um eine Zustimmung zu diesem neuen Verfahren. Das Programm sah nun insbesondere die Erhebung der personenbezogenen Reisedaten, der Fahrkarte (Preis, Abgangs- und Zielbahnhof, Gültigkeitsbeginn, Wagenklasse, Kaufdatum, Verkaufsstelle) sowie die Verarbeitung zu Marketingzwecken vor.

Die entsprechenden Informationsschreiben der DB AG an Bestands- bzw. Altkunden enthielten jedoch unklare bis irritierende Ausführungen zum Werbewiderspruch und dessen Konsequenz für die Sammlung von Bonuspunkten. Ebenso waren die entsprechenden Antragsformulare für Neukunden missverständlich und insgesamt verbesserungsbedürftig.

Unsere Forderungen nach Transparenz und Verhältnismäßigkeit der Datenerhebung und -verarbeitung hat die DB AG umgesetzt. Nunmehr gilt für die Teilnahme am bahn.bonus-Programm für Alt- und Neukunden Folgendes:

- Es ist jederzeit ein Werbewiderspruch möglich.
- Eine Sammlung von Bonuspunkten ist auch trotz Werbewiderspruchs möglich.
- Es werden keinerlei Daten an Dritte weitergegeben. Insbesondere haben auch Kooperationspartner des Programms keinen Zugriff auf die Daten.
- Es werden keine sensitiven Daten von Kunden erhoben und verarbeitet.
- Der Hinweistext im Antragsformular zum bahn.bonus-Programm wird zur besseren Lesbarkeit vergrößert und hervorgehoben.
- Handschriftlich vermerkte Widersprüche auf dem Antragsformular sind möglich und werden von der DB AG beachtet.
- Eine Profilbildung anhand der erhobenen Reisedaten findet nicht statt.
- Die Daten werden nach drei Jahren automatisch gelöscht. Die Aufbewahrungs- bzw. Speicherfrist entspricht der Gültigkeitsdauer der gesammelten Bonuspunkte.

- Der Kunde hat jederzeit die Möglichkeit, das Programm zu kündigen und die sofortige Löschung seiner Reisedaten zu verlangen.

Auch Prämienprogramme haben sich am Gebot der Datensparsamkeit, Transparenz und Verhältnismäßigkeit zu orientieren.

5 Justiz

5.1 Gesetz über den Vollzug der Sicherungsverwahrung

Im Mai 2011 erklärte das Bundesverfassungsgericht die gesetzlichen Vorgaben zur Sicherungsverwahrung für nicht vereinbar mit dem Grundgesetz. Insbesondere sah es das Freiheitsgrundrecht der Untergebrachten durch die Gesetzgebung verletzt. Das Gericht gab den Bundes- und Landesgesetzgebern auf, ein neues Gesamtkonzept der Sicherungsverwahrung zu erarbeiten. Die Senatsverwaltung für Justiz und Verbraucherschutz hat uns den Entwurf eines Gesetzes über den Vollzug der Sicherungsverwahrung in Berlin zur Stellungnahme übersandt.

In vielen Teilen des Entwurfs wurde die Zulässigkeit der Datenverarbeitung lediglich an deren Zweckmäßigkeit geknüpft. Dies widerspricht dem Grundsatz der Erforderlichkeit, wonach die Verarbeitung personenbezogener Daten nur zulässig ist, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.[122] Erschwerend kommt hinzu, dass den Regelungen oftmals nicht zu entnehmen ist, für welche verantwortliche Stelle sie gelten sollen. Nicht abschließend normiert ist z.B., welche Personen und Stellen an den Fallkonferenzen zu Vollzugs- und Eingliederungsplanungen, an den therapeutischen Maßnahmen, an Entscheidungen über Disziplinarmaßnahmen und an der Vorbereitung der Eingliederung beteiligt sind und in welchem Umfang in diesem Zusammenhang die zum Teil sehr sensitiven Daten der Untergebrachten verarbeitet werden. Wir haben darauf hingewiesen, dass es einer Klarstellung bzw. Konkretisierung der Art und des Umfangs der Verarbeitung personenbezogener Daten sowie einer genauen Benennung der jeweiligen verantwortlichen Stellen bedarf.

Möchten Untergebrachte externen ärztlichen Rat einholen, kann ihnen dies versagt werden, wenn sie die gewählte ärztliche Vertrauensperson und den ärzt-

122 Siehe § 9 Abs. 1 BlnDSG

lichen Dienst der Einrichtung nicht wechselseitig von der Schweigepflicht entbinden. Hingegen unterliegen die im Justizvollzug mit der Behandlung von Strafgefangenen befassten Ärzten ebenso wie externe Ärzte im Verhältnis zueinander der Schweigepflicht, die ohne Einwilligung des Gefangenen nur dann aufgehoben werden kann, wenn dies zum Zwecke einer zielgerichteten gemeinsamen Behandlung erforderlich ist.[123] Es ist nicht ersichtlich, weshalb bei der Sicherungsverwahrung, die im Gegensatz zum Strafvollzug nicht der Ahndung von Straftaten, sondern der Verhinderung zukünftiger Straftaten dient, strengere Maßstäbe angesetzt werden.

Unsere Empfehlungen wurden insoweit im Gesetzgebungsverfahren nicht berücksichtigt.[124] Jedoch konnten wir erreichen, dass sich Untergebrachte, die einem Beschäftigungsverhältnis außerhalb der Einrichtung nachgehen, das hierfür vorgesehene Entgelt auf ein externes Konto überweisen lassen können, sodass der Arbeitgeber keine Kenntnis von der Unterbringung erlangt, soweit dies nicht dem Vollzugsziel zuwiderläuft. Auch wurde aufgrund unseres Hinweises geregelt, dass Angehörige bei einer schweren Erkrankung des Untergebrachten nicht gegen dessen Willen benachrichtigt werden.

Der vom Bundesverfassungsgericht geforderte deutliche Abstand des Freiheitsentzugs durch Sicherungsverwahrung zum Strafvollzug (sog. Abstandsgebot) betrifft auch das Recht der Untergebrachten auf informationelle Selbstbestimmung und muss in den gesetzlichen Regelungen zur Ausgestaltung des Vollzugs durch konkrete Vorgaben zur Art und Weise der Datenverarbeitung hinreichend Beachtung finden.

5.2 Das Justizvollzugsdatenschutzgesetz im Praxistest

Im Juli 2011 trat das Justizvollzugsdatenschutzgesetz in Kraft. Wir hatten während des Gesetzgebungsverfahrens die Möglichkeit, eigene Empfehlungen einzubringen, die zum Teil übernommen wurden.[125] Nun haben wir in

123 § 51 Justizvollzugsdatenschutzgesetz
124 Siehe Berliner Sicherungsverwahrungsvollzugsgesetz vom 27. März 2013, GVBl. S. 71
125 Siehe JB 2011, 2.2.3

den Justizvollzugsanstalten (JVA) Tegel und Moabit geprüft, wie das Gesetz in der Praxis umgesetzt wird. Die Prüfung umfasste insbesondere Regelungen, die sich gegenüber der bisherigen Gesetzgebung grundlegend geändert bzw. gegen die wir im Gesetzgebungsverfahren Bedenken vorgetragen hatten.

Die JVA erheben bei der Aufnahme von Gefangenen erkennungsdienstliche Daten wie Größe, Gestalt, Haar- und Augenfarbe sowie körperliche Besonderheiten, jedoch keine biometrischen Merkmale. Hieran zeigt sich, dass die von uns bereits im Gesetzgebungsverfahren mangels Erforderlichkeit kritisierte Regelung zur Erhebung und Verarbeitung biometrischer Merkmale Gefangener in der Praxis nicht für den Vollzug benötigt wird.

Obwohl das Gesetz seit einiger Zeit in Kraft ist, wurde bisher entgegen der gesetzlichen Vorgaben[126] keine Rücksicht auf die elementaren Bedürfnisse der Gefangenen nach Wahrung ihrer Intimsphäre bei der Videoüberwachung in besonders gesicherten Hafträumen genommen. Die JVA haben zugesagt, zukünftig Bilder, die die Überwachungskamera auf den Kontrollmonitor überträgt, in den (körperlichen) Bereichen, die die Intimsphäre der Gefangenen betreffen, per Wärmebildkamera zu verpixeln.

Das Auslesen elektronischer Datenspeicher wie etwa Mobilfunkgeräte, die Gefangene unerlaubt besitzen, erfolgt in der JVA Tegel anstaltsintern. Die Daten werden unabhängig von ihrer Kernbereichsrelevanz erst am Ende des Jahres, in dem die Auslesung stattfand, gelöscht. Dies ist rechtswidrig, weil das Gesetz vorschreibt, dass Daten, die dem Kernbereich der privaten Lebensgestaltung angehören, unverzüglich zu löschen sind.[127] Zudem wird die Löschung der Daten derzeit nicht wie vorgeschrieben dokumentiert.[128] Wir werden darauf hinwirken, dass die JVA Tegel diese Praxis zeitnah ändert.

Die JVA Moabit hatte es lange Zeit versäumt, die Gefangenen wie vorgeschrieben schriftlich über die nach dem Gesetz bestehenden Offenbarungspflichten und -befugnisse der Berufsgeheimnisträger wie Ärzte und Sozialarbeiter zu

126 § 21 Abs. 3 JVollzDSG
127 § 25 Abs. 2 Satz 2 JVollzDSG
128 § 25 Abs. 2 Satz 3 JVollzDSG

unterrichten.[129] Zwischenzeitlich wurden die Aufnahmeverhandlungsprotokolle entsprechend angepasst.

Das Justizvollzugsdatenschutzgesetz hat dazu beigetragen, einen neuen Fokus auf die informationelle Selbstbestimmung der Gefangenen zu setzen. Jedoch ist zu bemängeln, dass einzelne Teile des Gesetzes über zwei Jahre nach dessen Inkrafttreten noch nicht umgesetzt wurden.

5.3 Neue Presserichtlinien für die Justiz

In den Presserichtlinien für die Berliner Justiz werden Aufbau und Aufgaben der Justizpressestellen näher geregelt. Sie enthalten konkrete Vorgaben zur Berücksichtigung der Interessen der von Auskünften an die Presse Betroffenen. Im Mai wurden die Richtlinien neu erlassen. Im Vorfeld gab uns die Senatsverwaltung für Justiz und Verbraucherschutz die Möglichkeit, Stellung zu nehmen.

Bislang hatten die Presserichtlinien festgelegt, dass Namen und ähnliche Angaben, die zur Identifizierung von Verfahrensbeteiligten geeignet sind, nur mit deren Einwilligung den Medien genannt werden dürfen. Lediglich bei Personen der Zeitgeschichte und bei Straftaten in Ausübung eines öffentlichen Amtes wurden bei entsprechender Interessenabwägung Ausnahmen zugelassen. Der Entwurf der neuen Presserichtlinien sah nunmehr zunächst anstelle der Einholung einer Einwilligung eine Anhörung der Betroffenen vor, und dies auch nur, sofern es erforderlich erschien. Es war zu befürchten, dass dies in der Praxis dazu führt, dass häufiger als bisher Namen und ähnliche Identifikationsmerkmale von Verfahrensbeteiligten von den Vertretern der Presse erfragt würden. Wie sich in der Vergangenheit gezeigt hat, kann eine Presseveröffentlichung, die eine Identifizierung von Verfahrensbeteiligten ermöglicht, im Einzelfall erhebliche Folgen für die Betroffenen haben, insbesondere bei nachträglich erwiesener Unschuld. Wir haben daher empfohlen, die bisherigen Bestimmungen beizubehalten.

129 § 57 JVollzDSG

Die Senatsverwaltung für Justiz und Verbraucherschutz folgte dieser Empfehlung nur bedingt. In den Richtlinien wird nun betont, dass identifizierende Angaben zu Verfahrensbeteiligten ohne deren vorherige Zustimmung gegenüber Pressevertretern in der Regel nicht mitgeteilt werden dürfen. Die Zustimmung muss jedoch zukünftig nicht eingeholt werden, wenn dies nach einer entsprechenden Interessenabwägung nicht erforderlich erscheint. Eine Anhörungspflicht besteht ebenfalls nicht, wenn dies nicht für erforderlich gehalten wird.

Im Entwurf der Richtlinien war zunächst auch die bisherige Regelung gestrichen worden, nach der Namen von jugendlichen Beschuldigten und Verfahrensbeteiligten nur bei außergewöhnlich schweren Straftaten genannt werden. Wegen des im Jugendstrafrecht im Vordergrund stehenden Resozialisierungsgedankens und der damit einhergehenden Schutzpflichten hielten wir es für geboten, die ursprünglichen Bestimmungen beizubehalten. Die Senatsverwaltung für Justiz und Verbraucherschutz ist unserer Empfehlung in diesem Punkt gefolgt.

Die Justiz muss bei der Unterstützung der Aufgabe der Presse, über Gerichtsverfahren zu berichten, die im Informationsinteresse der Öffentlichkeit liegen, die schutzwürdigen Interessen der Betroffenen beachten.

5.4 Funkzellenabfragen – wie weiter?

Im letzten Jahr haben wir stichprobenartig die Umsetzung der gesetzlichen Vorgaben zu Funkzellenabfragen durch die Berliner Strafverfolgungsbehörden geprüft und mussten strukturelle Mängel bei der Durchführung der Maßnahmen feststellen.[130] Unser Prüfbericht ist u. a. im parlamentarischen Bereich auch über die Landesgrenze hinaus auf große Resonanz gestoßen. So hat etwa der Innen- und Rechtsausschuss des Landtags Schleswig-Holstein das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein gebeten, in Anleh-

130 JB 2012, 2.1

nung an unseren Abschlussbericht eine entsprechende Prüfung in Schleswig-Holstein durchzuführen.[131]

Das Abgeordnetenhaus hat in Folge unserer Prüfung beschlossen, dass die Durchführung von Funkzellenabfragen auf das erforderliche Maß beschränkt werden muss.[132] Es forderte den Senat auf, sich im Bundesrat für eine gesetzliche Begrenzung des Ermittlungsinstruments auf die Verfolgung schwerer Straftaten[133] einzusetzen und eine allgemein zugängliche Information der Öffentlichkeit über Zeit und Ort einer Funkzellenabfrage (z.B. auf der Internetseite der zuständigen Senatsverwaltung) zu gewährleisten. Weiterhin forderte das Parlament die Senatsverwaltung für Justiz und Verbraucherschutz auf, die Staatsanwaltschaft anzuweisen, die Prüfung der Verhältnismäßigkeit einer nichtindividualisierten Funkzellenabfrage stärker zu strukturieren und dem Abgeordnetenhaus jährlich über die Anzahl der Funkzellenabfragen im Vorjahr sowie Umfang der dabei abgefragten Daten zu berichten.

Die Senatsverwaltung für Justiz und Verbraucherschutz berichtete, dass der seit Ende 2011 im Rechtsausschuss des Bundesrates zur Beratung befindliche Gesetzentwurf des Freistaats Sachsen zur Neuregelung der nichtindividualisierten Verkehrsdatenerhebung[134] vom Senat unterstützt wird.[135] Die Erfolgsaussichten dieses Entwurfs sind allerdings offen. Einer Internetveröffentlichung über durchgeführte Funkzellenabfragen steht sie derzeit hingegen skeptisch gegenüber, da sie deren individuellen Informationswert für eher gering hält und noch geprüft werden müsse, ob hierfür möglicherweise ein bundeseinheitliches Vorgehen oder eine Gesetzesänderung erforderlich ist. Auch die vom Abgeordnetenhaus zur Machbarkeitsprüfung vorgeschlagene Möglichkeit, die Betroffenen auf Wunsch per SMS über eine Erhebung ihrer Verkehrsdaten zu informieren, hält sie finanziell und rechtlich für problematisch.

Der Generalstaatsanwalt hat gemäß dem Beschluss des Abgeordnetenhauses Vorgaben für die Durchführung von Funkzellenabfragen durch die Staatsanwaltschaft erarbeitet, wonach u. a. die Prüfung der Verhältnismäßigkeit dokumentiert werden muss sowie die Beantragung der Auswertung einer Funkzelle der zuständigen Abteilungsleitung zur Kenntnis und Billigung vorzulegen bzw. vorzutragen ist.

131 Protokoll der Ausschusssitzung vom 4. September 2013, S. 13-14
132 Plenarprotokoll 17/18 vom 7. März 2013
133 Sog. Katalogstraftaten nach § 100a Abs. 2 StPO
134 BR-Drs. 532/11
135 Abghs.-Drs. 17/1281

Parallel hierzu hat der Leitende Oberstaatsanwalt in Abstimmung mit uns eine Generalienverfügung erstellt, in der näher erläutert wird, wann Betroffene über eine Funkzellenabfrage zu informieren sind und in welcher Weise die Sperrung und Löschung der Abfragedaten zu erfolgen hat.

Die – noch immer zu weit gefassten – gesetzlichen Vorgaben zu Funkzellenabfragen werden in Berlin nun besser beachtet. Da die Bundesratsinitiative Sachsens zur notwendigen Einschränkung dieser Vorgaben nicht vorankommt, bleibt die Entscheidung des Bundesverfassungsgerichts abzuwarten, dem mehrere Verfassungsbeschwerden vorliegen.

6 Finanzen

6.1 City Tax

Aus der Praxis

Die Regierungsfraktionen SPD und CDU haben im April den Entwurf eines Gesetzes über eine Übernachtungsteuer in Berlin (Übernachtungsteuergesetz – ÜnStG[136]) in das Abgeordnetenhaus eingebracht. Der Entwurf bestimmte als Steuergegenstand „eine Übernachtungsteuer auf den Aufwand für entgeltliche Übernachtungen". Steuerschuldner (und damit steuerpflichtig) sollte der Betreiber des Beherbergungsbetriebes sein.

Mit Beschränkung der Steuerpflicht auf privat veranlasste Übernachtungen[137] griff der Entwurf die Rechtsprechung des Bundesverwaltungsgerichts[138] auf, wonach die Erhebung einer Übernachtungsteuer für beruflich bedingte Übernachtungen unzulässig ist. Der steuerbefreiende Ausnahmetatbestand sollte nur greifen, wenn „der Übernachtungsgast die berufliche Veranlassung für die Übernachtung gegenüber dem Beherbergungsbetrieb glaubhaft macht."[139] Der Gesetzesbegründung[140] ist zu entnehmen, dass die Glaubhaftmachung bei abhängig Beschäftigten gegeben ist, „sofern die Rechnung auf den Arbeitgeber ausgestellt und unmittelbar durch diesen bezahlt wird oder die Buchung unmittelbar durch den Arbeitgeber erfolgt." Ansonsten kann die Glaubhaftmachung auch durch „Vorlage einer Bestätigung des Arbeitgebers, aus der freiwillige Angaben zum Namen und Sitz des Arbeitgebers und zum Zeitpunkt des Aufenthalts hervorgehen, erfolgen." Der Übernachtungsgast kann die berufliche Veranlassung der Übernachtung auch selbst gegenüber dem Beherbergungsbetrieb dadurch bestätigen, dass er „für Zwecke der Überprüfung durch die Finanzbehörde freiwillig neben den Angaben zur eigenen Person und des Zeitraums des Aufenthalts auch Angaben zum Namen und Sitz des Arbeitgebers" macht. Das inzwischen beschlossene und am 1. Januar 2014 in Kraft tretende ÜnStG geht daher davon aus, dass der Beherbergungsbetrieb zur Feststellung des steuerrelevanten Sachverhalts personenbezogene Daten von den Übernachtungsgästen erhebt und verarbeitet.

136 Abghs.-Drs. 17/0951
137 § 1 Abs. 3 Satz 1 ÜnStG-Entwurf
138 BVerwG, Urteile vom 11. Juli 2012 – 9 CN 12.11 und 9 CN 2.11
139 So jetzt auch § 1 Abs. 3 Satz 2 des beschlossenen Gesetzes vom 18. Dezember 2013, GVBl. S. 924
140 Abghs.-Drs. 17/0951, S. 10

Nach der Abgabenordnung haben Beteiligte (z.B. Steuerschuldner) und andere Personen der Finanzbehörde die zur Feststellung des relevanten Sachverhalts erforderlichen Auskünfte zu erteilen.[141] Andere Personen als die Beteiligten sollten jedoch erst dann zur Auskunft herangezogen werden, wenn die Aufklärung des Sachverhalts durch die Beteiligten selbst nicht zum Ziel führt oder keinen Erfolg verspricht.

Steuerpflichtig ist nach dem ÜnStG der Beherbergungsbetrieb. Die gesetzliche Auskunftspflicht richtet sich daher vorrangig an dessen Betreiber. Maßgebliches Kriterium für die Entstehung der Steuerschuld ist der Übernachtungsanlass des Übernachtungsgastes, den der Beherbergungsbetrieb jedoch nicht kennt. Zur Offenlegung dieser Information kann er den nicht steuerpflichtigen Gast nicht zwingen. Auch eine steuerrechtliche Vorschrift, die die Erhebung und Verarbeitung von personenbezogenen Daten des am Steuerverfahren unbeteiligten Gastes erlaubt, ist nicht gegeben.

Allerdings könnte der Hotelier nach dem Bundesdatenschutzgesetz[142] zur Erhebung von personenbezogenen Daten zur Erfüllung eigener Geschäftszwecke befugt sein, wenn es zur Wahrung der berechtigten Interessen der verantwortlichen Stelle (Beherbergungsbetrieb) erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen (Übernachtungsgast) an dem Ausschluss der Verarbeitung überwiegt. Zweifellos hat der Beherbergungsbetrieb ein berechtigtes Interesse daran, die für die Feststellung des steuerrelevanten Sachverhalts erforderlichen Daten beim Übernachtungsgast zu erheben. Ob das schutzwürdige Interesse des Gastes an der Geheimhaltung seiner Daten das berechtigte Interesse des Beherbergungsbetriebs überwiegt, ist jedoch vom Einzelfall abhängig. Eine allgemeine Grundaussage kann hier nicht getroffen werden, da durchaus Fälle möglich sind, in denen der Übernachtungsgast den Anlass seiner Übernachtung nicht gegenüber dem Beherbergungsbetrieb offenbaren möchte.

141 § 93 Abs. 1 Satz 1 AO
142 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Die Datenerhebung durch den Beherbergungsbetrieb ist damit zweifelsfrei nur zulässig, wenn sie auf die freiwillige Eigenbestätigung des Gastes oder eine ebenfalls freiwillige Bestätigung des Arbeitgebers über die berufliche Veranlassung der Übernachtung gestützt werden kann. Das ÜnStG selbst enthält dazu keine ausdrücklichen Regelungen. Es normiert ganz allgemein nur die Glaubhaftmachung der beruflichen Veranlassung der Übernachtung durch den Gast, der hierzu laut Gesetzesbegründung gegenüber dem Hotelier nicht verpflichtet ist. Wir haben empfohlen, die Freiwilligkeit der Angaben – im Interesse der Normenklarheit – als Tatbestandsmerkmal in den Gesetzestext aufzunehmen. Unsere Empfehlung wurde nicht berücksichtigt.

Wenn der Gast gegenüber dem Hotelier den Grund seines Aufenthalts allerdings nicht offenlegen will, muss er die City Tax zunächst selbst zahlen und kann sie sich innerhalb von vier Monaten vom Finanzamt erstatten lassen. Erst in diesem Erstattungsverfahren ist er verpflichtet, die berufliche Veranlassung seiner Übernachtung gegenüber dem Finanzamt glaubhaft zu machen. [143]

Hotelgäste, die in Berlin aus beruflichen Gründen übernachten, sind nicht verpflichtet, im Hotel Angaben zu diesen Gründen zu machen. Allerdings müssen sie die City Tax selbst tragen, wenn sie diese Gründe nicht anschließend gegenüber dem Finanzamt glaubhaft machen.

6.2 Unverschlüsselter Mail-Verkehr mit dem Finanzamt

Ein blinder Bürger bat das Finanzamt unter Berufung auf § 16 Landesgleichberechtigungsgesetz, ihm den Steuerbescheid in einer für ihn wahrnehmbaren Form zu übersenden. Das Finanzamt erklärte dem Bürger, dass der Versand der Unterlagen in der von ihm gewünschten Form aus technischen Gründen nicht möglich sei. Er könne die Bescheide entweder in schriftlicher Form oder elektronisch als E-Mail-Anhang erhalten. Der E-Mail-Versand der Unterlagen könne jedoch nur unverschlüsselt erfolgen. Es könne daher nicht ausgeschlossen werden, dass Unbefugte Kenntnis von den personenbezogenen Steuerdaten des Bürgers in der E-Mail erlangen. Eine Übermittlung des Steuerbescheides in elektronischer Form könne daher nur erfolgen, wenn der Bürger zuvor seine Einwilligung in diese risikobehaftete Kommunikation erteilen würde. Dieser wandte sich an uns.

In ihrer Stellungnahme teilte uns die Senatsverwaltung für Finanzen mit, dass das Steuergeheimnis[144] einer unverschlüsselten elektronischen Kommunikation, bei der die Daten einem unbefugten Dritten zur Kenntnis gelangen können, grundsätzlich entgegenstehe. Insofern habe § 87 a Abs. 1 Satz 3 Abgabenordnung (AO), wonach die Finanzbehörde Daten, die dem Steuergeheimnis unterliegen, im elektronischen Datenaustausch mit Dritten zu verschlüsseln haben, nur deklaratorischen Charakter. Die Finanzbehörde könne Daten, die dem Steuergeheimnis unterliegen, mit ausdrücklicher Zustimmung des Steuerpflichtigen offenbaren.[145] Wenn der Steuerpflichtige einer an sich unbefugten Offenbarung von Steuerdaten zustimmen und damit auf den Schutz seiner personenbezogenen Daten verzichten könne, müsse Gleiches auch für die Schutznorm des § 87 a Abs. 1 Satz 3 AO gelten. Daher könne die Finanzbehörde auf eine Verschlüsselung von Daten bei der elektronischen Kommunikation verzichten, wenn die oder der Betroffene der unverschlüsselten Übermittlung zuvor ausdrücklich zugestimmt habe. Datenschutzrechtliche Regelungen hätten angesichts dieser speziellen bundesgesetzlichen Bestimmungen zurückzustehen und seien nicht anwendbar.

Diese Auffassung ist unzutreffend. Bei der elektronischen Übermittlung von personenbezogenen Steuerdaten kommen nach der Rechtsprechung des Bundesverfassungsgerichts ergänzend zu den Regelungen der AO die datenschutzrechtlichen Bestimmungen zur Anwendung. [146] Nach der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz haben die datenverarbeitenden Stellen Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, dass personenbezogene 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. Laut Empfehlung

143 § 8 ÜnStG

144 § 30 Abs. 1 und 2 Abgabenordnung
145 § 30 Abs. 4 AO
146 Beschluss des BVerfG vom 10. März 2008 – 1 BvR 2388/03

des Bundesamts für Sicherheit in der Informationstechnik[147] sind zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität von E-Mails, die nicht offenkundige Daten enthalten, zusätzliche Maßnahmen wie etwa eine Verschlüsselung erforderlich.[148]

Die genannten datenschutzrechtlichen Vorgaben gelten nach § 5 Abs. 1 und 2 Berliner Datenschutzgesetz (BlnDSG) auch für alle Behörden und öffentlichen Stellen des Landes Berlin. Die Rechtmäßigkeit der Datenverarbeitung in den Berliner Behörden setzt daher nicht nur eine Rechtsgrundlage oder die wirksame Einwilligung des Betroffenen voraus.[149] Die Behörden sind auch zu den genannten technisch-organisatorischen (Datensicherheits-) Maßnahmen verpflichtet. Einen Verzicht auf diese Maßnahmen – gestützt auf eine Einwilligung der oder des Betroffenen – sieht das Gesetz nicht vor.[150] Er wäre auch bereits deshalb unzulässig, weil es sich bei den genannten Normen um ordnungsrechtliche Vorschriften handelt, deren Adressat die verantwortliche Stelle ist.

Die nach datenschutzrechtlichen Bestimmungen zu treffenden technischen und organisatorischen Maßnahmen dienen nicht nur den Betroffenen. Die Schutzvorschriften sind angesichts der sich ständig ändernden Gefahren für informationstechnische Systeme auch für die verantwortliche Stelle (Behörde) aus Gründen des Eigenschutzes unverzichtbar. Unabhängig davon würde die Disponibilität dieser Maßnahmen den Behörden erlauben, sich von den Betroffenen eine umfassende Einwilligung in den Verzicht der darin vorgesehenen Sicherheitsanforderungen erteilen zu lassen. Damit wäre eine Umgehung der gesetzlich festgelegten Datensicherheitsschranken (z.B. aus wirtschaftlichen Erwägungen) unproblematisch möglich. Dies würde dem Zweck der datenschutzrechtlichen Vorschriften zuwiderlaufen.

Eine wirksame Einwilligung von Steuerpflichtigen in den Verzicht auf die Pflicht der Finanzbehörden zur Verschlüsselung von Steuerdaten im elektronischen Rechtsverkehr ist nicht möglich. Unsere Empfehlung, diese datenschutzrechtliche Vorgabe durch geeignete Maßnahmen in den Berliner Finanzbehörden umzusetzen, hat die Senatsverwaltung für Finanzen abgelehnt.

147 BSI-Standard 100-2
148 Siehe Baustein B 5.3, dort insbesondere G 5.77 und M 5.108
149 § 6 Abs. 1 BlnDSG
150 Siehe auch 12.1.3 und 14.2

6.3 Überprüfung der Zugriffe von Beschäftigten der Finanzverwaltung auf Steuerdaten

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg unterrichtete uns davon, dass die Innenrevision des Ministeriums der Finanzen in Brandenburg in 2012 und 2013 für einen Zeitraum von 19 Monaten alle von den Beschäftigten der brandenburgischen Finanzämter getätigten Abrufe von Steuerdaten, die nach der Steuerdaten-Abrufverordnung (StDAV) aufgezeichnet wurden, auf ihre Rechtmäßigkeit kontrolliert habe. Zur Begründung für die Vollkontrolle aller Beschäftigten habe das Ministerium darauf hingewiesen, dass die Innenrevision der Senatsverwaltung für Finanzen Berlin der Innenrevision des Ministeriums der Finanzen Brandenburg mitgeteilt habe, dass in mehreren Berliner Finanzämtern eine Prüfung der Datenabrufe erfolgt sei und weiterhin erfolgen würde. Im Rahmen dieser Prüfungen sei eine Vielzahl von unberechtigten Datenabrufen festgestellt worden. Daher sei eine entsprechende Prüfung in Brandenburg für sinnvoll erachtet worden.

Wir haben die Angelegenheit mit der Senatsverwaltung für Finanzen erörtert. Sie teilte mit, dass das Verfahren zur Überprüfung der Zugriffe von Dienstkräften der Finanzverwaltung auf Steuerdaten nach der StDAV in einer Dienstanweisung festgelegt sei, die primär der Prävention und erst sekundär der Kontrolle von Beschäftigtenverhalten diene. Nach der Dienstanweisung sei für jedes Finanzamt aus dem Bereich der Geschäftsstelle eine StDAV-Prüfkraft zu benennen. Je nach Größe des Finanzamtes habe die StDAV-Prüfkraft drei bis zehn Dienstkräfte in der Woche zu überprüfen. Die Auswahl der zu überprüfenden Dienstkräfte werde anhand der Anwendung „StDAV-Auswertung“ vorgenommen. Die Anwendung „StDAV-Auswertung“ diene ausschließlich der Prüfung der Zulässigkeit von Abfragen[151] und als Verfahrensdokumentation für die prü-

151 § 6 Abs. 3 StDAV

fende Dienstkraft. Eine Auswertung sei möglich nach Angaben zur Dienstkraft, zum Zeitraum, zum Vorgang (Abfrageart), zu einzelnen Ordnungskriterien oder zu einer Kombination der genannten Möglichkeiten. Jede Dienstkraft eines Finanzamtes würde grundsätzlich einmal, nur in Einzelfällen zweimal im Jahr überprüft, habe jedoch jederzeit mit einer Überprüfung zu rechnen. Dabei würden von der StDAV-Prüfkraft (im Beisein der überprüften Dienstkraft) ein bis zwei der protokollierten Datenabfragen aus den letzten 48 Stunden ausgewertet. Bestehen Zweifel an der Zulässigkeit eines Datenzugriffs, werde dies der Amtsleitung mitgeteilt. Die Durchführung des Verfahrens werde regelmäßig von der Innenrevision der Senatsverwaltung für Finanzen kontrolliert. Ein eigenständiger Zugriff der Innenrevision auf die Protokolldaten sei nur vor Ort im Finanzamt möglich und erfolge nur aus konkretem Anlass (z.B. nach Anzeigen). Ein zentralisierter Zugriff der Innenrevision auf die Protokolldatenbank sei nicht gegeben.

Die Senatsverwaltung für Finanzen bestätigte auf Nachfrage, dass es in den Berliner Finanzämtern keine flächendeckende Überprüfung der Zugriffe aller Beschäftigten gegeben habe und dies für die Zukunft auch nicht vorgesehen sei. Insofern sei der Hinweis der Brandenburger Finanzbehörden an die Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg, die Senatsverwaltung für Finanzen habe dem Brandenburger Ministerium der Finanzen eine Mitteilung über vergleichbare Prüfungen in Berlin gemacht, nicht nachvollziehbar.

Aus datenschutzrechtlicher Sicht bestehen gegen das in Berlin praktizierte Verfahren zur Überprüfung der Rechtmäßigkeit von Datenzugriffen durch Beschäftigte auf Steuerdaten im Rahmen der StDAV keine Bedenken. Das Verfahren ist sowohl geeignet als auch verhältnismäßig. Auch die notwendige Kontrolle der Einhaltung von datenschutzrechtlichen Zugriffsbeschränkungen rechtfertigt keine flächendeckende Vollkontrolle von Beschäftigten.

7 Jugend und Soziales

7.1 Vormerksystem für Kita-Plätze

Um den gesetzlichen Anspruch auf einen Kita-Platz sicherstellen zu können, besteht in Berlin ein Interesse an verlässlichen Daten, die die Planung des künftigen Bedarfs an Kita-Plätzen und den Nachweis freier Plätze erleichtern können. Es liegen derzeit keine Zahlen vor, die Auskunft geben, wie viele Kinder tatsächlich einen Kita-Platz benötigen. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat deswegen ein zentrales Vormerksystem für Kita-Plätze eingerichtet. Die Realisierung erfolgt mit dem in der Jugendhilfe eingesetzten IT-Fachverfahren.[152] Des Weiteren wurde ein Verfahren entwickelt, mit dem Eltern den Antrag auf Erteilung des für einen Kita-Platz notwendigen Gutscheins elektronisch beantragen können. Die Senatsverwaltung hat uns von Beginn an einbezogen, sodass wir die datenschutzrechtlichen Anforderungen frühzeitig einbringen konnten.

Da Eltern ihre Kinder häufig in mehreren Kita-Einrichtungen anmelden, damit zu einem bestimmten Zeitpunkt tatsächlich ein Betreuungsplatz für das Kind zur Verfügung steht, werden Planungen zum tatsächlichen Bedarf an freien Kita-Plätzen erschwert. Mit der Realisierung des zentralen Vormerksystems kann die Planung des Bedarfs erheblich vereinfacht werden. Die Eintragung der personenbezogenen Daten der Eltern und Kinder kann mangels entsprechender Rechtsgrundlage allerdings lediglich mit der Einwilligung der Eltern erfolgen. Die entsprechende Einwilligungserklärung haben wir mit der Senatsverwaltung abgestimmt. Da eine Auswertung der Vormerkungen nur in anonymisierter Form erfolgt, um verlässliche Prognosen über den Bedarf an Kita-Plätzen treffen zu können, ist dies datenschutzrechtlich zulässig.

Der von der Senatsverwaltung für Bildung, Jugend und Wissenschaft außerdem entwickelte „Kita-Gutschein-Online-Antrag“, der es Eltern ermöglicht, über den vom Land Berlin zur Verfügung gestellten Formularservice des ITDZ‘

152 Integrierte Software Berliner Jugendhilfe – ISBJ

elektronisch einen Kita-Gutschein zu beantragen, ist ebenfalls datenschutzkonform. Sollten sich Eltern entscheiden, ihren Kita-Gutschein online beantragen zu wollen, können sie ihre Daten elektronisch in das Formular eintragen. Sie werden gleichzeitig darüber informiert, welche Daten über sie im zentralen IT-Fachverfahren gespeichert werden und was mit diesen weiterhin passiert. Nach Eingang eines von den Eltern unterschriebenen schriftlichen Kurzantrages beim zuständigen Jugendamt kann dieses die Daten abrufen und weiterverarbeiten. Wir haben mit der Senatsverwaltung die entsprechenden Datenschutzerklärungen abgestimmt und die technische Realisierung unter dem Aspekt der Datensicherheit begleitet.

Mit dem Vormerksystem wurde ein datenschutzgerechtes Verfahren gefunden, das es erleichtert, den Bedarf an Kita-Plätzen im Land Berlin zu planen. Mit der Möglichkeit, einen Kita-Gutschein online zu beantragen, wird das Verfahren sowohl für die Eltern als auch für die Jugendämter erleichtert. Durch unsere frühzeitige Einbindung konnten die datenschutzrechtlichen Anforderungen von vornherein bei der Entwicklung des Verfahrens berücksichtigt werden.

7.2 Evaluation des Kinderschutzgesetzes

Zwei Jahre nach Beginn der Arbeit der bei der Charité eingerichteten Zentralen Stelle[153] stand die gesetzlich vorgesehene Evaluation[154] ihrer Arbeit an. Die Zentrale Stelle führt das Einladungswesen zu den freiwilligen Vorsorgeuntersuchungen der Kinder durch.

Die Senatsverwaltung für Gesundheit und Soziales hat nach dem Gesetz einen Dritten mit der Durchführung der Evaluation zu beauftragen und die in einem Bericht zusammengestellten Evaluationsergebnisse zu veröffentlichen. Wir haben die Senatsverwaltung sowie die Zentrale Stelle im Hinblick auf die datenschutzrechtlichen Rahmenbedingungen für die Evaluation beraten. Nach

153 Siehe JB 2009, 7.1.2

154 § 7 Berliner Gesetz zum Schutz und Wohl des Kindes (Berliner Kinderschutzgesetz)

einer Sichtung sowohl der im Rahmen der Geschäftsstatistik der Zentralen Stelle erhobenen Daten als auch der von den Kinder- und Jugendgesundheitsdiensten der Bezirke im Rahmen der Durchführung des Einladungswesens erhobenen Daten haben wir datenschutzrechtliche Anforderungen definiert, um sicherzustellen, dass die verwendeten Statistiken einen Personenbezug nicht mehr herstellen lassen.

Wir gehen davon aus, dass die ausstehende Evaluation datenschutzgerecht durchgeführt wird. Wir werden auch weitere Evaluationen des Einladungswesens im Hinblick auf die Einhaltung datenschutzrechtlicher Anforderungen intensiv begleiten.

7.3 Elternzufriedenheit – Verschlusssache für Tagesmütter?

Mehrere Tagespflegepersonen (Tagesmütter) beschwerten sich bei uns, weil ihnen das Jugendamt, das die Aufsicht über die Tagesmütter führt, mitgeteilt hatte, künftig einen Elternzufriedenheitsbogen zu verwenden. Die Eltern der betreuten Kleinkinder sollten im Falle der Kündigung des Vertrages mit der Tagesmutter in dem Bogen zahlreiche Fragen zur Zufriedenheit mit der Betreuung (z.B. Zustand der Räume, Speiseplan) beantworten. Den betroffenen Tagesmüttern verwehrte das Jugendamt allerdings die Einsicht in die Bögen. Lediglich im Rahmen der alle fünf Jahre gesetzlich notwendigen Erneuerung ihrer Zulassung sollten sie sich über die Ergebnisse informieren dürfen.

Wir haben dem Jugendamt mitgeteilt, dass die Datenerhebung hinter dem Rücken der Tagesmütter unzulässig ist. Das Jugendamt darf im Rahmen der Aufsicht Hausbesuche bei den Tagesmüttern durchführen. Die Befragung der Eltern, die einen Vertrag – aus welchen Gründen auch immer – gekündigt haben, mittels eines standardisierten Bogens hielten wir aufgrund der subjektiven Wahrnehmungen der einzelnen Familien dagegen für unangemessen. Selbstverständlich bleibt es dem Jugendamt unbenommen, nach Erhalt einer Kündigung die Eltern im Einzelfall anlassbezogen gezielt anzusprechen, wenn

Anhaltspunkte bestehen, dass im Rahmen der Betreuung Missstände auftraten. Hier jedoch standardisiert und flächendeckend eine Vielzahl von Daten über die Tagesmütter zu erheben und ihnen selbst den Erhebungsbogen mit Antworten vorzuenthalten, ist datenschutzrechtlich unzulässig. Nach einem mit dem betroffenen Jugendamt geführten Schriftwechsel hat es uns mitgeteilt, den Bogen nicht mehr zu verwenden.

Tagesmütter sollten im gesetzlichen Rahmen beaufsichtigt werden und nicht, indem man die Eltern über sie befragt und ihnen die Ergebnisse vorenthält.

7.4 Elterngeldstatistik

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft bat uns um Rat, da das Statistische Bundesamt im Rahmen der Bundesstatistik zum Bezug von Elterngeld und Betreuungsgeld [155] um die Übermittlung zusätzlicher Merkmale gebeten hatte. Es handelte sich um die Merkmale Steuerklasse, Kirchensteuerpflicht, Anzahl der Freibeträge für Kinder, Rentenversicherungspflicht, Krankenversicherungspflicht, Arbeitslosenversicherungspflicht sowie Bemessungsgrundlagen für die Abzüge für Steuern und Sozialabgaben.

Unsere Prüfung hat ergeben, dass die Übermittlung dieser Merkmale mangels Rechtsgrundlage unzulässig ist. Die Statistik erfasst als Erhebungsmerkmale die Grundlagen der Berechnung des zustehenden Monatsbetrags nach Art und Höhe[156] und verweist hierzu enumerativ auf bestimmte Vorschriften.[157] Diese Aufzählung umfasst jedoch nicht die die zusätzlichen Merkmale betreffenden Vorschriften bezüglich der Abzüge für Steuern und Sozialabgaben,[158] sodass diese nach dem Willen des Gesetzgebers von der Statistik ausdrücklich nicht erfasst werden sollen. Hierfür spricht insbesondere, dass die entsprechenden Vorschriften erst im September 2012 systematisch neu gefasst wurden, ohne dass der Gesetzgeber den Regelungsgehalt in diesen Punkten geändert hat.

155 § 22 Bundeselterngeld- und Elternzeitgesetz (BEEG)
156 § 22 Abs. 2 Nr. 2 BEEG
157 § 2 Abs. 1, 2, 3 oder 4, § 2a Abs. 1 oder 4, § 2c oder § 2d BEEG
158 §§ 2e und 2f BEEG

Zudem geht es bei den zusätzlichen Merkmalen auch nicht um Grundlagen der Berechnung, da diese nicht den Einkommensunterlagen der antragstellenden Person zu entnehmen sind, sondern von der sachbearbeitenden Person erst anhand verschiedener Kriterien ermittelt werden müssen bzw. lediglich Zwischenschritte der Berechnung im Rahmen der Antragsbearbeitung darstellen. Daher handelt es sich bei den Merkmalen gerade nicht um Grundlagen, sondern vielmehr um Ergebnisse bzw. Zwischenergebnisse von Berechnungen.

Wir haben der Senatsverwaltung mitgeteilt, dass die zusätzlichen Merkmale nicht an das Statistische Bundesamt übermittelt werden dürfen und eine Übermittlung erst dann in Betracht kommt, wenn der Gesetzgeber die Vorschriften entsprechend angepasst hat.

Für die Übermittlung von Merkmalen im Rahmen von Statistiken ist eine Rechtsgrundlage erforderlich. Soweit der Gesetzgeber die zu übermittelnden Merkmale abschließend geregelt hat, kommt eine Übermittlung weitergehender Merkmale nicht in Betracht.

7.5 Widersprüchliche Schweigepflichtentbindung bei Sozialleistungen

Eine Petentin erhielt Sozialleistungen nach dem sozialen Entschädigungsrecht vom Versorgungsamt des Landesamtes für Gesundheit und Soziales (LAGeSo). Dem Versorgungsamt lagen zwei sich widersprechende Schweigepflichtentbindungserklärungen der Petentin vor. In einer Erklärung aus dem Jahre 2007 entband die Petentin ausschließlich ihre Hausärztin von der Schweigepflicht und war damit einverstanden, dass das Versorgungsamt die erforderlichen Auskünfte bei der Hausärztin einholt. Bereits im Jahre 1995 hatte die Petentin jedoch eine Einwilligungserklärung zur Beiziehung von Unterlagen und Einholung von Auskünften unterzeichnet, verbunden mit einer Entbindung sämtlicher beteiligter Ärzte von der diesen obliegenden Schweigepflicht. Das Versorgungsamt bediente sich der jeweils passenden Erklärung, um Auskünfte von Ärzten einzuholen.

Die sich widersprechenden Erklärungen hätten das Versorgungsamt veranlassen müssen, sich bei der Petentin nach ihrem aktuellen Willen zu erkundigen. Dass sich das Versorgungsamt stattdessen zwecks Einholung von Patienteninformationen der jeweils passenden Erklärung bedient hat, verstößt gegen den Grundsatz von Treu und Glauben.[159] Er verschafft den in unserer Gesellschaft herrschenden Wertvorstellungen Eingang in alle Rechtsbereiche und verpflichtet auch Behörden zur Rücksichtnahme auf die schutzwürdigen Interessen anderer und zu einem redlichen Verhalten. Eine dagegen verstoßende Rechtsausübung ist missbräuchlich und unzulässig.

Will das Versorgungsamt Auskünfte von den behandelnden Ärzten einholen, ist dafür eine von der oder dem Betroffenen zu erteilende Einwilligung in die Datenübermittlung vom Arzt an das Versorgungsamt und eine Schweigepflichtentbindungserklärung erforderlich. Die Einwilligung dient als Rechtsgrundlage für die Übermittlung von Patientendaten durch den Arzt an das Versorgungsamt.[160] Hingegen ist die Schweigepflichtentbindungserklärung in erster Linie strafrechtlich relevant. Sie dient dazu, den entsprechenden Straftatbestand auszuschließen.[161]

Damit es sich um wirksame Erklärungen handelt, muss die oder der Betroffene die Möglichkeit haben, die jeweiligen Ärzte konkret zu benennen. Es muss hinreichend deutlich sein, wer zur Datenübermittlung autorisiert und von der Schweigepflicht entbunden werden soll. Nur auf diese Weise kann die oder der Betroffene die Tragweite und die Bedeutung der zu erteilenden Erklärungen überblicken und „informierte“ Erklärungen abgeben. Möchte jemand diese Erklärungen nicht abgeben, besteht alternativ die Möglichkeit, die benötigten Informationen selbstständig beim jeweiligen Arzt einzuholen und an das Versorgungsamt weiterzugeben. Hintergrund ist der Grundsatz der Direkterhebung, wonach Sozialdaten vorrangig bei der betroffenen Person und eben nicht bei Dritten zu erheben sind.[162] Das Versorgungsamt ist als Sozialleistungsträger an

159 § 242 BGB
160 § 100 Abs. 1 Satz 1 Nr. 2 SGB X
161 Nach § 203 Abs. 1 Satz 1 Nr. 1 StGB wird u. a. derjenige, der unbefugt ein zum privaten Lebensbereich gehörendes Geheimnis offenbart, das ihm in seiner Eigenschaft als Arzt anvertraut worden oder sonst bekannt geworden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
162 § 67 a Abs. 2 Satz 1 SGB X

diesen Grundsatz gebunden. Er verleiht dem Recht des Menschen auf informationelle Selbstbestimmung ein hohes Maß an Effektivität. Denn wer eigene Sozialdaten selbst zur Verfügung stellt, kann gleichzeitig kontrollieren, welche Sozialdaten im Umlauf sind.

Das Versorgungsamt ist unserer Empfehlung gefolgt und hat die Vordrucke für Anträge nach dem sozialen Entschädigungsrecht überarbeitet. Die aktuellen Fassungen enthalten sowohl eine Schweigepflichtentbindungserklärung als auch eine Einwilligung in die Datenübermittlung vom jeweiligen Arzt an das Versorgungsamt. In den Vordrucken sind die behandelnden Ärzte konkret zu benennen.

Das Versorgungsamt darf bei der Bearbeitung von Anträgen nach dem sozialen Entschädigungsrecht Auskünfte über den Gesundheitszustand von Betroffenen direkt bei den behandelnden Ärzten einholen, wenn die oder der Betroffene eingewilligt und den konkreten Arzt von der Schweigepflicht entbunden hat. Alternativ kann die betroffene Person die vom Versorgungsamt benötigten Informationen selbstständig beim jeweiligen Arzt einholen und anschließend beim Versorgungsamt einreichen.

7.6 Grundsicherung nur gegen Kopie der Krankenversichertenkarte?

Ein Petent bezog als Rentner ergänzende Grundsicherung vom Sozialamt Tempelhof-Schöneberg. Das Sozialamt hat ihn aufgefordert, eine Kopie seiner Krankenversichertenkarte einzureichen. Es begründete dieses Vorgehen damit, dass in jedem Fall geprüft werden müsse, ob und ggf. welche Krankenversicherungsverhältnisse bestehen, ob diese auch nach der den Grundsicherungsbezug auslösenden Einkommensveränderung (z.B. Wechsel aus dem ALG II-Bezug, Verrentung) weiter bestehen und ob etwaige Beiträge direkt vom Einkommen abgeführt werden oder vom Sozialhilfeträger zu übernehmen seien.

Bei den Daten auf der Krankenversichertenkarte handelt es sich um Sozialdaten. Sie dürfen nur dann erhoben werden, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle, hier also des Sozialamtes, erforderlich ist.[163] Die Kenntnis der Daten ist nur dann erforderlich, wenn das Sozialamt ohne diese Daten im konkreten Einzelfall die ihm gesetzlich zugewiesenen Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann.

Unter bestimmten Voraussetzungen übernimmt das Sozialamt bei der Grundsicherung im Alter die Krankenversicherungsbeiträge für Pflichtversicherte und für freiwillig Versicherte.[164] Allerdings enthält die Kopie einer Krankenversichertenkarte Informationen, die das Sozialamt gerade nicht in jedem Einzelfall benötigt, um die Entscheidung über die Leistungsberechtigung und den jeweiligen Hilfebedarf zu treffen. Dafür ist lediglich ein Nachweis über Art und Bestehen bzw. Nichtbestehen eines Krankenversicherungsverhältnisses erforderlich. Die Mitgliedsnummer darf nur dann erhoben werden, wenn das Sozialamt von vornherein zur Direktüberweisung der Beiträge an die Krankenkasse verpflichtet ist oder wenn eine entsprechende Anforderung durch die Krankenkasse vorliegt.[165]

Aufgrund unserer Hinweise hat das Sozialamt das Antragsprüfverfahren umgestellt. Es wird nun den genannten Vorgaben gerecht. Die Leistungsberechtigten können jetzt einen grundsätzlich frei wählbaren Nachweis über Art und Bestehen eines Krankenversicherungsverhältnisses einreichen. Die Mitgliedsnummer wird nur noch erfragt, wenn das Sozialamt die Beiträge direkt an die Krankenkasse zahlen muss.

Um eine Entscheidung über die Leistungsberechtigung und den konkreten Hilfebedarf zu treffen, benötigt das Sozialamt keine Kopie der Krankenversichertenkarte. Auch die pauschale Erhebung der Mitgliedsnummer, also eine Erhebung unabhängig von den Besonderheiten des Einzelfalls, ist unzulässig.

163 § 67 a Abs. 1 Satz 1 SGB X
164 § 32 Abs. 1 und Abs. 2 SGB XII
165 § 32 Abs. 1 Satz 3, Abs. 5 Satz 5 SGB XII

7.7 Datenerhebung über Betreuende

Ein als Rechtsanwalt tätiger Petent wollte als ehrenamtlicher Betreuer arbeiten. Das für die Bestellung zum Betreuer zuständige Bezirksamt Mitte forderte ihn auf, vor der Bestellung einen Vordruck auszufüllen. Dieser Vordruck enthielt den Hinweis, dass das Bezirksamt Auskünfte über die Person, die sich zum Betreuer bestellen lassen möchte, aus dem Schuldnerverzeichnis einholt.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.[166] Die Erhebung personenbezogener Daten ist eine Unterform der Datenverarbeitung.[167] Eine Rechtsvorschrift, die die Einholung von Auskünften aus dem Schuldnerverzeichnis durch das Bezirksamt erlaubt, gibt es nicht. § 1897 Abs. 7 Satz 2 BGB, den das Bezirksamt für eine ausreichende Rechtsgrundlage gehalten hat, besagt lediglich, dass die zuständige Behörde die Person auffordern soll, ein Führungszeugnis und eine Auskunft aus dem Schuldnerverzeichnis vorzulegen. Die Vorschrift berechtigt die zuständige Behörde nicht, selbsttätig Auskünfte aus dem Schuldnerverzeichnis einzuholen. Somit darf das Bezirksamt nur aufgrund einer Einwilligung der Person, die zum Betreuer bestellt werden möchte, Auskünfte einholen. Das Bezirksamt hat sich in der Vergangenheit jedoch keine Einwilligungen erteilen lassen und dennoch die benötigten Auskünfte erbeten.

Wir haben gegenüber dem Bezirksamt einen datenschutzrechtlichen Mangel festgestellt.[168] Das Bezirksamt hat daraufhin den Vordruck überarbeitet. Aus ihm geht nunmehr hinreichend deutlich hervor, dass im Rahmen des Bestellungsverfahrens eine Auskunft aus dem Schuldnerverzeichnis vorzulegen ist und dass die Betroffenen diese Auskunft selbst einholen und dem Bezirksamt vorlegen oder aber das Bezirksamt ermächtigen können, dies zu tun.

Ohne eine Einwilligung der Person, die sich zum Betreuer bestellen lassen möchte, darf das Bezirksamt keine Auskünfte aus dem Schuldnerverzeichnis einholen.

166 § 6 Abs. 1 Satz 1 BlnDSG
167 § 4 Abs. 2 Satz 1 BlnDSG
168 § 26 Abs. 2 BlnDSG

8 Gesundheitswesen

8.1 „Doku-Soap“ im Kreißsaal?

Aus der Praxis

Presseberichten entnahmen wir, dass auf der Entbindungsstation des Vivantes-Klinikums Im Friedrichshain Filmaufnahmen für die RTL-Serie „Babyboom – Willkommen im Leben“ gedreht werden sollten. Die Datenverarbeitung sollte auf Einwilligungserklärungen der Eltern und Beschäftigten gestützt werden.

Schon hinsichtlich der Wirksamkeit der Einwilligungserklärung der Eltern für das Kind bestanden prinzipielle Bedenken. Durch die Filmaufnahmen wären sowohl das verfassungsrechtlich garantierte Recht des Kindes auf informationelle Selbstbestimmung als auch das allgemeine Persönlichkeitsrecht beeinträchtigt worden, da zum damaligen Zeitpunkt die Folgen einer irreversiblen Veröffentlichung der Filmaufnahmen nicht abzusehen waren.

Bei der Einwilligung der Eltern für sich selbst war ein doppelter Einwilligungsvorbehalt vorgesehen. Neben der Einwilligung und Erklärung der Schweigepflichtentbindung gegenüber den beteiligten Klinikbeschäftigten vor Beginn der Dreharbeiten sollten die Eltern zusätzlich noch eine zweite Einwilligungserklärung frühestens eine Woche nach der Geburt unterzeichnen, damit die Filmaufnahmen hätten genutzt werden können. Nicht berücksichtigt wurde dabei allerdings, dass die Rechte der Eltern nur dann hinreichend gewahrt worden wären, wenn die zweite Einwilligungserklärung erst nach der Möglichkeit der Sichtung des Filmmaterials eingeholt worden wäre. Nur so hätten die Eltern die Entscheidung in Kenntnis der aufgezeichneten Bilder treffen können.

Auch hinsichtlich der Ausgestaltung der Einwilligungserklärung der Beschäftigten bestanden erhebliche Einwände. Anders als den werdenden Eltern und deren Angehörigen wurde den Beschäftigten nur ein eingeschränktes Widerrufsrecht eingeräumt, das erst nach Prüfung und Bestätigung von mindestens einem Mitglied des „Fachlichen Beirates“, bestehend aus einem Vertreter von Vivantes, der Produktionsfirma sowie der RTL Group, hätte Wirkung entfalten können.

So wie die Einwilligung die präventive Kontrolle der Verwendungsabsichten Dritter sichert, wird durch den Widerruf das Recht der Betroffenen auf nachträgliche Korrektur einer zunächst gebilligten Verwendung der eigenen Daten umgesetzt. Betroffene müssen unabhängig von der Erfüllung bestimmter Voraussetzungen und der Bestätigung des Widerrufs durch Dritte die Möglichkeit haben, eventuell zu spät erkannte Verwendungsfolgen auffangen zu können. Dies wäre durch die geschlossene Vereinbarung nicht gewährleistet gewesen.

Der Aufsichtsrat der Vivantes Netzwerk für Gesundheit GmbH hatte die Filmarbeiten bereits vor einer abschließenden datenschutzrechtlichen Bewertung gestoppt und somit unseren Einwänden Rechnung getragen.

„Doku-Soaps“ in Krankenhäusern sind stets problematisch und in Geburtskliniken wegen der Persönlichkeitsrechte der Ungeborenen in aller Regel unzulässig. Im Übrigen dürfen sie nur mit Einwilligung aller betroffenen Personen ausgestrahlt werden, die wirksam nur in Kenntnis der zu sendenden Filmaufnahmen erteilt werden kann und vor der Ausstrahlung frei widerruflich sein muss.

8.2 Videoüberwachung und -aufzeichnung im Krankenhaus

Aus der Praxis

Ein Bürger hat uns darauf hingewiesen, dass die zentrale Notaufnahme eines Krankenhauses videoüberwacht wird. In einem anderen Fall wurde uns gemeldet, dass ein Gerät mit Videoaufzeichnungen gestohlen worden war, auf denen Patienten so zu sehen waren, dass auf ihre Erkrankungen geschlossen werden konnte.

Die Videoüberwachung findet sowohl in öffentlich als auch in nicht-öffentlich zugänglichen Räumen der Notaufnahme statt. Zu den öffentlich zugänglichen Räumen zählen Bereiche, die ohne Beschränkung von jedermann betreten werden können. Dazu gehören der Zugang zur Notfallbehandlung und die äußeren Wartebereiche, in denen Patienten und deren Angehörige eintreffen und sich vor einer Behandlung aufhalten. Nicht öffentlich zugänglich sind

dagegen alle Bereiche, die der Beobachtung und Behandlung der Patienten dienen, wie der Liegendwartebereich, Verfügungs- und Ausnüchterungsräume. In diesen nicht-öffentlich zugänglichen Behandlungsräumen befinden sich die Patienten teilweise in einem überwachungspflichtigen Zustand, z.B. wenn eine Alkoholvergiftung festgestellt oder eine Betäubung bzw. Narkose verabreicht wurde. Da häufig mehrere Notfälle parallel behandelt werden müssen, können nicht alle Räume gleichzeitig von Beschäftigten persönlich überwacht werden. Die Behandlungsräume werden dann von einem zentralen Arbeitsplatz über Monitore live beobachtet.

Unter diesen Bedingungen ist eine Videoüberwachung, nicht jedoch eine längerfristige Aufzeichnung statthaft. Sie muss für die Patienten erkennbar sein. Umgekehrt hat das Krankenhaus dafür zu sorgen, dass Patienten dann nicht beobachtet werden, wenn sie keiner Überwachung bedürfen. Auch dies muss für die Patienten – z.B. durch einen deutlich sichtbar angebrachten Verschlussdeckel auf der Kamera – offensichtlich werden.

Die Videoüberwachung der Zugangs- und Wartebereiche dient einerseits dem Schutz der Patienten, die sich vor einer Behandlung mitunter in einem physisch und psychisch labilen Ausnahmezustand befinden. Andererseits dient sie dem Schutz der Beschäftigten, da es abhängig vom Gesundheitszustand zu aggressiven Übergriffen durch Angehörige oder Patienten kommen kann. Dies veranlasste den Betriebsrat des Krankenhauses, der Videoüberwachung unter der Voraussetzung zuzustimmen, dass die Auswertung der Bilddaten nicht zur Leistungs- und Verhaltenskontrolle des Personals verwendet wird.

Sowohl eine Videoüberwachung als auch kurzzeitige Aufzeichnungen auf besonders geschützten Medien, die nur auf besondere Veranlassung von vorab bestimmten Beschäftigten ausgewertet werden dürfen, halten wir unter diesen Bedingungen für zulässig. Dass Aufzeichnungsmedien besonders geschützt werden müssen, zeigte ein anderer Fall, bei dem eine Videokamera mitsamt Aufnahmen von Patienten gestohlen wurde.[169] Erschwerend kam hinzu, dass Patienten der Psychiatrie betroffen waren. Jeder, dem die gestohlene Kamera in die Hände kommt, kann die Bilder einsehen, speichern und weitergeben. Dies ist ein untragbares Risiko.

169 Zum Diebstahl von Gesundheitsdaten siehe auch 8.9

Um dieses Risiko zu vermeiden, muss die Speicherung der Videos entweder unmittelbar auf einem geschützten Server erfolgen – das ist das deutlich vorzuziehende Vorgehen – oder es müssen bei mobilen Kameras die Speichermedien unmittelbar nach der Aufnahme auf einen geschützten zentralen Speicher kopiert und dann geleert werden. Ein derartiges Vorgehen sagte uns das Krankenhaus zu. Es wird regelmäßiger Kontrolle bedürfen.

Unter engen Voraussetzungen können Videoüberwachungen und sogar -aufzeichnungen in der Notaufnahme eines Krankenhauses zulässig sein. Ein Diebstahl von mobilen IT-Geräten, Kameras oder Aufzeichnungsmedien darf nicht zur Offenlegung der gespeicherten Videobilder führen.

8.3 Zertifizierung von Tumorzentren

Tumorzentren können sich zertifizieren lassen und somit nachweisen, dass sie die hohen Anforderungen an die Versorgung onkologischer Patienten erfüllen. Diese Zertifizierungen werden bundesweit ausschließlich durch das unabhängige Zertifizierungsinstitut der Deutschen Krebsgesellschaft (DKG), die Onkozert GmbH, durchgeführt. Im Verlauf der Zertifizierung wurde von der Onkozert GmbH zwingend die Offenbarung von Patientendaten vorgegeben, z.B. in Form einer Live-Abfrage im produktiven Tumor-Dokumentationssystem und einer Einsicht von Patientenakten. Das jeweilige Tumorzentrum wurde dabei aufgefordert, innerhalb kurzer Zeit die vollständige Patientenakte bereitzustellen.

Gespräche mit der DKG ergaben, dass die Kenntnis der Namen der Patienten zur Durchführung der Zertifizierung nicht erforderlich ist, sodass eine Offenbarung auch nicht auf eine entsprechende Regelung des Berliner Landeskrankenhausgesetzes gestützt werden kann.

Die DKG hat daraufhin ein datenschutzfreundliches Verfahren entwickelt, bei dem keine Patientenstammdaten mehr den Auditoren bekannt gegeben werden. Dabei soll das Verfahren nun so ausgestaltet werden, dass nur die Beschäftigten des Tumorzentrums Einblick in die ungeschwärzte Patientenakte nehmen.

Der Auditor gibt vor, welche Teile der Akte er zwecks Prüfung benötigt; diese sollen dann vom Einrichtungsmitarbeiter herausgenommen, kopiert und dem Auditor geschwärzt zur Verfügung gestellt oder die Stammdaten der Patienten abgedeckt werden. Auch bei der Auswahl der Patientenakten sollen die Patientenlisten so pseudonymisiert werden, dass lediglich noch eine Behandlungsnummer vorhanden ist; die Stammdaten wie Name, Adresse und Geburtsdatum sollen geschwärzt werden. Auf diese Weise wird sichergestellt, dass es sich um eine „echte" Patientenliste handelt, bei der jedoch die Stammdaten nicht zur Kenntnis genommen werden können.

Die Umstellung auf dieses datenschutzfreundliche Verfahren ist zu begrüßen. Insbesondere kann ein solches Verfahren auch in Bundesländern, die keine entsprechende Regelung im Landeskrankenhausgesetz haben, einheitlich umgesetzt werden.

Auch im Bereich der Zertifizierungen ist die ärztliche Schweigepflicht zwingend zu beachten. Ein Zertifizierungsverfahren, bei dem die Patientendaten pseudonymisiert übermittelt werden, wahrt die Rechte der Patienten, ohne dass das Zertifizierungsverfahren selbst beeinträchtigt wird.

8.4 Auskunft aus dem Gemeinsamen Krebsregister

Eine Petentin hatte sich bei uns darüber beschwert, dass das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen ihr die Auskunft zur konkreten Todesursache einer Angehörigen verweigert habe.

Die Auskunftserteilung zu Daten aus dem Gemeinsamen Krebsregister ist im Krebsregistergesetz (KRG) geregelt.[170] Danach hat das Gemeinsame Krebsregister auf Antrag der erkrankten Person einem von ihr benannten Arzt oder Zahnarzt mitzuteilen, ob und welche Eintragungen zu ihrer Person gespeichert sind. Der Arzt oder Zahnarzt darf die Patientinnen und Patienten über die Mitteilung des Gemeinsamen Krebsregisters nur mündlich oder durch Einsicht in die Mitteilung informieren. Weder die schriftliche Auskunft des Gemeinsamen Krebsregisters noch eine Ablichtung oder Abschrift der schriftlichen Auskunft darf an diese weitergegeben werden. Auch mit Einwilligung der erkrankten Person darf der Arzt oder Zahnarzt die ihm erteilte Auskunft weder mündlich noch schriftlich an Dritte weitergeben.

Die Regelung des KRG scheint auf den ersten Blick die Auskunftsrechte der Betroffenen stark einzuengen. Aus der Gesetzesbegründung geht jedoch hervor, dass auf diese Weise die medizinische Beratung und ein Aufklärungsgespräch durch das ärztliche Personal gewährleistet und bei möglichen Problemen eine ärztliche Krisenintervention sichergestellt werden soll. Kern dieser Vorschrift ist, insbesondere sog. Negativ-Atteste unmöglich zu machen. Ein Negativ-Attest wäre dann gegeben, wenn eine Person, der bekannt ist, dass sie nicht an Krebs erkrankt ist und für die auch keine Meldung im Gemeinsamen Krebsregister vorliegt, sich diese Tatsache durch ein Auskunftsbegehren beim Gemeinsamen Krebsregister oder bei einem anderen Krebsregister in anderen Bundesländern zunutze macht, um sich z. B. gegenüber einem Versicherungsunternehmen Vorteile zu verschaffen. Die Bedeutung dieses Anliegens hat der Bundesgesetzgeber insbesondere dadurch unterstrichen, dass er einen Verstoß gegen diese Regelung unter Strafe gestellt hat.

Mit dem im April in Kraft getretenen Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister[171] hat der Bundesgesetzgeber die Länder verpflichtet, einheitliche Regeln für klinische Krebsregister zu erlassen.

Die Regelung zur Auskunftserteilung ist hinsichtlich der beim Gemeinsamen Krebsregister gespeicherten Daten abschließend. Anders als z. B. das neue Patientenrechtegesetz sieht das KRG gerade keine Auskunft gegenüber Angehörigen vor. In den überwiegenden Fällen werden die behandelnden Einrichtungen das Auskunftsersuchen der Angehörigen ausreichend beantworten können, soweit die Patientenunterlagen nicht nach Ablauf der Aufbewahrungsfristen bereits vernichtet worden sind.

170 § 9 KRG

171 BGBl. I, S. 617

8.5 Ärztliche Schweigepflicht im MVZ

Aufgrund einer Beschwerde untersuchten wir in einem Medizinischen Versorgungszentrum (MVZ), auf welchem Wege die ärztliche Schweigepflicht auch zwischen den verschiedenen Ärzten und anderen Beschäftigten gewährleistet wird.

Im Gegensatz zu Praxen einzelner niedergelassener Ärzte, in denen ein Arzt allein oder allenfalls zwei oder drei Ärzte im Rahmen einer Gemeinschaftspraxis zusammen behandeln, ist in einem MVZ eine Vielzahl von Ärzten verschiedener Fachgebiete tätig. In einem MVZ haben die Patienten die Erwartung, dass sie trotz der Vielzahl der Ärzte nur einen bestimmten einzelnen Arzt aufsuchen, der sie behandelt. Insoweit vertrauen sie auf die ärztliche Schweigepflicht innerhalb des MVZ. Anders als in einer Gemeinschaftspraxis, in der für den Patienten offensichtlich ist, dass sich die wenigen Ärzte bei Abwesenheit gegenseitig vertreten, rechnet der Patient bei einem MVZ nicht damit, dass alle dort Tätigen Zugriff auf die Patientendaten haben.

Unsere Prüfung ergab, dass in dem MVZ das gesamte medizinische Personal auf alle Patientendaten zugreifen konnte, ohne dass für derart vielfältige Zugriffe eine Erforderlichkeit bestand. Das MVZ sah zunächst technisch keine Möglichkeit, die Zugriffsmöglichkeiten einzuschränken.

Das Vertrauen in die Zuverlässigkeit der eigenen Beschäftigten unbenommen, darf sich die Einrichtung dennoch nicht ausschließlich darauf Verlassen, dass alle ihre Beschäftigten stets nur auf die Daten derjenigen Patienten zugreifen, mit denen sie unmittelbar zu tun haben. Sie benötigt daher Software, die es ihr ermöglicht, die eigenen organisatorischen Abläufe so abzubilden, dass Zugriffsrechte an den Erforderlichkeiten ausgerichtet werden können.

Der Effektivität eines Zugriffskonzepts sind zwar natürliche Grenzen gesetzt. So kommen Beschäftigte, die als Gehilfen für eine große Zahl von untereinander schweigepflichtigen Ärzten tätig sind, zwangsläufig mit den Akten all dieser Ärzte in Berührung. Wo Zugriffsrechte nicht ausreichend eng gesetzt werden können, muss es zumindest möglich sein, im Nachhinein nachvollziehen zu können, wer welche Akte eingesehen hat. Unberechtigte Zugriffe können aufgeklärt, ggf. Auskunft an die Patienten erteilt werden.

Im gegebenen Fall bot die eingesetzte Software rudimentäre, bisher ungenutzte Funktionen zur Rechteverwaltung. Wir haben das MVZ aufgefordert, die organisatorischen Abläufe zu analysieren, zu entscheiden, inwieweit die genannten Funktionen genutzt werden können, um die Gewährleistung der ärztlichen Schweigepflicht zu stärken, für die Nachvollziehbarkeit lesender Zugriffe auf Patientenakten zu sorgen und die Patienten über die unvermeidliche Breite der bestehenden Zugriffsrechte bei der Erstvorstellung zu informieren.

MVZ sind wie alle medizinischen Einrichtungen mit Beschäftigten, die untereinander schweigepflichtig sind, bei der Beschaffung der eingesetzten Software verpflichtet, solche Produkte zu wählen, die datenschutzgerecht betrieben werden können. Möglichkeiten für den Zugriffsschutz und die Nachvollziehbarkeit des Umgangs mit Patientenakten sind auszuschöpfen.

8.6 Online-Terminvereinbarungen in Arztpraxen

Verschiedene Dienstleister bieten Patienten die Möglichkeit, online Behandlungstermine in Arztpraxen zu buchen. Dies wird oft mit dem Angebot gekoppelt, Patienten an anstehende Termine per SMS zu erinnern. Wir untersuchten in drei Fällen, ob hierbei die ärztliche Schweigepflicht gewahrt wird.

Die untersuchten Dienste versprechen den Patienten Hilfe bei der Suche nach kurzfristigen Terminen bei Ärzten bestimmter Fachrichtungen. Mit wenigen Klicks kann man Praxen suchen und unter den dort freien Terminen wählen. Bei einem von uns geprüften Dienst können dem Arzt bereits vorab Informationen über den Anlass des Arztbesuchs mitgeteilt werden. Nicht selten werden die Eintragungen einiges über den jeweiligen Gesundheitszustand verraten.

Vielfach ist den Patienten unklar, dass die Daten, die sie bei dem Webdienst eintragen, noch nicht der ärztlichen Schweigepflicht unterliegen – auch dann nicht, wenn das entsprechende Formular in die Webseite der Praxis eingebunden ist. Die Anbieter müssen diesen Sachverhalt daher klarstellen und die Nutzenden bitten, sich mit der Verarbeitung ihrer Daten durch Personen einverstanden zu erklären, die keiner Schweigepflicht unterliegen.

Umgekehrt lassen Ärzte ihre Termine durch den genannten Anbieter verwalten. Dabei darf dieser den Namen der bestellten Patienten höchstens dann erfahren, wenn sie schriftlich den jeweiligen Arzt von der Schweigepflicht gegenüber dem Anbieter (und ggf. die von ihm eingeschalteten Dienstleister) befreit haben. Gleiches gilt, wenn der Arzt den Anbieter bittet, Patienten an Termine zu erinnern, die nicht über dessen Portal gebucht wurden. In einem der untersuchten Fälle hatte die auftraggebende Praxis diese unbedingt erforderliche Sorgfalt missen lassen. Wir mussten daher einen Datenschutzverstoß feststellen.

Ein zweiter Anbieter setzte ein komplexes kryptografisches Verfahren ein, um zu garantieren, dass die auftraggebenden Arztpraxen die alleinige Kontrolle über ihre Daten behalten. Leider versäumte es der Anbieter, das Verfahren einer unabhängigen sachverständigen Kontrolle zu unterziehen. Es wies vermeidbare Schwachstellen auf, die zur Offenlegung von Daten der Praxen hätten genutzt werden können. Auf unsere Aufforderung hin wurden die Schwachstellen behoben.

Am einfachsten war die Lage im dritten überprüften Fall: Es werden nur die zur Buchung und Terminerinnerung unbedingt notwendigen Daten über eine sichere Verbindung erhoben. Eine weitergehende Verwaltung der Patientendaten findet über die Plattform nicht statt.

Dienste zur Online-Vergabe von Behandlungsterminen müssen sowohl rechtlich durch gesetzeskonform ausgestaltete Vertragsbeziehungen zwischen Arztpraxen und Dienstleistern als auch technisch durch sorgfältig eingesetzte Sicherheitstechniken abgesichert werden. Für die Patienten muss transparent sein, wie weit die ärztliche Schweigepflicht reicht. Sollen Daten außerhalb dieses Bereichs bei den Anbietern verarbeitet werden, bedarf es ihres ausdrücklichen Einverständnisses.

8.7 Personalausweiskopien in Arztpraxen

Mehrfach erhielten wir Beschwerden, dass in Arztpraxen Kopien des Personalausweises zur Patientenakte genommen würden.

Eine Identifizierung der Versicherten mittels Personalausweis kann nur in Einzelfällen, etwa bei begründeten Zweifeln an der Identität des Versicherten, als zulässig angesehen werden. Ohne Vorliegen besonderer Anhaltspunkte ist ein solches Vorgehen unzulässig. Es ist ausreichend, dass sich die Person mit ihrer Krankenversichertenkarte identifiziert. Personalausweisdaten sind in aller Regel für den Abschluss und die Durchführung eines Behandlungsvertrages oder die Abrechnung der erbrachten Leistungen nicht erforderlich.

Das Anfertigen von Ausweiskopien und deren Ablage in der Patientenakte ist darüber hinaus in keinem Fall zulässig. Für eine mögliche Identitätskontrolle genügt die Vorlage des Ausweises. Darüber hinaus ist zu berücksichtigen, dass die Speicherung der auf dem Personalausweis neben Name und Anschrift vorhandenen Daten[172] in der Patientenakte zur Erfüllung des Vertrags ebenfalls nicht erforderlich und damit unzulässig ist. Die betroffenen Praxen haben auf unsere Aufforderung hin die in den Patientenakten abgelegten Personalausweiskopien vernichtet und uns mitgeteilt, dass sie künftig auf das Kopieren von Personalausweisen verzichten.

Es ist ausreichend, wenn sich die erkrankte Person mit der Krankenversichertenkarte gegenüber der Praxis ausweist. In Ausnahmefällen kann die Vorlage des Personalausweises zum Abgleich der Identität verlangt werden, z. B. wenn im Einzelfall konkrete Anhaltspunkte für einen Missbrauch der Krankenversichertenkarte vorliegen. Die Fertigung einer Kopie ist in jedem Fall unzulässig.

172 Wie die Personalausweisnummer, Größe, Augenfarbe, Geburtsort und ausstellende Behörde

8.8 Irreguläres bei den Kinder- und Jugendgesundheitsdiensten

Für die Durchführung der Einschulungsuntersuchungen und anderer Aufgaben speichern die Kinder- und Jugendgesundheitsdienste (KJGD) der Bezirke zum Teil sensitive Angaben über eine große Zahl von Kindern. Bei der Einführung datenschutzgerechter Software-Systeme, der technischen Gewährleistung der ärztlichen Schweigepflicht und der sicheren Ablage von Papierakten tut man sich schwer.

Wenn der öffentlichen Verwaltung für die Erfüllung ihrer Aufgaben sensitive Angaben über Familien und Kinder anvertraut werden, so steht dahinter die Erwartung, dass diese Angaben sicher verwahrt und nur denjenigen zur Kenntnis gebracht werden, die sie benötigen. Um dies auch im Zeitalter komplexer Software-Systeme zu gewährleisten, müssen bei der Einführung neuer Technik gesetzlich festgelegte Schritte gegangen und unsere Behörde einbezogen werden.

Bei einer Kontrolle eines Dienstes mussten wir feststellen, dass jahrelang eine „wild" eingeführte und ungeprüfte Software eingesetzt wurde. Wenngleich der Wunsch der KJGD-Beschäftigten nach technischer Unterstützung verständlich und ihre Frustration wegen deren schleppender Einführung nachvollziehbar ist, darf in Eigenregie getroffene Abhilfe nicht zulasten der Betroffenen gehen. Die Vertraulichkeit der Daten ist zu wahren, ein Zugriff auf Daten darf nur im Rahmen der Erforderlichkeit gewährt werden. Im Nachhinein muss nachvollziehbar sein, was mit den Daten geschehen ist. Weder in dem kontrollierten noch in einem weiteren KJGD, zu dem wir zur Beratung gerufen wurden, wird diesen gesetzlichen Vorgaben vollständig entsprochen.

In einem zweiten Fall war zu bemängeln, dass die Regelung zu Aktenhaltung und -zugriff den schweigepflichtigen Ärztinnen und Ärzten des KJGD die Kontrolle darüber entzieht, wer die von ihnen aufgenommenen Daten sieht. In einem exemplarischen Fall hatte eine vormals mit einem Fall beschäftigte Sozialarbeiterin Informationen aus der aktuellen ärztlichen Akte an das Jugendamt übermittelt, ohne dass dies vorher mit der verantwortlichen Ärztin abgesprochen worden war. In dem letztgenannten KJGD mussten wir auch feststellen, dass auch anderweitig mit den Papierakten nicht angemessen umgegangen wurde: Sie lagerten teilweise in nicht abgeschlossenen Aktenschränken in einem Raum, der auch Beschäftigten anderer bezirklicher Stellen zugänglich war.

Die Einführung des nunmehr anvisierten neuen Software-Systems für die KJGD werden wir intensiv begleiten und auf eine sachgemäße Regelung des Zugriffs auf Papier- und elektronische Akten hinwirken.

Zwischen den Beschäftigten der KJGD und gegenüber anderen Stellen ist die Schweigepflicht zu wahren, wofür die Bezirke die sachlichen Voraussetzungen zu schaffen haben. Nur sorgfältig und datenschutzkonform eingeführte IT-Systeme werden den Erwartungen der Menschen an den Schutz ihrer Daten gerecht.

8.9 Diebstahl von Gesundheitsdaten

Mehrere Computer eines sozialen Dienstes wurden entwendet und die auf ihnen ungeschützt gespeicherten Daten der betreuten Personen damit Dritten zugänglich.

Soziale Dienste speichern auf ihren Rechnern sensitive Daten über die betreuten Personen, neben allgemeinen Angaben auch solche zu Gesundheitszustand und Biographie. Werden die elektronischen Akten der Betreuten dezentral geführt, besteht an all diesen Orten die Gefahr, dass Dritte sich die Daten aneignen, sei es, dass sie sich Geldmittel durch den Verkauf gestohlener Computertechnik beschaffen wollen, sei es, dass Neugier oder Misstrauen sie treibt.

Die Vergabe von Kennwörtern für die Anmeldung am Betriebssystem der Computer schützt nur gegen die einfachsten Versuche, sich Zugang zu den Daten zu verschaffen. Wer durch Diebstahl oder längeren physischen Zugriff auf das Gerät Verfügungsgewalt über einen derart „geschützten" Rechner erlangt, dem stehen die Daten komplett offen. Zwei Strategien helfen: Die Verschlüsselung der Speichermedien mobiler Geräte – nicht nur der Festplatten, sondern auch der USB-Sticks und anderer eingesetzter Sicherungsmedien – sowie bei allen stationären Geräten eine Zentralisierung der Datenspeicherung.

Der betroffene Sozialdienst wählte mit unserer Zustimmung den zweiten Weg. Wir haben ihn dahingehend beraten, bei der Anbindung der Zweigstellen besondere Sorgfalt anzuwenden: Es muss ein sicherer Verbindungskanal aufgebaut werden, der nicht durch Fehler der Nutzenden geschwächt werden kann. Diese Sicherheit wird durch Verschlüsselung und gegenseitige Authentisierung der verbundenen Geräte in einem virtuellen privaten Netzwerk erreicht.

Sensitive Daten dürfen auf Geräten, die leicht gestohlen werden können, nicht unverschlüsselt gespeichert werden.

8.10 Veröffentlichung von Patientendaten

Wir sind darauf aufmerksam geworden, dass die Kassenärztliche Vereinigung (KV) in ihrem Mitteilungsblatt (KV-Blatt) die Anfangsbuchstaben des Vor- und Nachnamens, den Wohnort, das Geburtsjahr sowie die Krankenkasse und die Versichertennummer von Personen veröffentlichte, um auf Medikamentenmissbrauch hinzuweisen.

Diese Veröffentlichung ist datenschutzrechtlich unzulässig. Das KV-Blatt ist über das Internet-Angebot der KV abrufbar, sodass eine Kenntnisnahme von Dritten jederzeit möglich war. Bei der lebenslang gültigen Versichertennummer handelt es sich um ein personenbezogenes Datum. Dieses kann von diversen Dritten – z.B. Ärzten, Apothekern oder auch Beschäftigten von Krankenkassen – direkt der erkrankten Person zugeordnet werden. Zudem kann auch über die weiteren Angaben wie den Vornamen und ersten Buchstaben des Nachnamens sowie das Alter und den Bezirk eine Identifizierung der konkreten Person nicht ausgeschlossen werden.

Die KV hat entsprechend unserer Aufforderung die Veröffentlichung personenbezogener Daten im KV-Blatt eingestellt und die Darstellung betreffend Medikamentenmissbrauch geändert.

Soweit Informationen zum Medikamentenmissbrauch von Versicherten ohne Einwilligung oder Rechtsgrundlage veröffentlicht werden sollen, müssen diese Informationen stets anonymisiert werden, sodass nicht mehr auf die Identität der Versicherten geschlossen werden kann.

9 Beschäftigtendatenschutz

9.1 Dienstvereinbarung zur privaten Nutzung von Internet und E-Mail

Aus der Praxis

Die Dienstvereinbarung für den Einsatz der Internet-Technologie bei den Berliner Wasserbetrieben sah u. a. vor, dass über Internet-Zugriffe von Beschäftigten ein Protokoll geführt wird (unter Pseudonym). Eine Auswertung sollte nur anonymisiert oder namentlich bei begründetem Verdacht auf Verstoß gegen die Dienstvereinbarung erfolgen.

Bei den erhobenen Daten zum Internet-Nutzungsverhalten handelt es sich um Personaldaten. Auch die Speicherung der Nutzungsdaten unter Pseudonym ist eine Verarbeitung personenbezogener Daten, die durch keine Rechtsvorschrift erlaubt wird.[173] Die vollständige Protokollierung des Nutzungsverhaltens unter Pseudonym ist als eine Vollkontrolle der Beschäftigten zu werten und stellt einen schwerwiegenden Eingriff in ihr Persönlichkeitsrecht dar. Sie ist daher nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig.

Aufgrund unserer Interventionen werden die vollständigen Internet-Log-Daten nunmehr für maximal zehn Tage gespeichert, um ggf. Fehleranalysen durchführen zu können. Sie dürfen nicht für Verhaltens- und Leistungskontrollen herangezogen werden. Nach zehn Tagen werden die Daten automatisch gelöscht.

Auf Basis der o. g. Log-Daten werden wöchentlich nun folgende anonyme Reports automatisch angefertigt:

- die 100 häufigsten Domains der am meisten im Internet aufgerufenen Webseiten
- die 100 häufigsten Domains der Internet-Seiten mit dem größten Datenaufkommen

Bei Auffälligkeiten werden auf Anforderung eines Gremiums spezielle Reports erstellt. Diese werden dann für die Zukunft für einen festgelegten Zeitraum

173 § 2 Abs. 2 Berliner Datenschutzgesetz i.V. m. § 32 Bundesdatenschutzgesetz

wöchentlich automatisch angefertigt. Es werden nutzerbezogene Auswertungen nach einer bestimmten aufgerufenen Internet-Seite (URL) erfolgen. Nach einem bestimmten Benutzer (UserID) werden Auswertungen nur für die Zukunft vorgenommen, wenn das Gremium einen konkreten personenbezogenen Anfangsverdacht festgestellt hat. Die Betroffenen müssen in diesem Fall nicht vorab unterrichtet werden, sondern sind nur im Nachhinein zu informieren.[174]

Eine anlasslose Protokollierung von Nutzungsdaten der Beschäftigten ist eine unzulässige Vorratsdatenspeicherung. Den berechtigten Interessen des Arbeitgebers bzw. Dienstherrn kann durch datensparsame Verfahren Rechnung getragen werden.

9.2 Übermittlung von Bewerberdaten durch die Deutsche Bahn International GmbH an Dritte

Aus der Praxis

Die DB International GmbH (DBI) übermittelte Unterlagen eines Bewerbers während eines laufenden Bewerbungsverfahrens an ein anderes Unternehmen, um mit ihm für Akquisitionszwecke Werbung zu machen. Die Übermittlung der Unterlagen erfolgte ohne vorherige Kenntnis des Bewerbers. Die DBI begründete die Übermittlung mit der allgemein herrschenden Praxis, in einem Angebotsprozess wegen der langen Akquisitionsdauer auch Experten zu berücksichtigen, die erst künftig im Dienst des Unternehmens stehen. Ferner wurde darauf hingewiesen, dass der Personalbogen eine Einwilligungserklärung des Mitarbeiters enthalte, seinen Lebenslauf an Dritte zu Zwecken der Akquisition und Durchführung eines Projekts zu übermitteln.

Die Übermittlung von Bewerberdaten an Dritte ist zulässig, wenn dies zur Begründung des Beschäftigungsverhältnisses erforderlich ist[175] oder die Einwilligung der betroffenen Person vorliegt.[176]

174 Siehe § 5 Abs. 3 der Dienstvereinbarung über die Nutzung des Internets und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung
175 § 32 Abs. 1 BDSG
176 § 4a BDSG

Die Einverständniserklärung wurde vom Betroffenen im vorliegenden Fall erst nach der Übermittlung seiner Bewerbungsunterlagen abgegeben und erfolgte vorbehaltlich einer rechtzeitigen einzelfallbezogenen Information bezüglich der konkreten Übermittlung dieser Daten. Zudem stand die Einwilligung unter der Bedingung, dass die DBI die tatsächliche Erforderlichkeit der Übermittlung der einzelnen Datensätze für den Abschluss oder die Erfüllung eines Vertrages prüft. Aus dem uns zur Verfügung gestellten E-Mail-Verkehr ergab sich, dass die Weitergabe der Unterlagen zum Zeitpunkt der Übermittlung von der zuständigen Leitungskraft der DBI gar nicht vorgesehen bzw. als notwendig angesehen wurde.

Da damit weder eine wirksame Einwilligung des Betroffenen noch die Erforderlichkeit der Datenübermittlung durch die DBI vor Einstellung des Bewerbers vorlagen, erfolgte die Übermittlung seiner Bewerbungsunterlagen an das andere Unternehmen ohne Rechtsgrundlage und war damit rechtswidrig. Die DBI sicherte zu, geeignete Maßnahmen zu ergreifen, um zu verhindern, dass sich derartige Vorfälle wiederholen.

Bewerberdaten sind ebenso vertraulich zu behandeln wie Daten von Beschäftigten.

9.3 Anonymität von Beschäftigtenbefragungen

Mehrere Senatsverwaltungen planen Beschäftigtenbefragungen. Kernstücke der Fragebögen sind neben Angaben zu der Person und Organisationseinheit detaillierte Fragen zur Arbeitszufriedenheit und dem Allgemeinbefinden wie Arbeitsbelastung, soziale Beziehungen, Verhältnis zwischen Arbeit und Privatleben, Einflüsse der Arbeitsumgebung, Zufriedenheit und Verbundenheit mit dem Behördenbereich sowie subjektive Einschätzungen der Befragten zu Führungsqualitäten ihrer jeweiligen Vorgesetzten und Leitungskräfte. Die Fragebögen der Senatsverwaltung für Bildung, Wissenschaft und Forschung sehen sogar Angaben zur Gesundheit bzw. zu konkreten Gesundheitsbeschwerden sowie emotionalen Befindlichkeiten der Befragten vor.

Die Teilnahme an der Befragung soll anonym und den Beschäftigten freigestellt sein. Die Fragebögen wurden uns im Entwurf zur Prüfung vorgelegt.

Der Dienstherr bzw. Arbeitgeber darf personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses erheben, verarbeiten oder nutzen, wenn dies z.B. für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.[177]

Bei den genannten Daten handelt es sich um sensitive Personaldaten der Beschäftigten, die besonders schützenswert sind. Eine Erforderlichkeit zur Erhebung dieser Daten in personenbezogener Form ist für arbeits- oder dienstrechtliche Zwecke nicht gegeben. Die Fürsorgepflicht des Dienstherrn bzw. Arbeitgebers gebietet zwar, dass seine Beschäftigten nicht übermäßig belastet werden und keinen Gesundheitsgefahren ausgesetzt sind. Gleichwohl sind die o. g. Fragen sehr persönlich und gehen weit über die gebotene Fürsorgepflicht hinaus. Ebenso ist eine Einwilligung der Beschäftigten grundsätzlich wegen ihrer sozialen Abhängigkeit problematisch und daher in der Regel unwirksam. Beschäftigtenbefragungen können insoweit nur auf freiwilliger Basis und anonym erfolgen. Dafür ist sicherzustellen, dass keinerlei Rückschlüsse auf die Person der Befragten möglich sind.

Dies ist jedoch nicht einfach zu gewährleisten. Anonymität liegt jedenfalls dann vor, wenn niemand einen ausgefüllten Fragebogen einer Person zuordnen kann. Eine derartige Zuordnung kann jedenfalls auf Angaben über die antwortende Person basieren, die Dritten, z.B. Vorgesetzten, bekannt sind. Dazu gehören Alter, Berufserfahrung, Bildungsgrad oder Wohnort. Das Risiko der Herstellung eines Personenbezugs wächst mit der Zahl solcher Angaben, je nachdem wie viele Beschäftigte an der Befragung teilnehmen. Somit bedarf es sorgfältiger Prüfung, welche potenziell identifizierenden Angaben bei einer Beschäftigtenbefragung erhoben werden. Sie müssen sich strikt am Erkenntnisinteresse des Arbeitgebers ausrichten.

Ein häufiger Typ von Befragungen dient der Gewinnung von Hypothesen über Zusammenhänge, etwa zwischen dem Führungsverhalten von Vorgesetzten und der Motivation der Beschäftigten. Da die Einflussfaktoren noch unbekannt sind,

177 § 2 Abs. 2 BlnDSG i.V. m. § 32 BDSG

werden auch viele möglicherweise identifizierende Angaben erhoben. Daher ist es dem Arbeitgeber nicht erlaubt, die Befragung selbst durchzuführen. Er muss einen Dritten, z.B. ein wissenschaftliches Institut oder das Amt für Statistik Berlin-Brandenburg, mit der Durchführung beauftragen und darf nur vollständig anonymisierte Auswertungsergebnisse erhalten. Selbstverständlich muss auch in diesem Szenario die Freiwilligkeit der Teilnahme gewahrt werden, und der Arbeitgeber darf nicht erfahren, welche seiner Beschäftigten sich beteiligt haben.

Die zweite Variante von Befragungen geht bereits von einer Vermutung aus. Ein Umstand, den der Arbeitgeber beeinflussen kann, zieht eine bestimmte erwünschte oder unerwünschte Folge nach sich. Hierfür wird eine Bestätigung gesucht. Die hierzu eingesetzte Befragung darf nur Angaben enthalten, die sich auf den zu überprüfenden Zustand beziehen.

Schließlich wollen Arbeitgeber in anderen Fällen nur bestimmen, wo in ihrem Verantwortungsbereich bestimmte Probleme bestehen. Hier wird der Kreis der Befragten durch Fragen nach den Bereichen und Positionen, in denen sie tätig sind, stark eingegrenzt. Auf identifizierende Angaben muss in aller Regel verzichtet werden. Die Fragen sind darauf zu beschränken, den Problemzustand anhand bekannter Faktoren oder ihrer Auswirkungen festzustellen.

Wir raten dazu, das Ziel der Befragungen frühzeitig festzulegen und Mischformen zu vermeiden, da diese sich in aller Regel nicht datenschutzgerecht durchführen lassen.

Die Senatsverwaltungen sind unseren Empfehlungen gefolgt und haben zugesagt, die Befragung entweder dem Amt für Statistik Berlin-Brandenburg zu übertragen und auf den Zugang zu den Antworten der Beschäftigten zu verzichten oder die Fragebögen geeignet zu modifizieren.

Beschäftigtenbefragungen dürfen nur auf freiwilliger Basis durchgeführt werden. Es darf dem Arbeitgeber nicht möglich sein, im Zuge der Befragung Schlussfolgerungen über einzelne Beschäftigte zu ziehen.

9.4 Datenschutz bei einer Gewerkschaft

9.4.1 Beschäftigtendaten in Tarifauseinandersetzungen

Mehrere Beschäftigte beschwerten sich bei uns über einen Gewerkschaftssekretär, der im Rahmen seines Zugangsrechts[178] als Beauftragter einer im Betrieb vertretenen Gewerkschaft Beschäftigtendaten aus öffentlichen Aushängen im Betrieb erhoben hatte. Diese Daten hatte er mithilfe verschiedener Quellen um Informationen zu Funktionen, Stellenanteilen und Entgeltgrundlagen der einzelnen Beschäftigten angereichert. Die so erstellte Übersicht sollte der Gewerkschaft als verlässliche Grundlage in einer Tarifauseinandersetzung mit dem Arbeitgeber dienen.

Die Datenerhebung und -verarbeitung waren unzulässig. Da die Betroffenen nicht in die Erhebung und Verarbeitung eingewilligt hatten, hätte es einer legitimierenden Rechtsgrundlage bedurft.[179]

Spezielle Bestimmungen zur Datenverarbeitung innerhalb von gewerkschaftlich ausgerichteten Organisationen[180] waren in diesem Fall nicht anwendbar, da Beschäftigtendaten ohne Bezug auf eine Gewerkschaftszugehörigkeit der Betroffenen verarbeitet wurden. Auch auf die allgemeinen Regelungen des § 28 BDSG, die die Verarbeitung von Daten zu eigenen Geschäftszwecken im nicht-öffentlichen Bereich gestatten, konnte sich die Gewerkschaft nicht stützen. Zwar verfolgte sie mit dem Ziel, eine verlässliche Datengrundlage für die tarifliche Auseinandersetzung mit dem Arbeitgeber zu erstellen, grundsätzlich ein berechtigtes Interesse an der Datenverarbeitung. Jedoch war diese weder geeignet noch erforderlich, um die bezweckten Ziele zu erreichen. Insbesondere war aufgrund der willkürlichen Profilbildung der Beschäftigten nicht gewährleistet, dass die Daten aussagekräftig sind. Zudem hätte die Gewerkschaft sich gleichermaßen anonymisierter Daten bedienen können, um die Tarifsituation innerhalb des Betriebes darzustellen. Nicht zuletzt überwogen die schutzwürdigen Interessen der Betroffenen an der Geheimhaltung ihrer

178 § 2 Abs. 2 Betriebsverfassungsgesetz
179 § 4 Abs. 1 BDSG
180 § 28 Abs. 9 BDSG

Beschäftigtendaten gegenüber dem Gewerkschaftsinteresse, die Daten für ihre Auseinandersetzung mit dem Arbeitgeber zu nutzen.

Das grundrechtlich geschützte Zugangsrecht von betrieblichen Gewerkschaftsbeauftragten berechtigt sie nicht zur willkürlichen Datenbeschaffung.

9.4.2 Weitergabe von Mitgliederdaten für „Rückgewinnungsgespräche“

Ein ehemaliges Gewerkschaftsmitglied fragte uns, ob die Gewerkschaft ohne seine Kenntnis und Einwilligung Informationen über die Mitgliedschaft an eine Kollegin weitergeben durfte. Die Kollegin war ihrerseits Mitglied der Gewerkschaft und mit der Durchführung eines sog. Rückgewinnungsgesprächs betraut worden. Damit sollen austrittswillige Mitglieder im Rahmen eines persönlichen Gesprächs „zurückgeholt“ und anderenfalls statistische Daten über die Austrittsgründe gesammelt werden. Durchgeführt werden die Gespräche von Gewerkschaftsmitgliedern in den jeweiligen Betrieben, die zu ehrenamtlichen Vertrauensleuten gewählt oder ernannt wurden.

Die Weitergabe und Nutzung von Mitgliederdaten an eine gewählte oder ernannte Vertrauensperson einer Gewerkschaft ist zulässig, wenn sie für die Tätigkeit der Organisation erforderlich ist.[181] Die Rückgewinnungsgespräche dienen einer positiven Mitgliederentwicklung in der Gewerkschaft, die notwendig ist, um die satzungsmäßigen Aufgaben der Organisation zu erfüllen. Da es sich bei den Vertrauensleuten um Gewerkschaftsmitglieder handelt, bleiben die im Rahmen der Gespräche genutzten Daten innerhalb der Organisation. Um sicherzustellen, dass Vertrauensleute auch vertrauensvoll mit den ihnen in ihrer Funktion bekannt gegebenen Informationen umgehen, werden diese zudem auf das Datengeheimnis verpflichtet,[182] wodurch ihre Schweigepflicht auch mit Ende ihrer Tätigkeit fortbesteht. Unter diesen Voraussetzungen ist die Datenweitergabe und -nutzung für Zwecke der Mitgliederrückgewinnung zulässig. Dies gilt auch für die Datenerhebung im Rahmen eines solchen Gesprächs (z.B. Austrittsgründe). Hierbei sind die Betroffenen vorab auf die Freiwilligkeit ihrer Angaben hinzuweisen.[183]

Gleichwohl ist die Benennung von Beschäftigten eines Betriebs zu Vertrauensleuten im eigenen Betrieb kritisch, da nicht ausgeschlossen werden kann, dass auch Personen mit Personalverantwortung und Weisungsbefugnissen zur Vertrauensperson ernannt werden. In einer solchen Konstellation ist nicht sichergestellt, dass das ausscheidende Mitglied freiwillig am Rückgewinnungsgespräch teilnimmt, wodurch auch die im Gespräch erfolgte Datenerhebung unzulässig wäre. Zudem wächst dadurch die Gefahr, dass Beschäftigte, die innerhalb einer Dienststelle oder eines Betriebs auf Personaldaten zugreifen dürfen, diese pflichtwidrig an eine Gewerkschaft weitergeben. Im vorliegenden Fall lagen solche Umstände nicht vor. Um sicherzustellen, dass die Datenerhebung im Rückgewinnungsgespräch freiwillig erfolgt, sollten die Gewerkschaftssekretariate die Betroffenen vorab um ihr Einverständnis zur Teilnahme am Gespräch bitten und dabei die vorgesehene Vertrauensperson ausdrücklich benennen.[184]

Die Erhebung und Nutzung von Mitgliederdaten für Zwecke der Rückgewinnung von Gewerkschaftsmitgliedern sind zulässig, sofern die freiwillige Teilnahme an dem Rückgewinnungsgespräch gewährleistet ist.

181 § 28 Abs. 9 BDSG
182 § 5 BDSG
183 § 4 Abs. 3 Satz 2 BDSG
184 § 9 Satz 1 BDSG

10 Wohnen und Umwelt

10.1 Datenschutz bei einem Online-Makler

Aus der Praxis

Ein Betreiber eines Immobilienportals bot in Kooperation mit der SCHUFA eine kostenpflichtige Möglichkeit zur Selbstauskunft über die zur eigenen Person bei der SCHUFA gespeicherten Bonitätsdaten an. Das Angebot war mehrfach Gegenstand von Beschwerden, da sich bei ausreichender Kenntnis über eine Person scheinbar auch Dritte aufgrund mangelnder Prüfung der Daten Informationen über eine andere Person durch die Online-Auskunft verschaffen konnten.

Für die Anfrage verlangte der Anbieter zunächst einige personenbezogene Daten der antragstellenden Person. Bei böswilliger Absicht und hinreichender Kenntnis konnten hier jedoch auch Daten Dritter verwendet werden, sodass ein Identitätsmissbrauch möglich war. Bedenklich war auch, dass die über das Internet erfolgende Anfrage zur Bonität begonnen werden konnte, ohne dass sich die oder der Betroffene ausreichend identifizieren musste, da bereits im ersten Schritt des Verfahrens Daten an die SCHUFA weitergegeben wurden. Zwar wies der Anbieter auf seiner Internetseite darauf hin, dass der Abruf der Bonitätsinformationen nur zur eigenen Person erfolgen darf, eine weitere Überprüfung, wer diese Auskunft beantragt hatte, erfolgte jedoch nicht.

Eine Prüfung des Verfahrens vor Ort bei dem betreffenden Anbieter ergab, dass manche Befürchtungen der Petenten unbegründet waren, gleichwohl jedoch auch Sicherheitsmängel bei dem Anbieter bestanden. Wir konnten feststellen, dass viele Sorgen der Petenten allein daraus entstanden sind, dass das Verfahren in seiner damaligen Form für die Nutzenden nicht ausreichend transparent war. Deshalb haben wir den Anbieter aufgefordert, die festgestellten Sicherheits- und Transparenzmängel zu beheben, um so die Sicherheit und den Schutz der Kundendaten vor missbräuchlicher Verwendung zu erhöhen. Positiv hervorzuheben ist, dass der Anbieter sich kooperativ verhalten hat und dank unserer Hinweise eine Verbesserung der Datensicherheit bei dem Angebot erreicht wurde. Wir führen weitere Gespräche mit dem Anbieter, um noch bestehende Mängel hinsichtlich der Transparenz des Verfahrens zu beheben.

Die Nutzung von Angeboten im Internet bietet viele Vorteile, birgt aber auch die Gefahr, dass personenbezogene Daten von Dritten missbraucht werden. Dies zu verhindern, ist nicht allein Sache der Nutzenden, sondern auch die datenverarbeitenden Unternehmen haben stets dafür zu sorgen, dass die Kundendaten gegen Diebstahl und Missbrauch geschützt sind.

10.2 Das Liegenschaftskataster als Marketing-Reservoir?

Aus der Praxis

Vor dem Hintergrund des zunehmend angespannten Immobilienmarkts haben uns vermehrt Beschwerden über unerwünschte Werbeschreiben von Immobilienmaklern erreicht. Oft erhielten die Betroffenen mehrere Briefe von verschiedenen Maklern mit der Anfrage, ob sie ihr Grundstück oder ihre Eigentumswohnung verkaufen möchten. Dabei war für die Betroffenen unklar, woher die Makler die Informationen hatten, dass die Angeschriebenen Eigentümer einer Immobilie sind und welche Anschrift diese hat.

Unsere Ermittlungen haben ergeben, dass die Daten in einigen Fällen von Adresshändlern erworben wurden, aber teilweise auch aus dem Liegenschaftskataster der bezirklichen Vermessungsämter stammten. Die Vermessungsämter dürfen Eigentümerdaten grundsätzlich nur an Personen herausgeben, die ein berechtigtes Interesse an dem Erhalt der Daten haben.[185] Dieses kann z.B. vorliegen, wenn ein Makler zum Kauf der konkreten Immobilie beauftragt wurde. Ein solches berechtigtes Interesse liegt aber nicht bei gebietsweisen Massenabfragen zu bloßen Werbezwecken vor.

Die Verarbeitung und Nutzung der Eigentümerdaten zu Werbezwecken ohne Einwilligung des Betroffenen ist in jedem Fall rechtswidrig. Ohne Einwilligung dürfen nur bestimmte Daten (z.B. Name, Anschrift, Berufsbezeichnung) zu Werbezwecken verwendet werden, wenn diese Daten aus allgemein zugänglichen Quellen erhoben wurden, wie z.B. dem Telefonbuch oder dem Bran-

185 § 17 Abs. 1 Satz 2 Nr. 2 Vermessungsgesetz Berlin; siehe auch 18.3.3

chenverzeichnis.[186] Da Eigentümerdaten nicht dazu gehören und da weder die Datenbanken von Adresshändlern noch das Liegenschaftskataster allgemein zugängliche Quellen darstellen, dürfen diese Daten nicht zur Werbung verwendet werden.

Wir mussten zahlreiche Bußgeldverfahren gegen Unternehmen einleiten, die sich nicht an dieses Verbot gehalten haben. Außerdem hat die Senatsverwaltung für Stadtentwicklung und Umwelt auf unsere Bitte die bezirklichen Vermessungsämter auf diese Problematik aufmerksam gemacht. Wir konnten durchsetzen, dass bei Abrufen von Eigentümerdaten aus dem Liegenschaftkataster darauf hingewiesen wird, dass die Daten nicht zu Werbezwecken missbraucht werden dürfen. Zusätzlich sind wir an die entsprechenden Berufsverbände herangetreten. Wir haben diese ebenfalls auf das Verbot und das bei Zuwiderhandlung drohende Bußgeld hingewiesen, um die Branche für diese Problematik zu sensibilisieren.

Diesen Weg werden wir weiter beschreiten, um zu erreichen, dass die Menschen künftig nicht mehr mit unerwünschter Werbung belästigt werden. Es bleibt aber unser Ziel durchzusetzen, dass Eigentümerdaten erst gar nicht zu Werbezwecken aus dem Liegenschaftskataster abgerufen werden können. Dazu müsste schon beim Abruf strenger überprüft werden, ob ein berechtigtes Interesse vorliegt. Im Rahmen der angekündigten Novellierung des Vermessungsgesetzes setzen wir uns dafür ein, dass der Begriff des berechtigten Interesses konkretisiert wird, um den bezirklichen Vermessungsämtern die Prüfung zu erleichtern, in welchen Fällen Eigentümerdaten herausgegeben werden dürfen und wann nicht.

Ein weiteres Problem besteht darin, dass die gegenwärtige Rechtslage vorsieht, dass besonders „zuverlässige“ Unternehmen von der Senatsverwaltung für Stadtentwicklung und Umwelt von der Pflicht befreit werden können, ihr berechtigtes Interesse bei jedem einzelnen Abruf darzulegen.[187] Wir werden uns im Zuge der genannten Novellierung des Vermessungsgesetzes ebenfalls dafür einsetzen, dass im Gesetz genauer definiert wird, welche Voraussetzungen ein Unternehmen bzw. ein Makler zu erfüllen hat, um als „zuverlässig“ zu

186 § 28 Abs. 3 Satz 2 Nr. 1 BDSG
187 § 17 Abs. 1 Satz 4 Vermessungsgesetz Berlin

gelten. Bislang geht die Senatsverwaltung ohne weitere Prüfung grundsätzlich von der Zuverlässigkeit aller Antragsteller aus. Diese wird nur dann verneint, wenn andere Tatsachen bekannt sind, z.B. dass der Antragsteller in der Presse als hochgradig straftatverdächtig in Erscheinung getreten ist. Außerdem möchten wir erreichen, dass solchen Unternehmen die Zuverlässigkeit nachträglich aberkannt wird, wenn sie gegen datenschutzrechtliche Vorschriften verstoßen. Die Senatsverwaltung für Stadtentwicklung und Umwelt hat zugesagt, uns bei der Erarbeitung der Gesetzesänderung frühzeitig zu beteiligen.

Den Missbrauch von Eigentümerdaten zu Werbezwecken verfolgen wir mit hohen Bußgeldern. Der Abruf Von Eigentümerdaten aus dem Liegenschaftskataster sollte künftig strenger reglementiert werden.

11 Forschung

11.1 Nationale Kohorte

Aus der Praxis

Für die Teilnahme an einer groß angelegten Langzeit-Bevölkerungsstudie zur Erforschung von häufigen chronischen Krankheiten sollen bundesweit 200.000 Frauen und Männer im Alter von 20 bis 69 Jahren gewonnen werden. Das Vorhaben wird vom Bundesministerium für Bildung und Forschung gefördert und von einem Netzwerk deutscher Forschungseinrichtungen durchgeführt, die dazu im Sommer den Verein „Nationale Kohorte e.V." gegründet haben. Mit den vorbereitenden sog. Pretests (Machbarkeitsprüfungen) hatten wir uns bereits 2011 befasst.[188] Nun soll die Hauptstudie beginnen. Die Rekrutierung, Untersuchung und Nachbeobachtung der an der Studie Teilnehmenden soll durch insgesamt 18 lokale Studienzentren erfolgen. Im Cluster Berlin-Brandenburg werden sich das Max-Delbrück-Centrum für Molekulare Medizin Berlin-Buch, das Institut für Sozialmedizin, Epidemiologie und Gesundheitsökonomie an der Charité Berlin und das Deutsche Institut für Ernährungsforschung Potsdam-Rehbrücke an dem Vorhaben beteiligen.

Kohortenstudien dienen in der epidemiologischen Forschung dazu, bestimmte Personengruppen über einen längeren Zeitraum bei ihrem biografischen „Vorrücken" (die Kohorte war eine römische Armee-Einheit) wissenschaftlich zu begleiten. Die Nationale Kohorte ist seit langem eine der größten entsprechenden Untersuchungen, die bundesweit durchgeführt wird.

In einer Basisuntersuchung werden alle Teilnehmenden zu ihrer Lebensweise und Krankheiten befragt, körperlich untersucht und einer Reihe von kognitiven Tests unterzogen. Darüber hinaus sollen von allen Teilnehmenden Biomaterialien, u. a. Proben vom Blut, Plasma, Speichel, gesammelt werden. Zusätzlich ist vorgesehen, Daten aus externen Quellen, z.B. bei Krankenkassen und bei der Deutsche Rentenversicherung Bund abzufragen, um u. a. Diagnose- und Abrechnungsdaten sowie Daten zum bisherigen Arbeitsleben zu erhalten. Auch

188 JB 2011, 8.1.3

frühere Wohnadressen sollen erhoben und im Hinblick auf mögliche Umweltbelastungen ausgewertet werden. Für ausgewählte Teilnehmende sollen zusätzliche Befragungen und Untersuchungen durchgeführt oder Magnetresonanztomographien (MRT) erstellt werden. Nach ca. vier bis fünf Jahren werden alle an der Studie Teilnehmenden zu einer Folgeuntersuchung eingeladen. Zudem werden sie alle zwei bis drei Jahre gebeten, Fragebögen zu ihrem Lebensstil sowie zu Erkrankungen auszufüllen. Sämtliche Daten aus den Studienzentren und den externen Quellen sollen pseudonymisiert in einer Studiendatenbank zentral zusammengeführt und dort vorgehalten werden. Für die Biomaterialien wird eine Biobank mit Sitz in München aufgebaut.

Aus wissenschaftlicher Sicht ist eine solche umfassende Gesundheitsstudie sicherlich zu begrüßen. Allerdings können die umfassenden Profile zur Gesundheit und zu den individuellen Lebensumständen der Probanden, die im Rahmen der Studie entstehen und für einen sehr langen Zeitraum vorgehalten werden, Begehrlichkeiten wecken, vor denen die Betroffenen geschützt werden müssen. Federführend wird das Vorhaben derzeit vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit betreut. Für die Datenerhebungen und -verarbeitungen der einzelnen Studienzentren in den Ländern sind die Länder einzubeziehen. In Berlin hat es dazu bereits erste Kontakte mit den Studienzentren gegeben. Neben einer Reihe von Einzelfragen sind insbesondere drei Punkte für die datenschutzrechtliche Bewertung wesentlich:

- Die Datenerhebungen, -verarbeitungen und -nutzungen sollen auf die Einwilligung der Teilnehmenden gestützt werden. Problematisch ist, dass die Daten- und Proben-Ressourcen im Laufe der Zeit externen Forschenden für gesundheitsbezogene Forschung zur Verfügung gestellt werden sollen. Zum Zeitpunkt der Entscheidung über die Studienteilnahme ist aber noch nicht klar, um welche Forschende, welche Zwecke und welche Daten es dabei gehen wird. Ob der Zugang zu den Daten gewährt wird, soll dann vom Verein „Nationale Kohorte" entschieden werden. Um die Rechte der Betroffenen abzusichern, müssen die dabei zugrunde gelegten Entscheidungskriterien bereits zum Zeitpunkt der Einwilligung konkret festgelegt und für die Betroffenen transparent gemacht werden. Zudem sollte ein Verfahren der Mitwirkung und Entscheidung der Betroffenen für die Datenfreigabe bei späteren Forschungsanfragen eingerichtet werden.

- Nach der Studienkonzeption sollen die einzelnen Studienzentren als Datenverarbeiter im Auftrag des Vereins „Nationale Kohorte“ tätig werden, sodass er gegenüber den Betroffenen datenschutzrechtlich verantwortlich ist und die Studienzentren nur im Rahmen der Weisungen des Vereins Daten verarbeiten dürfen. Fraglich ist, ob diese Verantwortungsverteilung mit den tatsächlichen Gegebenheiten übereinstimmt. Die Studienzentren sind die primären Ansprechpartner für die an der Studie Teilnehmenden und zeichnen medizinisch für die durchgeführten Untersuchungen und Tests verantwortlich. Aus den bisherigen Entwürfen zu den Einwilligungserklärungen geht nicht eindeutig hervor, dass der Verein „Nationale Kohorte“ verantwortliche Stelle ist. Zudem ist nicht ausgeschlossen, dass die Studienzentren eigene Forschung mit den erhobenen Daten betreiben wollen. Dies spricht nicht für eine Auftragsdatenverarbeitung.
- Es soll eine unabhängige Treuhandstelle eingerichtet werden, die die personenbezogenen Daten der Probanden durch Pseudonyme ersetzt und die Zuordnungen verwaltet. Gleichzeitig soll die Treuhandstelle dafür zuständig sein, bei den externen Datenquellen die Daten über die Probanden zu erheben. Wie die Treuhandstelle organisatorisch in die Studienstruktur eingebunden werden soll, ist bisher nicht geklärt. Davon abhängig ist die Frage, auf welcher Rechtsgrundlage diese tätig wird.

Nach Informationen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sollen noch Änderungen am Studienkonzept und an den Einwilligungserklärungen vorgenommen werden. Die Prüfung des Gesamtkonzepts durch den Bundesbeauftragten dauert an. Auch wir werden uns weiterhin in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder mit dem Vorhaben beschäftigen. Die Rekrutierung von Probanden ist für das Frühjahr 2014 geplant.

11.2 Evaluation des Neuköllner Modells

Die Hochschule für Wirtschaft und Recht (HWR) wurde von der Senatsverwaltung für Justiz und Verbraucherschutz mit der Evaluation des „Neuköllner Modells“ beauftragt. Das „Neuköllner Modell“ bezeichnet eine spezifische Anwendung des vereinfachten gerichtlichen Jugendverfahrens.[189] Seit Juni 2010 wird dieses beschleunigte Verfahren berlinweit mit dem Ziel eingesetzt, durch eine Verkürzung des Zeitraums zwischen der Tat und der strafrechtlichen Reaktion die pädagogische Wirksamkeit des Verfahrens zu erhöhen. Die HWR plante, zur Evaluation des Modells strafprozessuale Akten zu analysieren, vorhandene Statistiken auszuwerten, Interviews mit Experten aus Polizei, den Staatsanwaltschaften, der Richterschaft und Jugendgerichtshilfe sowie mit jugendlichen Straftätern bzw. Tatverdächtigen zu führen und Hauptverhandlungen zu beobachten. Die HWR bat uns um Beratung bei der Erstellung des Datenschutzkonzepts.

Das Vorhaben warf eine Reihe von Fragen auf. So war zu prüfen, ob die Beschäftigten der HWR die Akten bei der Staatsanwaltschaft selbst einsehen und daraus personenbezogene Daten erheben durften. Eine Übermittlung personenbezogener Daten aus Akten der Staatsanwaltschaft an Hochschulen zur wissenschaftlichen Forschung setzt voraus, dass die Nutzung anonymisierter Daten für die Durchführung der Forschungsarbeit nicht möglich oder die Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden ist.[190] Auf unsere Anregung erörterten die Forscher mit Vertretern der Senatsverwaltung für Justiz und Verbraucherschutz, ob die Daten durch die Staatsanwaltschaft anonymisiert zur Verfügung gestellt werden können. Mit Verweis auf einen längeren Schulungsbedarf für die mit dieser Aufgabe betrauten Dienstkräfte der Staatsanwaltschaft, auf eine erforderliche Freistellung vom Dienst sowie auf einen Arbeitsaufwand von mehreren Wochen lehnte die Senatsverwaltung diese Vorgehensweise ab.

Zusätzlich stellte sich die Frage, ob das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse der Betroffenen am Ausschluss der Übermittlung erheblich überwiegt. Die Forschenden wiesen u. a. darauf hin, dass es sich bei dem „Neuköllner Modell“ um einen wichtigen Baustein im jugendstrafrechtlichen Sanktionssystem Berlins handelt, das bisher keiner Evaluation unterzogen worden sei. Sie legten plausibel dar, dass die Evaluation bedeutende Hinweise dafür liefern könne, ob das Modell geeignet ist, wo Schwachstellen bestehen und wie die Qualität der Zusammenarbeit der verschiedenen Betei-

189 § 76 JGG
190 § 476 Abs. 1 Satz 1 Nr. 2 StPO

ligten verbessert werden kann. Im Hinblick auf die schutzwürdigen Interessen der Betroffenen war zu berücksichtigen, dass die Beschäftigten zwar Einsicht in die Akten erhielten, die verfahrensbezogenen Daten aber ausschließlich bezogen auf eine Nummer ohne identifizierende Daten speicherten. Die Zuordnung zwischen der Nummer und der jeweiligen Akte sollte in einer gesonderten Liste geführt werden, die auf unsere Anregung bei der Staatsanwaltschaft verbleiben sollte. Die Anzahl der auswertenden Beschäftigten der HWR war auf zwei Personen beschränkt, die auf das Datengeheimnis nach dem Berliner Datenschutzgesetz verpflichtet werden sollten. Auf dieser Grundlage ist es akzeptabel, dass die Daten nicht vorab anonymisiert wurden.

Soweit es bei der Datenverarbeitung zu Forschungszwecken nicht auf die Person des Betroffenen ankommt, ist eine vorherige Anonymisierung der Daten in der Regel erforderlich.

11.3 Pädophilie-Diskussion in einer Bürgerrechtsorganisation

Im Rahmen eines Forschungsprojekts, das sich mit pädophilen Forderungen im Bereich bestimmter politischer Bewegungen auseinandersetzt, bat die Georg-August-Universität Göttingen den Humanistischen Union e. V. um Einsicht in das Vereinsarchiv. Recherchiert werden sollten entsprechende Diskussionen in den Vereinsgremien auf der Grundlage von Sitzungsprotokollen, Korrespondenzen und Berichten. Der Verein bat uns um Beratung, um den Zugang datenschutzkonform zu gewähren.

Für das Forschungsvorhaben kam es darauf an, die Aussagen einzelner Personen und deren Bedeutung für die Diskussionen nachzuzeichnen. Eine Unkenntlichmachung der beteiligten Personen in den Unterlagen war daher ausgeschlossen. Die in den Unterlagen enthaltenen Informationen waren jedenfalls teilweise als besondere Arten personenbezogener Daten[191] einzustufen, da sie politische Meinungen oder philosophische Überzeugungen

191 § 3 Abs. 9 BDSG

enthalten konnten. Soweit solche Daten wie hier der Fremdforschung zur Verfügung gestellt werden sollen, ist fraglich, ob die Übermittlung der Daten auf gesetzlicher Grundlage zulässig ist. Dafür ist in jedem Fall erforderlich, dass das wissenschaftliche Interesse an der Durchführung des Vorhabens das Interesse der Betroffenen an dem Ausschluss der Datenweitergabe erheblich überwiegt.[192] Von der Universität, die Zugang zu den Akten erhalten wollte, wurden keine Angaben zur Abwägung der Interessen dargelegt. Auch war die von der Universität vorgelegte Zugriffs- und Nutzungsvereinbarung im Hinblick auf die Absicherung der Rechte der Betroffenen nicht aussagekräftig. Es fehlten präzise Angaben, wie das forschende Institut mit den erhobenen personenbezogenen Daten umgehen würde, welche konkreten datenschutzrechtlichen Vorschriften dabei zur Anwendung kommen und in welchen Fällen und auf welcher Grundlage Daten personenbezogen veröffentlicht werden sollten. Außerdem setzte die Datenschutzordnung des Vereins für die Übermittlung von Daten an Dritte in anderen als den in der Datenschutzordnung beschriebenen Fällen die Zustimmung der Betroffenen voraus. Dadurch wurde für die Mitglieder ein Vertrauenstatbestand geschaffen, der gegenüber den Forschungsinteressen beachtlich war. Eine Übermittlung auf gesetzlicher Grundlage kam danach nicht in Betracht.

Wir empfahlen der Humanistischen Union, die Einwilligung der Betroffenen für die Übermittlung der Daten einzuholen und darauf hinzuwirken, dass die Universität präzisiert, wie sie mit den Daten insbesondere im Hinblick auf eine Veröffentlichung weiter verfahren wird. Diese Präzisierung ist erforderlich, um auch die Betroffenen zu informieren, damit sie die Einwilligung wirksam erteilen können.

Forschungsinstitute dürfen personenbezogene Daten nur dann veröffentlichen, wenn die Betroffenen eingewilligt haben oder dies für die Darstellung zeitgeschichtlicher Ereignisse unerlässlich ist.[193] Letzteres muss durch das Forschungsinstitut nachvollziehbar dargelegt werden.

192 § 28 Abs. 6 BDSG
193 § 30 Abs. 5 BlnDSG, § 40 Abs. 3 Nr. 2 BDSG

11.4 Notenerhebung

Aus der Praxis

Für ein Forschungsprojekt zur Notengebung an deutschen Hochschulen wollte die Universität Flensburg Magister- und Diplomnoten von ehemaligen Studierenden an der FU Berlin sowie Noten der Ersten Staatsprüfungen in den Fächern Deutsch und Mathematik in dem Zeitraum bis zum Wintersemester 1995/1996 bei der Senatsverwaltung für Bildung, Jugend und Wissenschaft erheben. Die Daten sollten von den Forschenden vor Ort selbst erfasst und ausgewertet werden.

In beiden Fällen bedurfte es für die Übermittlung der Daten der Genehmigung durch die Senatsverwaltung, die uns beteiligte.[194] Im Ergebnis hielten wir die Übermittlung der Daten ohne Einwilligung der Betroffenen für zulässig, da das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwog.[195] Die Universität Flensburg hatte plausibel dargelegt, dass das Forschungsvorhaben dazu diente, die Kenntnisse bei der unterschiedlichen Verteilung der Noten zu vertiefen und die nicht leistungsbezogenen Einflüsse zu bestimmen, um mehr Transparenz zu schaffen. Die Auswertung der Daten sollte aggregiert erfolgen. Das Verfahren der Erhebung war so angelegt, dass die ohne Namensnennung erhobenen Daten nur während einer kurzen Zeitspanne ohne erhöhten Aufwand auf einzelne Personen zurückgeführt werden konnten. Zwar sind Informationen zu Examina, insbesondere die Note, als besonders schutzwürdig einzustufen. Die Prüfungen lagen allerdings mehr als 16 Jahre zurück, sodass die Gefahr einer missbräuchlichen Nutzung als eher gering zu bewerten war.

Wir empfahlen der Senatsverwaltung, zunächst zu prüfen, ob die Datenerhebung auch durch Beschäftigte der Senatsverwaltung durchgeführt werden könnte, sodass die Daten nur in pseudonymisierter Form an die Forschenden übermittelt werden würden. Für den Fall, dass dieses Vorgehen aufgrund des zu hohen Aufwandes nicht in Betracht kam, machten wir zur Absicherung der Rechte der Betroffenen eine Reihe von Maßnahmen zur Bedingung, die u. a. die Festlegung der zu erhebenden Daten, die spätere Pseudonymisierung der Daten, die Verpflichtungen der Forschenden zur Geheimhaltung sowie die Prüfung der Tätigkeit der Forschenden durch die Senatsverwaltung betrafen. Die Senatsverwaltung hat dies aufgegriffen.

194 § 30 Abs. 1 Satz 2 und 3 BlnDSG
195 § 30 Abs. 1 Satz 1 Nr. 2 BlnDSG

Wenn öffentliche Stellen ohne Einwilligung der Betroffenen Daten zu Forschungszwecken an Dritte übermitteln wollen, müssen sie prüfen, ob der Zweck der Forschung nicht auch dadurch erreicht werden kann, dass die Daten zuvor anonymisiert oder pseudonymisiert werden.

11.5 Mehr Studierende aus nicht-akademischen Familien

Aus der Praxis

Mehrere kooperierende Forschungsinstitute stellten uns ein Forschungsvorhaben vor, mit dem die Gründe dafür identifiziert und bewertet werden sollten, dass Studierende aus nicht-akademisch gebildeten Elternhäusern an deutschen Universitäten unterrepräsentiert sind. Das Vorhaben war als Längsschnittstudie[196] konzipiert und sollte mit einer Befragung der Zielpersonen zu Schulzeiten beginnen und dann über vier weitere Erhebungszeitpunkte hinweg durchgeführt werden. Der vorgelegte Fragebogen für die Erstbefragung der Schüler enthielt Fragen zum Bildungshintergrund der Eltern und Geschwister. Eine gesonderte Zustimmung dieser Personen war dafür nicht vorgesehen.

Die Erhebung von Daten anderer Personen (Drittdaten) kommt im Rahmen von Befragungen für Forschungsvorhaben häufig vor, insbesondere bei Schülerbefragungen. Für die Bewertung solcher Erhebungen muss zwischen verschiedenen Gestaltungen unterschieden werden:

Die Fragen können so weit formuliert sein, dass Dritte weder direkt bestimmt werden können noch der Inhalt der eingeholten Informationen eine solche Bestimmung indirekt zulässt. So können die Befragten aufgefordert werden, Angaben zu einer Bezugsperson oder einem Vorbild aus dem Verwandten- oder Bekanntenkreis zu machen. In der Regel wissen dann nur die Befragten selbst,

196 Untersuchung zu aufeinanderfolgenden Messzeitpunkten zur Erforschung von Wandlungsprozessen; siehe auch 11.1

über welche konkrete Person sie Auskunft erteilen, sodass eine Bestimmbarkeit dieser Person nicht ohne Weiteres gegeben ist.

In anderen Fällen wird zwar auf eine andere Person Bezug genommen, die erfragten Angaben lassen aber primär Aussagen über die befragte Person selbst zu und sind daher ihrer Sphäre zuzurechnen. So kann nach einer bestimmten Wahrnehmung gefragt werden, die sich auf die Tätigkeit einer anderen Person bezieht, ohne dass dabei Drittdaten erhoben werden.

Soweit die Dritten hingegen bestimmbar sind und bei der Befragung Einzelangaben zu diesen Personen eingeholt werden, müssen diese in der Regel um ihr Einverständnis gebeten werden. Etwas anderes kommt nur dann in Betracht, wenn eine Erhebung auf gesetzlicher Grundlage zulässig ist, etwa dann, wenn ein herausragendes Interesse an der Erhebung von Drittdaten besteht, eine Einwilligung nicht eingeholt werden kann, sonstige mildere Mittel nicht zur Verfügung stehen und keine Anhaltspunkte dafür gegeben sind, dass schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

So lag der Fall auch hier: Die Forschungsinstitute erläuterten, dass die Frage nach dem Bildungshintergrund der Eltern eine der Kernfragen der Studie sei und eine Befragung der Eltern selbst bzw. die Einholung einer Einverständniserklärung als mildere Mittel nur mit einem unverhältnismäßigen Aufwand erreicht werden könnten. Da der Rücklauf Von Einverständniserklärungen und Elternfragebögen nach den Erfahrungen aus anderen Studien sehr gering sei, würden genau die Schülerinnen und Schüler aus der Befragung herausfallen, die die eigentliche Zielgruppe darstellten. Schutzwürdige Interessen seien nur so gering wie möglich betroffen, da die Antwortkategorien sehr grob gewählt worden seien und die erhobenen Daten ausschließlich bezogen auf die Schülerinnen und Schüler zum Verständnis ihres Bildungshintergrundes ausgewertet werden würden. Aufgrund der Darlegungen der Forschungsinstitute kamen wir zu dem Ergebnis, dass ausnahmsweise keine Einwilligung für die Erhebung der Drittdaten erforderlich war.

Für die Erhebung von personenbezogenen Daten über Dritte bei Befragungen im Rahmen von Studien ist in der Regel die Zustimmung der betroffenen Dritten erforderlich.

11.6 WIMES

Im letzten Jahr hatten wir bereits über das webbasierte Verfahren WIMES („**Wi**rkungen **mes**sen“) berichtet, mit dem die Wirksamkeit von Hilfen im Jugendbereich evaluiert werden soll. Angesichts der gespeicherten sensitiven Jugendhilfedaten hatten wir das Verfahren als kritisch bewertet.[197] Die von der federführenden Senatsverwaltung für Bildung, Jugend und Wissenschaft zunächst geplante fachliche Erweiterung des Verfahrens, die wir als sehr problematisch angesehen hatten, wurde erfreulicherweise nicht weiterverfolgt. Umso erstaunter waren wir, als uns ein Bezirksamt darüber informierte, dass die Senatsverwaltung nun ein Praxisforschungsprojekt genehmigt hat, das die Analyse von konkreten Fallakten der Jugendämter beinhaltete.

Gegenstand des Projektes war, die Gründe für den Abbruch von stationären Hilfen durch die Untersuchung von im WIMES-Verfahren enthaltenen Daten unter Einbeziehung konkreter Fallakten zu untersuchen. Eine Mitarbeiterin des das WIMES-Verfahren betreibenden privaten Dienstleisters nahm in den Jugendämtern Einblick in ausgewählte Akten von Jugendlichen, die eine stationäre Hilfe abgebrochen hatten. Sie entnahm die für die Analyse notwendigen Informationen, um diese mit den im WIMES-Datenbestand enthaltenen Daten abzugleichen. Die Senatsverwaltung ließ die Mitarbeiterin zwar eine Verpflichtung zur Einhaltung des Datengeheimnisses unterschreiben, übersah dabei jedoch, dass die Einsichtnahme in die Fallakten bereits als Datenübermittlung zu bewerten war. Eine Rechtsgrundlage, die die Übermittlung der Sozialdaten zugelassen hätte, existierte nicht. Zwar ist die Nutzung von Sozialdaten zu Forschungszwecken ohne Einwilligung der Betroffenen unter bestimmten Voraussetzungen zulässig.[198] Diese waren hier jedoch nicht erfüllt. Angesichts der äußerst sensitiven Daten (z.B. Intelligenz, Behinderung, psychische Erkrankung, Delinquenz) wäre die Einholung einer Einwilligung der Betroffenen zwingend erforderlich gewesen. Hierauf wurde jedoch verzichtet.

Diesen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften haben wir gegenüber der Senatorin für Bildung, Jugend und Wissenschaft förmlich bean-

197 JB 2012, 8.1
198 § 75 SGB X

standet.[199] Sie hat daraufhin mitgeteilt, unsere Rechtsauffassung zu teilen, und uns um Beratung hinsichtlich der datenschutzrechtlichen Anforderungen bei der Genehmigung von Forschungsvorhaben gebeten.

Angesichts der früheren Gespräche zum WIMES-Verfahren, die eigentlich zu einer Sensibilisierung bei der Senatsverwaltung hätten führen müssen, ist es unverständlich, dass auf unsere weitere Einbeziehung verzichtet wurde. Wir gehen davon aus, dass mit der Senatsverwaltung ein Weg gefunden wird, der die Einhaltung des Datenschutzes bei der Genehmigung von Forschungsvorhaben künftig gewährleistet.

11.7 Forschungsprojekt Smart Senior – Intelligente Dienste und Dienstleistungen für Senioren

Aus der Praxis

Die Vertreter eines Konsortiums von Unternehmen und Forschungseinrichtungen mit medizinischem und technologischem Fokus stellten uns im Juli 2010 das Forschungsprojekt „Smart Senior“ vor, welches durch das Bundesministerium für Bildung und Forschung gefördert wurde. Ziel des Projektes war es, neue Technologien zu entwickeln, die ältere Menschen in ihrem Alltag zu Hause und in Notfallsituationen unterstützen und ihnen damit einen möglichst langen selbständigen Verbleib in den eigenen vier Wänden ermöglichen sollten. Dazu sollte ein Notfallerkennungs- und Assistenz-System für die sichere Fortbewegung entwickelt, bestehende medizinische und pflegerische Dienstleistungen integriert und eine altersgerechte Kommunikationsinfrastruktur aufgebaut werden. Geplant war, im Rahmen eines Feldtests Musterwohnungen mit den Technologien auszustatten und diese mit einer Reihe von Probanden in der Praxis zu testen.

Wir berieten das Konsortium bei der Erstellung des notwendigen Datenschutzkonzepts für die Durchführung des Projektes und insbesondere des Feldtests. Dazu nahmen wir über ein Jahr an den Sitzungen einer im Rahmen des Projekts gegründeten Datenschutz-Arbeitsgruppe teil und prüften zuletzt Teile von Vorversionen des Datenschutzkonzeptes. Die gemeinsame Arbeit verlief

199 § 26 Abs. 1 Satz 1 Nr. 1 BlnDSG

zunächst sehr konstruktiv. Im Verlauf des Projektes schienen jedoch Unstimmigkeiten zwischen den Projektpartnern zu entstehen, die auch zulasten der Koordination bei der Erstellung des Datenschutzkonzepts gingen. Im Juni 2011 machten wir unsere Ansprechpartner darauf aufmerksam, dass noch erheblicher Nachbesserungsbedarf bestand. So war zu diesem Zeitpunkt immer noch nicht abschließend geklärt, wer für welche Datenverarbeitungen verantwortlich und damit Adressat für die Geltendmachung von Rechten durch die Betroffenen/Probanden sein sollte. Zudem waren die Verfahren nicht so beschrieben, dass auf dieser Grundlage eine abschließende rechtliche Bewertung der Datenverarbeitungen und die Beschreibung der notwendigen Maßnahmen zur Umsetzung der rechtlichen Anforderungen möglich gewesen wären. Dementsprechend waren auch noch keine Entwürfe für Einwilligungs-, Teilnahme- und Schweigepflichtentbindungserklärungen für den Feldtest formuliert. Wir wiesen darauf hin, dass der Start eines Feldtests ohne eine abgeschlossene datenschutzrechtliche Prüfung (einschließlich einer Vorabkontrolle und Umsetzung der rechtlichen Anforderungen) sowie ohne fertiges Datenschutzkonzept datenschutzrechtlich unzulässig sei. Daraufhin informierte uns der Koordinator des Projekts, dass die Vervollständigung der datenschutzrechtlichen Materialien bis Januar 2012 zu erwarten sei und wir diese dann zur Prüfung erhalten würden.

Seitdem haben wir keine weitere Nachricht zum Stand des Projektes erhalten. Erst im November 2012 erfuhren wir von anderen Teilnehmern der Datenschutz-Arbeitsgruppe, dass das Projekt samt Feldtest bereits im Sommer 2012 abgeschlossen worden war. Trotz mehrfacher telefonischer und postalischer Aufforderung bis ins Jahr 2013 hinein, haben wir bis heute weder die Endversion des Datenschutzkonzepts, die Voten der Datenschutzbeauftragten der beteiligten Projektpartner noch den Abschlussbericht des Projektes für das Bundesministerium für Bildung und Forschung zur Kenntnis erhalten. Über das Vorgehen des Projektkoordinators und die Art der Zusammenarbeit sind wir sehr irritiert. Wir haben nicht unerhebliche Personalressourcen eingesetzt mit dem Ergebnis, dass der Erfolg dieser Arbeit für uns letztlich nicht feststellbar ist.

Gerade Forschungsprojekte in sensitiven Bereichen dürfen nicht ohne überprüfbares Datenschutzkonzept durchgeführt werden.

12 Schulen und Hochschulen

12.1 Schulen

12.1.1 Kommunikation zwischen Lehrkräften und Schülern über Facebook

Aus der Praxis

Zunehmend nutzen Menschen jeder Altersgruppe soziale Netzwerke als zusätzliche Kommunikationsplattform. Insbesondere Jugendliche kommunizieren auf diesem Weg, um sich zu präsentieren, mit Freunden zu verabreden oder Erlebnisse miteinander zu teilen.[200] Vor diesem Hintergrund wird vielfach diskutiert, ob Lehrkräfte unter einem privaten oder dienstlichen Profil in sozialen Netzwerken mit ihren Schülerinnen und Schülern kommunizieren dürfen.

Zunächst ist grundsätzlich anzumerken, dass beamtete Lehrkräfte einer außerdienstlichen Wohlverhaltenspflicht unterliegen[201]. Neben der Vermittlung von Wissen beinhaltet ihre Tätigkeit auch einen Erziehungsauftrag, in dessen Rahmen sie die geistige und sittliche Entwicklung der ihnen anvertrauten Kinder zu fördern und zu schützen haben.[202] Auch angestellte Lehrkräfte haben für ihre Schülerinnen und Schüler eine besondere Vorbildfunktion, die sich auch auf ihre private Lebensführung erstreckt. Von ihnen wird erwartet, dass sie sich innerhalb und außerhalb des Dienstes regelgerecht – und somit auch datenschutzgerecht – verhalten.

Kommunizieren Lehrkräfte in sozialen Netzwerken mit ihren Schülerinnen und Schülern, um z.B. Hausaufgaben zu verteilen, Ergebnisse von Arbeiten, Unterrichtsausfälle mitzuteilen oder den nächsten Wandertag zu „besprechen“, werden personenbezogene Daten übermittelt. Diese Übermittlung ist nur zulässig, wenn sie den Anforderungen von § 5 Berliner Datenschutzgesetz

200 In Deutschland „treffen“ sich 77 % der jugendlichen Internetnutzer regelmäßig, meist sogar mehrmals täglich, um sich in sozialen Netzwerken auszutauschen (siehe JIM-Studie 2013, S. 37).

201 § 34 Satz 3 Beamtenstatusgesetz

202 BVerwG, Urteil vom 19. August 2012 – 2 C 5/10

gerecht wird. Insbesondere ist die Vertraulichkeit der übermittelten Daten und die Transparenz des genutzten Verfahrens sicherzustellen. Viele der genutzten Netzwerke, insbesondere Facebook, werden dem nicht gerecht. Die Server dieser Netzwerke liegen zumeist in den USA. Der dortige Datenschutzstandard entspricht jedoch nicht dem in Deutschland bzw. der EU. Die USA sind kein „sicherer Hafen“ mehr.[203] Die Lehrkräfte können daher nicht sicherstellen, dass die personenbezogenen Verkehrs- und Inhaltsdaten der Kommunikation vertraulich bleiben. Die dienstliche Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern, die über diese sozialen Netzwerke erfolgt und personenbezogene Daten enthält, verstößt somit gegen das Berliner Datenschutzgesetz.

Die Lehrkraft ist, ganz gleich, in welchem Zusammenhang sie mit ihren Schülern in Kontakt tritt, immer auch eine Vertreterin der Schule. Die Schülerinnen und Schüler können sich daher nicht freiwillig für eine Freundschaft mit der Lehrkraft entscheiden, da für sie nicht auszuschließen ist, dass mit der Absage der Freundschaftsanfrage schulische Nachteile verbunden sind. Eine Facebook-Freundschaft zwischen der Lehrkraft und den Jugendlichen ermöglicht zudem den wechselseitigen Einblick in die jeweiligen Profile des anderen und die dort hinterlegten Daten und Fotos. Dadurch lässt sich die gebotene Trennung zwischen dienstlichen und privaten Angelegenheiten (Distanzgebot) der Lehrkraft nicht mehr gewährleisten.

Im Übrigen ist die Nutzung von Facebook zur schulischen Kommunikation mit dem Erziehungsauftrag der Lehrkräfte nicht vereinbar, da das Geschäftsmodell dieses Unternehmens darauf ausgerichtet ist, die Informationen aus dem Kommunikations- und Nutzungsverhalten der jugendlichen Mitglieder zu vermarkten. Dass dabei den eigenen ökonomischen Interessen des Unternehmens der Vorrang vor den Persönlichkeitsrechten der Jugendlichen eingeräumt wird, ist offensichtlich.

Angesichts der erheblichen datenschutzrechtlichen Bedenken, die bei einer Nutzung von sozialen Netzwerken wie Facebook durch Lehrkräfte bestehen, hat das Ministerium für Kultus, Jugend und Sport Baden-Württemberg im Juli

203 Siehe 2.2

den Einsatz von „Sozialen Netzwerken“ an Schulen grundsätzlich untersagt.[204] Vergleichbar restriktive Vorgaben haben die Bildungsministerien in Bayern,[205] Rheinland-Pfalz[206] und – bereits 2012 – in Schleswig-Holstein[207] gemacht. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat zwar öffentlich bekundet, dass die Berliner Schulen auf den Einsatz von Facebook verzichten sollen.[208] Verbindliche Vorgaben für einen „restriktiven Umgang“ mit sozialen Netzwerken wurden von der Senatsverwaltung jedoch nicht erlassen. Sie vertraut vielmehr darauf, dass die Lehrkräfte ohne Vorgaben „verantwortungsvoll“ mit sozialen Netzwerken umgehen. Die vielen Anfragen, die uns erreichen, zeigen jedoch, dass in den Schulen – bei den Schulleitungen und den Lehrkräften – eine erhebliche Verunsicherung über den rechtmäßigen Einsatz dieser „neuen Kommunikationsmedien“ besteht.

Keine Einwände bestehen allerdings dagegen, wenn Lehrer Fragen des Datenschutzes bei Facebook zum Unterrichtsgegenstand machen.

Eine Vernetzung zwischen Lehrkräften und ihren Schülerinnen und Schülern auf Facebook begegnet erheblichen datenschutzrechtlichen Bedenken. Verbindliche Vorgaben zum restriktiven Umgang mit sozialen Netzwerken an den Berliner Schulen sind daher dringend erforderlich.

12.1.2 Elektronisches Klassenbuch und SMS gegen Schulschwänzen

Anlässlich der Beantwortung einer mündliche Anfrage, welche Maßnahmen der Senat zur Durchsetzung der gesetzlichen Schulpflicht und zur Reduzierung der Zahl der schwänzenden und schulverweigernden Jugendlichen unternehmen würde, erklärte die Senatorin für Bildung, Jugend und Wissenschaft im März 2012 im Abgeordnetenhaus, dass an zehn Schulen ein Pilotprojekt geplant sei, um die Einführung eines elektronischen Klassenbuchs zu erproben. Teil des Projektes sei es, die Eltern direkt aus dem Klassenzimmer per SMS darüber zu informieren, wenn ihre Kinder in der Schule fehlen.

In drei sog. Startschulen wurde die Vorbereitung des Testbetriebes für ein elektronisches Klassenbuch aufgenommen. Neben Namen und Vornamen sollen im elektronischen Klassenbuch zu den Schülerinnen und Schülern das Geburtsdatum, Geschlecht, die Abwesenheitszeiten, Befreiungen und Beurlaubungen und über die Erziehungsberechtigten z.B. Kommunikationsdaten gespeichert werden. Die Daten der Betroffenen sollen in der Erprobungsphase auf einem Server des Anbieters in Österreich verarbeitet werden.

Wir haben die Senatsverwaltung darauf hingewiesen, dass der Umfang der Datenverarbeitung im geplanten elektronischen Klassenbuch über den Datenkatalog hinausgeht, der in § 5 Abs. 1 SchulDatenVO abschließend für das traditionelle Klassenbuch definiert ist. Eine Rechtsgrundlage, auf die die Datenverarbeitung im elektronischen Klassenbuch gestützt werden kann, ist nicht gegeben. Die Verarbeitung von Daten, die im herkömmlichen Klassenbuch nicht enthalten sind, ist daher nur mit schriftlicher Einwilligung der Betroffenen (Schüler, Eltern, Lehrkräfte, Ausbilder) zulässig. Mit dem österreichischen Anbieter ist – unter Berücksichtigung der erforderlichen Datensicherheitsaspekte – ein Vertrag zur Auftragsdatenverarbeitung zu schließen. Da bei der Versendung der SMS an die Erziehungsberechtigten nicht festgestellt werden kann, wer das Handy gerade (physisch) in Besitz hat, ist der Text der Nachricht möglichst neutral zu halten. Von der Senatsverwaltung für Bildung, Jugend und Wissenschaft wurde erklärt, dass unsere Hinweise umgesetzt werden. Der Text für die SMS-Nachricht wurde im Einzelnen mit uns abgestimmt.

Bevor das elektronische Klassenbuch im Flächenbetrieb an den Schulen zum Einsatz kommt, sind die dafür erforderlichen gesetzlichen Datenverarbeitungsbefugnisse zu schaffen. Die Verarbeitung der Daten sollte nach Abschluss der Pilotphase auf einem lokalen Server in Berlin erfolgen.

204 Die entsprechende Handreichung ist abrufbar unter http://www.lmz-bw.de/news/news-details/article/der-einsatz-von-sozialen-netzwerkenan-schulen/409.html.
205 Verwaltungsvorschrift des Bayerischen Staatsministeriums für Unterricht und Kultus: Hinweise zum Umgang mit Sozialen Medien/Netzwerken vom 18. April 2013
206 Merkblatt “Lehrkräfte und Soziale Netzwerke (z.B. Facebook)“ des Ministeriums für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz vom 21. Oktober 2013
207 Rundschreiben des Ministeriums für Bildung und Wissenschaft des Landes Schleswig-Holstein vom 30. August 2012
208 Tagesspiegel vom 20. September 2013: „Berliner Senat gegen Facebook in Schulen und Verwaltung“

12.1.3 Verwaltung von Schülerdaten in den USA

Eine staatlich anerkannte Ersatzschule in freier Trägerschaft wollte sämtliche Schülerdaten (wie Namen, Adressen, Zensuren, Anwesenheiten, disziplinarische Maßnahmen) von dem Anbieter einer US-amerikanischen Website verwalten lassen.

Den uns von der Schule vorgelegten Unterlagen war zu entnehmen, dass die Datenverarbeitung in den USA und somit in einem Land ohne angemessenem Datenschutzniveau erfolgen sollte. Die Erklärung des Unternehmens, die Datenverarbeitung konform dem EU-Datenschutzrecht (entsprechend dem Safe Harbor-Abkommen) durchzuführen, änderte an dieser Einschätzung nichts.[209] Die angeführte TRUSTe-Zertifizierung[210] basierte im Wesentlichen auf einer Selbstbeschreibung oder -zertifizierung des Unternehmens. Der Nachweis einer aussagekräftigen Zertifizierung des Anbieters durch einen vertrauenswürdigen Dritten, die ein angemessenes Schutzniveau und die Einhaltung der EU-Datenschutzbestimmungen bei dem Anbieter garantieren, wurde nicht vorgelegt. Da die Datenverarbeitung in einem Land ohne angemessenem Datenschutzniveau außerhalb des Europäischen Wirtschaftsraumes erfolgen sollte, kam eine Auftragsdatenverarbeitung nach § 11 BDSG nicht in Betracht. Datenschutzrechtlich war vielmehr von einer Übermittlung der personenbezogenen Daten von Schülerinnen, Schülern und Lehrkräften in die USA auszugehen.

Eine Übermittlung von personenbezogenen Daten durch die Schule an einen privaten Dritten (den Betreiber eines Servers in den USA) ist grundsätzlich nur mit schriftlicher Einwilligung der Betroffenen zulässig.[211] Diese hat freiwillig zu erfolgen. Hier sollte die Einwilligung von den Betroffenen bei Schuleintritt durch Unterzeichnung des Schulvertrages eingeholt werden. Ein Besuch der Schule, ohne in die Datenübermittlung einzuwilligen, wurde nicht akzeptiert. Die Freiwilligkeit der Einwilligung in die Datenverarbeitung war somit nicht gegeben.

209 Siehe 2.2
210 TRUSTe ist ein US-Unternehmen, das Anbietern von Dienstleistungen aufgrund ihrer Selbstverpflichtung die Verwendung eines Gütesiegels gestattet.
211 § 64 Abs. 5 SchulG

Unabhängig davon haben die Schulen die vorgegebenen technisch-organisatorischen Maßnahmen umzusetzen.[212] Dies gilt auch für Ersatzschulen in freier Trägerschaft.[213] Das Produkt „Engrade“ des US-Anbieters entspricht diesen Vorgaben nicht. Als Authentifizierung der berechtigten Lehrkraft bietet die Software nur die Kombination aus Nutzername und Passwort an. Diese Art von Zugriffsschutz ist im Umfeld „Schule“ nicht ausreichend. Insbesondere bei einer dezentralen Nutzung (z.B. über Rechner in den Unterrichtsräumen) haben unbefugte Dritte (z.B. Schülerinnen und Schüler) leicht die Möglichkeit, Zugriff zum System zu erlangen. Durch den Einsatz von sog. Hardware-Keyloggern, die zwischen das Tastaturkabel gesteckt werden und jede Tastatureingabe aufzeichnen, können Passwörter leicht ermittelt und die Rechner unbefugt gestartet werden. Die Software „Engrade“ bietet damit keine sicheren Authentifizierungsmöglichkeiten. Einen Verzicht auf diese Maßnahmen – gestützt auf eine Einwilligung der oder des Betroffenen – hat der Gesetzgeber nicht vorgesehen. Die Maßnahmen sind vielmehr zwingend vorgeschrieben.[214] Sonst könnte die datenverarbeitende Stelle sich von den Betroffenen eine umfassende Einwilligung in den Verzicht der darin vorgesehenen Sicherheitsanforderungen erteilen lassen. Damit wäre eine Umgehung der gesetzlich festgelegten Datensicherheitsschranken (z.B. aus wirtschaftlichen Erwägungen) unproblematisch möglich. Das würde dem Zweck der datenschutzrechtlichen Vorschriften zuwiderlaufen.

Wir haben der Schule mitgeteilt, dass die vorgesehene Übermittlung von personenbezogenen Schülerdaten und Daten der Lehrkräfte auf den Server eines Betreibers in den USA unter Einsatz des Produktes „Engrade“ datenschutzrechtlich unzulässig ist.

12.1.4 Sprachlerntagebuch

Das in den Kindertageseinrichtungen verwendete Sprachlerntagebuch, mit dem die Sprachentwicklung der Kinder gefördert und Sprachdefizite mög-

212 § 5 Abs. 1 und 2 BlnDSG
213 § 6 Abs. 4 Satz 1 i.V. m. § 95 Abs. 4 Satz 1, 2. HS, § 65 Abs. 5 SchulG
214 Siehe auch 6.2 und 14.2

lichst frühzeitig erkannt werden sollen, war immer wieder Gegenstand von Presseberichten. Insbesondere wurde mitgeteilt, dass zwischen der Bildungssenatorin und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ein Dissens darüber bestehe, ob das Sprachlerntagebuch bzw. Teile daraus von den Kita-Einrichtungen an die künftigen Grundschulen der Kita-Kinder weitergegeben werden dürfen.

Wir haben bereits früher dargestellt, dass das Sprachlerntagebuch aus unterschiedlichen Abschnitten besteht, die zum Teil sehr vertrauliche Informationen über die Kinder und ihre Familien enthalten.[215] Wir haben darauf hingewiesen, dass es der Entscheidung der Eltern obliegt, der Verwendung des Sprachlerntagebuchs zuzustimmen und darin enthaltene Fragen ggf. nicht zu beantworten. Ihnen ist es auch freigestellt, den künftigen Lehrkräften ihres Kindes eine Einsicht in das Sprachlerntagebuch zu ermöglichen. Anliegen der Senatsverwaltung ist es, ausschließlich die Lerndokumentation, die als Teil des Sprachlerntagebuchs Angaben über für die Sprachentwicklung bedeutsame Kompetenzen enthält, im verbindlicheren Verfahren an die Grundschulen weiterzugeben, damit sich diese auf die Sprachkompetenz der neuen Schulkinder einstellen können.

Die Bildungssenatorin und der Berliner Beauftragte für Datenschutz und Informationsfreiheit haben in einem Gespräch die datenschutzrechtlichen Möglichkeiten und Grenzen erörtert. Dabei wurde eine Einigung darüber erzielt, dass ein Spielraum für die Weitergabe der Lerndokumentation an die Schulen besteht. Allerdings bedarf es einer aktiven Mitwirkung der Eltern, da ohne diese eine Übermittlungsbefugnis nicht besteht. Notwendig ist insoweit eine frühzeitige Information der Eltern. In anschließenden Gesprächen auf Arbeitsebene wurde die konkrete Ausgestaltung näher erörtert.

Die Weitergabe der Lerndokumentation durch die Kita-Einrichtungen an die Grundschulen setzt voraus, dass die Eltern damit einverstanden sind. Wir gehen davon aus, dass wir gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Wissenschaft ein datenschutzgerechtes Verfahren erreichen werden, das sowohl dem Interesse an einer Weiterentwicklung der Sprachkompetenz der Kinder beim Übergang in die Grundschule als auch den Datenschutzinteressen der Kinder und ihrer Familien Rechnung trägt.

215 JB 2006, 6.3.1; JB 2007, 7.1

12.1.5 Lehrervertreter im Internet

Die Leitung einer Grundschule informierte uns darüber, dass ein (Eltern-)Vertreter der Schulkonferenz einen Brief im Internet gepostet habe, in dem er Gesprächsinhalte zu Personalfragen mit der Schulaufsicht wiedergegeben und das Abstimmungsergebnis der Gesamtkonferenz zur Wahl der Lehrervertreter für die Schulgremien unter namentlicher Nennung einzelner Lehrkräfte kommentiert hat.

Der datenschutzrechtliche Status der schulischen Gremien ist im Schulgesetz nicht eindeutig geregelt. Dies betrifft insbesondere die Gremien (z.B. Schulkonferenz), zu denen Elternvertreter gehören. Es ist jedoch davon auszugehen, dass diese Gremien keine eigenen datenverarbeitenden Stellen (wie z.B. Personalvertretungen) sind. Sie gehören vielmehr zur Schulorganisation; für sie verantwortliche Stelle im Sinne des Berliner Datenschutzgesetzes ist damit die Schule. In den Bereichen, in denen das Datenschutzrecht berührt ist, besteht daher zwischen der Schulleitung und den schulischen Gremien (sowie deren Mitgliedern) ein Über- und Unterordnungsverhältnis mit einer rechtlichen Direktionsbefugnis der Schulleitung.

Die Zulässigkeit der Verarbeitung von personenbezogenen Daten durch schulische Gremien und durch deren Mitglieder richtet sich nach dem Schulgesetz.[216] Danach ist eine Verarbeitung von personenbezogenen Daten (z.B. der Lehrkräfte) nur rechtmäßig, wenn dies zur Erfüllung der den Gremien durch Rechtsvorschriften zugewiesenen schulbezogenen Aufgaben erforderlich ist.[217]

Durch die Veröffentlichung eines Briefes mit personenbezogenen Daten im Internet werden die Daten der Betroffenen (z.B. Lehrkräfte) von dem Absender an eine unbestimmte Anzahl von Empfängern (Dritten) übermittelt. Die Übermittlung von personenbezogenen Daten über Lehrkräfte an einen derartig unbestimmten Kreis von Adressaten ist für die Erfüllung der schulbezogenen Aufgaben eines Mitgliedes der Schulkonferenz in keinem Fall erforderlich und damit datenschutzrechtlich unzulässig. Dies gilt insbesondere dann, wenn es sich um vertrauliche Daten aus Personalgesprächen oder um namentliche

216 § 64 Abs. 1 SchulG
217 § 64 Abs. 1 SchulG

Abstimmungsergebnisse in schulischen Gremien handelt. Dem entspricht im Übrigen auch die Bestimmung des Schulgesetzes,[218] die die Mitglieder der im Schulgesetz genannten Gremien (z.B. der Schulkonferenz) in Angelegenheiten der Gremienarbeit zur Verschwiegenheit verpflichtet.

Wegen der unzulässigen Veröffentlichung von personenbezogenen Daten der Lehrkräfte im Internet durch ein Mitglied der Schulkonferenz haben wir gegenüber der Schule einen datenschutzrechtlichen Mangel festgestellt. Die Schulleitung hat die Angelegenheit im Beisein des Schuldatenschutzbeauftragten mit den Beteiligten erörtert. Alle Gremienmitglieder wurden umfassend über ihre Verschwiegenheitspflicht belehrt.

Vertrauliche Informationen aus Personalgesprächen und namentliche Abstimmungsergebnisse aus Schulgremien gehören nicht ins Internet.

12.1.6 Datenverarbeitung in den Musikschulen

Aus Anlass der Einführung eines neuen zentralisierten IT-Systems zur Verwaltung von Schülerinnen und Schülern sowie der Lehrkräfte an den bezirklichen Musikschulen haben wir die Datenverarbeitung sowohl rechtlich als auch technisch geprüft.

In rechtlicher Hinsicht war insbesondere die Änderung der Abrechnungsmodalitäten von einer pauschalen monatlichen Abrechnung der Ausbildungskosten hin zu einer stundenbasierten Abrechnung zu prüfen. Im Rahmen dieser Einzelstunden-Abrechnung sollten detaillierte personenbezogene Daten darüber, ob der Unterricht stattgefunden hat oder aus welchen Gründen dies nicht der Fall war, erfasst werden.

Das Schulgesetz enthält keine Erlaubnisnorm für die Verarbeitung von Schülerdaten in den Musikschulen. Die Ausführungsvorschriften über Honorare der Musikschulen kommen ebenfalls nicht als Rechtsgrundlage für die

218 § 120 Abs. 3 SchulG

Datenverarbeitung in Betracht, da es sich nur um Verwaltungsvorschriften und keine gesetzliche Regelung handelt. Die Verarbeitung der Schülerdaten in den Musikschulen ist daher nur mit Einwilligung der Betroffenen (bzw. der Erziehungsberechtigten) zulässig.

Eine wirksame Einwilligung setzt voraus, dass die oder der Betroffene bereits im Vorfeld der Erklärung umfassend über Art, Umfang und Dauer der Datenverarbeitung bzw. -speicherung informiert wird („informierte“ Einwilligung). Bisher wird die (schriftliche) Einwilligungserklärung der Betroffenen in die Datenverarbeitung bei der Unterzeichnung des Unterrichtsvertrages eingeholt. Die Erklärung bezieht sich dabei auf die Verarbeitung der Vertragsdaten „für die Vertragsabwicklung, die Überwachung des Zahlungseingangs und statistische Zwecke.“ Die erweiterte Datenverarbeitung von Schülerdaten zur Einzelstunden-Abrechnung ist von dieser Einwilligungserklärung nicht umfasst.

Wir haben empfohlen, den Text der Erklärung anzupassen, um die Betroffenen umfassend über Art, Umfang und Dauer (z.B. Angaben zum Unterrichtsausfall) der Verarbeitung ihrer Daten zu informieren und bei der Dauer der Datenverarbeitung die Grundsätze der Erforderlichkeit und der Datensparsamkeit zu berücksichtigen. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft will dieser Empfehlung folgen.

Das neue IT-Verfahren der Musikschulen (MS-IT) ist ein web- bzw. browserbasiertes Verfahren, das zentral auf Servern im ITDZ läuft.[219] Da es sich jedoch um Angebote der Bezirke handelt, verwalten diese ihre Daten auf dem Server weiterhin „logisch“ getrennt. Dies wird auch als Mandantentrennung bezeichnet.

Die Musikschulen streben jedoch zur Verwaltungsvereinfachung an, eine gemeinsame Datenbank mit den Stammdaten der Lehrkräfte sowie der Schülerinnen und Schüler zu nutzen. Letztere müssen dadurch die Änderung ihrer Adresse oder Telefonnummer nur einmalig melden, auch wenn sie Kurse an mehreren Schulen zugleich besuchen. Dies führt jedoch dazu, dass alle Angestellten der Musikschulen aus ganz Berlin auf die Daten aller Schülerinnen

219 Die Datenübertragung erfolgt hierbei angemessen verschlüsselt über die zusätzlich gesicherten Leitungen des Berliner Landesnetzes.

und Schüler zugreifen könnten. Wir konnten erreichen, dass die folgenden technisch-organisatorischen Maßnahmen ergriffen werden, um dieses Risiko zu reduzieren:

- Alle Beschäftigten werden zum sorgsamen Umgang mit personenbezogenen Daten schriftlich verpflichtet.
- Eine vollständige Auflistung aller Datensätze wird verhindert, indem eine Suche mindestens die Vorgabe von drei Datenfeldern (wie z.B. Name, Vorname und Postleitzahl) erfordert.
- In der Ergebnisliste ist nur Name, Vorname und Adresse sichtbar, um die sichere Auswahl des richtigen Eintrags zu ermöglichen.
- Die Einsichtnahme und Änderung von Daten ist erst dann möglich, wenn die betreffende Person mit der jeweiligen Musikschule verknüpft wird (z.B. Aufnahme als Musikschüler oder Interessent). Diese Verknüpfung wird revisionssicher protokolliert. Zudem wird organisatorisch sichergestellt, dass eine regelmäßige stichprobenhafte Überprüfung der Protokolle u. a. durch den behördlichen Datenschutzbeauftragten erfolgt.
- Besonders schutzwürdige Einträge wie Kontodaten werden nur gekürzt angezeigt.

Eine Überprüfung der Datenverarbeitung der Musikschulen führte dazu, dass die Transparenz für die Betroffenen verbessert wurde und dass das neue IT-System sowohl den Anforderungen des Datenschutzes entspricht als auch die angestrebten Arbeitserleichterungen erzielt.

12.2 Hochschulen

12.2.1 Die Datenschutzsatzung der Freien Universität

Der Akademische Senat der Freien Universität (FU) hat im Juli eine Datenschutzsatzung erlassen, die den hochschulinternen Datenschutz regelt und die Datenschutzrichtlinie ersetzt. Wir haben an der inhaltlichen Gestaltung der Satzung über mehrere Jahre intensiv mitgewirkt.

Schon 2010 hatten wir darauf hingewiesen, dass zur Regelung datenschutzrechtlicher Aspekte an der FU eine Satzung erforderlich ist.[220] Die Regelung des Datenschutzes durch eine nur die interne Selbstbindung der Verwaltung bewirkende Datenschutzrichtlinie ist unzulässig. Nunmehr hat der Akademische Senat von seiner Satzungsbefugnis, die sich aus dem Berliner Hochschulgesetz ergibt, Gebrauch gemacht.[221] Dabei hat er die inhaltlichen Grenzen der Satzungsbefugnis eingehalten und unsere inhaltlichen Empfehlungen aufgegriffen.[222]

Die Satzung legt fest, unter welchen Voraussetzungen personenbezogene Daten von Mitgliedern der FU und Dritten verarbeitet werden dürfen. Es werden die betroffenen Datenarten aufgeführt, darüber hinaus einzelne Verarbeitungszwecke (wie die Datenverarbeitung zur Evaluation von Forschung und Studium sowie zur Benutzung von Einrichtungen der FU) mitsamt den dafür erforderlichen Daten konkret benannt. Die Satzung legt auch fest, wann personenbezogene Daten zu löschen sind. Dass die im Berliner Hochschulgesetz zum Erlass einer Satzung gesetzte Frist um mehrere Jahre überschritten worden ist,[223] ist für deren Wirksamkeit unschädlich. Der Gesetzgeber hat den Erlass von Satzungen zur Verarbeitung personenbezogener Daten nicht in das Ermessen der Hochschulen gestellt.[224] Die Frist ist daher nicht im Sinne einer auflösenden Bedingung zu verstehen, bei deren Eintritt die Satzungsbefugnis erlischt. Die Regelungskompetenz mittels Satzung besteht demzufolge auch nach Ablauf der Frist.

Die Datenschutzsatzung regelt den hochschulinternen Datenschutz an der FU mit unmittelbarer Außenwirkung und genügt sowohl den Anforderungen des Berliner Datenschutzgesetzes als auch des Berliner Hochschulgesetzes.

220 JB 2010, 9.1.1
221 § 61 Abs. 1 Nr. 4 BerlHG
222 § 6 b Abs. 2 Satz 1 BerlHG i.V. m. § 6 Abs. 1 Satz 1 Nr. 2 bis 8 BerlHG
223 § 6 b Abs. 3 BerlHG
224 § 6 b Abs. 2 Satz 1 BerlHG

12.2.2 Ein nervendes Wissenschaftsnetz

Neben vielen anderen sozialen Netzwerken versucht auch das speziell an Wissenschaftlerinnen und Wissenschaftler gerichtete Netzwerk Researchgate die Daten vorhandener Mitglieder zu nutzen, um deren Bekannte als neue Mitglieder zu gewinnen. Dies geschieht über Funktionen der Plattformen, die mehr oder weniger automatisch im Namen des Mitglieds an Freunde oder Kollegen eine E-Mail-Einladung verschicken. Andere soziale Netzwerke greifen dazu – mit Erlaubnis des Mitglieds – auf seine Adressbücher wie bei E-Mail-Diensten oder auf dem Smartphone zu.

Researchgate verwendet als weitere Quelle die wissenschaftlichen Publikationen, um Kolleginnen und Kollegen des Mitglieds zu ermitteln. Die Plattform bietet jedem Mitglied an, Referenzen auf seine Publikationen zu veröffentlichen. Zugleich wird vorgeschlagen, die Mitautoren zu „der Publikation" einzuladen. Zwar ist bei genauem Lesen des „Kleingedruckten" (das zum Teil erst per Klick abgerufen werden kann) erkennbar, dass hierbei Einladungs-E-Mails für das Wissenschaftsnetz verschickt werden, die Transparenz ist aber verbesserungsbedürftig, z.B. indem jeder einzelne Eingeladene vom Initiator der Einladung bestätigt werden muss. Dies haben wir dem Plattformbetreiber nahegelegt.

Möglicherweise führte die derzeitige Vorgehensweise dazu, dass wir eine Reihe von Beschwerden über die Plattform wegen des mitunter mehrfachen Versandes von unerwünschten Werbe-E-Mails erhalten haben. Oft sagten die Petenten aus, dass die angeblichen Urheber der Einladungen sich nicht bewusst seien, einen entsprechenden Auftrag erteilt zu haben.

Datenschutzrechtlich existiert jedoch keine Handhabe für weitere Maßnahmen. Die verwendeten Daten der Mitautoren stammen aus den allgemein zugänglichen Publikationen sowie den darin angegebenen oder anderswo veröffentlichten E-Mail-Adressen der Wissenschaftlerinnen und Wissenschaftler. Eine unzulässige Nutzung von E-Mail-Adressen zu Werbezwecken kann zudem bestenfalls indirekt mit einem Bußgeld geahndet werden. Zudem wird die Einladungsfunktion datenschutzrechtlich als eine im Auftrag des Mitglieds versandte private E-Mail angesehen, zumindest solange gewisse Mindestanforderungen wie die Möglichkeit der Einsichtnahme in die verschickten E-Mails sowie die Auflistung und Auswahlmöglichkeit der Empfänger erfüllt sind. Allerdings hat

der Bundesgerichtshof kürzlich entschieden, dass der Betreiber entsprechender Plattformen die zivilrechtliche Verantwortung für die Versendung entsprechender Empfehlungsmails trägt.[225]

Funktionen zur Einladung neuer Mitglieder per E-Mail durch Mitglieder sind nicht zu beanstanden, wenn bestimmte Mindestanforderungen eingehalten werden. Bei elektronischer Übermittlung sollte allerdings die vorherige Einwilligung des Empfängers eingeholt werden.

225 BGH, Urteil vom 12. September 2013 – I ZR 208/12

13 Wirtschaft

13.1 Banken

13.1.1 Falsche Auskunft und Verstoß gegen § 6a BDSG

Aus der Praxis

Ein Bürger stellte online einen Kreditkartenantrag bei der Landesbank Berlin. Dieser wurde abgelehnt, da seine statistisch berechnete Kreditwürdigkeit (Kreditscore) nicht ausreichend war für die gewünschte Kreditkarte mit Teilzahlungsmöglichkeit. Die Bank teilte dem Kunden mit, dass die Ablehnung nach Auswertung seiner wirtschaftlichen Daten erfolge. Weiter hieß es: „Einzelne Entscheidungsgründe können wir Ihnen nicht offenlegen, so sehr wir Ihren Wunsch danach auch verstehen würden." Nach Erhalt dieses Schreibens verlangte der Betroffene Auskunft, was die Bank mit der Mitteilung beantwortete, über ihn seien keine Daten gespeichert.

Über Anträge auf Ausstellung einer Kreditkarte wird – wie bei Darlehensanträgen – regelmäßig nach einer automatisierten Bonitätsprüfung entschieden. Eine solche automatisierte Einzelentscheidung, die einen Antrag ablehnt, ist nur dann rechtmäßig, wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen – etwa eine Remonstrationsmöglichkeit – gewährleistet ist; dem Betroffenen sind auf Verlangen die wesentlichen Gründe der Entscheidung mitzuteilen und zu erläutern.[226] In dem Ablehnungsschreiben verweigerte die Bank dem Antragsteller die Möglichkeit, seinen Standpunkt geltend zu machen. Außerdem lehnte sie es ab, die wesentlichen Gründe der Entscheidung mitzuteilen und zu erläutern. Bei dem Schreiben an den Petenten handelte es sich um das Standardablehnungsschreiben für alle Kreditkartenanträge, welches die Bank schon mehrere Jahre verwendete. Aufgrund unseres Eingreifens hat die Bank das Schreiben umgehend „aus dem Verkehr gezogen".

Die Bank hatte obendrein dem Petenten die falsche Auskunft erteilt, über ihn seien keine personenbezogenen Daten gespeichert, weil sie bei Auskunftsansprüchen nur überprüfte, ob personenbezogene Daten im Kundensystem

226 § 6a Abs. 2 Nr. 2 BDSG

gespeichert sind. Dies war nicht der Fall, da die Bank den Betroffenen als Kunden abgelehnt hatte. Daneben betreibt die Bank aber eine Datei, in der Informationen über alle Antragsteller und damit auch den Petenten enthalten sind. Wir haben gegenüber der Bank durchgesetzt, dass bei Auskunftsbegehren künftig alle relevanten Dateien überprüft werden.

Nur bei der Gewährung von ausreichender Transparenz ist die Durchführung eines Kreditscorings rechtmäßig.

13.1.2 Kontaktlose Bezahlsysteme

Aus der Praxis

Zwei große Banken unter unserer Aufsicht geben Kreditkarten aus, mit denen in Geschäften bezahlt werden kann, ohne sie aus der Hand zu geben oder eine PIN eingeben zu müssen. Ein konkurrierendes Bezahlsystem, das Smartphones nutzt, wurde von einem Berliner Technologieunternehmen entwickelt und befindet sich bei Berliner Einzelhändlern im Einsatz. Wir analysierten Datenschutz und Datensicherheit beider Systeme.

Jeder Bezahlvorgang an einer Kasse kostet Zeit und Geld, gleich ob er mit Bargeld, mit EC- oder Kreditkarte ausgeführt wird. Dies ist Motivation genug, nach kostengünstigen Bezahlsystemen zu suchen, die den Vorgang beschleunigen. Ein zusätzlicher Anreiz entsteht für Händler oder Betreiber des Bezahlsystems, wenn ihnen die Kunden im Zusammenhang mit der Nutzung erlauben, Angaben über die Einkäufe personenbezogen zu speichern.

Kreditkarten, mit denen die Kunden nur gegen das Kassenterminal tippen müssen, um zu bezahlen, zielen primär auf einen beschleunigten Bezahlvorgang. Die ausgebenden Banken versichern, dass die Sicherheit gewahrt bleibt. Doch der Schutz weist Lücken auf, die erst mit der kontaktlosen Schnittstelle entstehen: Fremde, die sich der Brieftasche mit der Kreditkarte bis auf wenige Zentimeter nähern, können unter günstigen Umständen die Kreditkartennummer und das Ablaufdatum unbemerkt auslesen. Wer sich geschickt in der Nähe eines Kassenterminals platziert, schafft dies auch aus deutlich größerer Entfernung. Und schließlich wandert mit den kontaktlosen Kreditkarten ein weiteres elek-

tronisches Gerät in die Taschen der Bürgerinnen und Bürger, an deren Besitz sie aus der Ferne wiedererkannt werden können.

Wer sich gegen die erste und die letztgenannte Bedrohung wehren will, kann seine Karte in eine metallene Hülle stecken. Wer explizit nachfragt, erhält sie kostenpflichtig von der kartenausgebenden Bank. Doch wer fragt nach, wenn das Risiko unbekannt bleibt?

Die Banken preisen die Vorzüge des Verfahrens an, verschweigen aber die Risiken. Gegen die zweite o. g. Bedrohung (Auslesen der Karte in der Nähe von Kassenterminals) nützt nur eine Verschlüsselung der übertragenen Daten. Sie ist den Banken jedoch zu teuer. Davon erfahren die Kunden nichts. Ein Vertriebspartner behauptete gar auf seiner Webseite wahrheitswidrig, eine Verschlüsselung finde statt.

Solange die Banken untätig bleiben, hilft den Kunden nur die Abwahl der Kontaktlosfunktion. Da vielfach eine Abwahlmöglichkeit nicht angeboten wird, hieße dies derzeit, auf die jeweilige Kreditkarte ganz zu verzichten und ggf. den Anbieter zu wechseln.

In Abstimmung mit den anderen Datenschutzaufsichtsbehörden fordern wir, für die Kunden Transparenz und Wahlmöglichkeiten herzustellen, kostenlos und unaufgefordert Schutzhüllen oder eine Deaktivierung der Kontaktlosfunktion anzubieten und, sobald dies mit verhältnismäßigem Aufwand möglich ist, eine Verschlüsselung der Datenübertragung von der Karte zum Lesegerät vorzusehen.

Ein weiterer Trend sind mobile Zahlungslösungen, die von einem einzelnen Konzern bzw. für eine Kette von Einzelhändlern angeboten werden. In der Praxis wird dazu eine Smartphone-App bereitgestellt, die neben anderen Kundenbindungs- und Servicefunktionen auch eine bargeldlose Bezahlung in den Geschäften der Kette ermöglicht. Nach dem Download der App ist dazu eine Anmeldung zumindest bei dem Zahlungsdienstleister erforderlich. An der Kasse des Einzelhändlers wird zur Bezahlung eine nur kurzzeitig gültige Kennnummer eingegeben bzw. ein Barcode eingescannt, die von der App abgerufen und angezeigt werden.

Die Prüfung bei dem Technologieunternehmen ergab, dass das Verfahren durch die verwendete 2-Faktor-Authentisierung (Smartphone und PIN) vergleichsweise sicher ist. Der Einzelhändler vor Ort erhält über die Kunden keine zusätzlichen Kenntnisse. Der zur Abwicklung der Zahlungen eingeschaltete Dienstleister erhält ebenfalls nur die nötigsten Daten. Der Konzern speichert jedoch – als Service für die Kunden – zentral jeden Einkauf personenbezogen und sehr detailliert. Bisher ist es nicht möglich, diese „Einkaufszettel“ zu löschen bzw. wenigstens die zeitlich unbefristete Abrufbarkeit in der App zu sperren. Die Umsetzung einer entsprechenden Funktion wurde jedoch zugesagt. Gegenwärtig nicht eingesetzt, aber durchaus möglich wären Analysen des Kundenverhaltens auf Basis der detaillierten Einkaufsdaten z.B. für individuelle Angebote. Wir haben ausdrücklich darauf hingewiesen, dass eine derartige Nutzung der Daten nur mit „informierter“ Einwilligung der Betroffenen zulässig ist.

Wer ein neues Zahlungsmittel oder Bezahlsystem einführt, muss die Kunden über die Risiken unterrichten. Es fallen stets Datenspuren an. Die Entscheidung, ob zusätzlich Details über die getätigten Einkäufe gespeichert, wofür sie genutzt und wann gelöscht werden, muss vom Kunden getroffen werden. Die Luftschnittstelle kontaktlos operierender Karten und Geräte bedarf besonderen Schutzes. Wer das nicht leistet, muss es offenlegen. Bargeld bleibt das datenschutzfreundlichste Zahlungsmittel.

13.1.3 Kontrolle der Girokontodaten zur Gebührenprüfung

Ein Petent erhielt von einer Bank die Mitteilung, bei der Überprüfung seines Girokontos sei festgestellt worden, dass er sein kostengünstiges Privatkonto für geschäftliche Zwecke genutzt habe. Deshalb kündige die Bank dieses Konto; er habe aber die Möglichkeit, sein Konto als Geschäftskonto weiterlaufen zu lassen. Der Petent war der Auffassung, dass die Kontrolle der Bank rechtswidrig erfolgte.

Banken mit unterschiedlichen Konditionen für Privat- und Geschäftsgirokonten haben grundsätzlich das Recht, Privatgirokonten darauf zu überprüfen,

ob sie falsch deklariert sind. Allerdings stellt eine Girokontoüberprüfung eine Datennutzung dar, die nicht unbeschränkt möglich ist. Beschäftigte, die derartige Kontrollen durchführen, sollten anhand von Compliance-Regelungen vorgeben, wann und nach welchen Kriterien Überprüfungen vorgenommen und in welchen Fällen Zufallsfunde berücksichtigt werden können.[227] Das Verfahren sollte für die Kunden möglichst transparent sein.

Die Bank konnte uns keine relevanten Kriterien benennen, nach denen Girokontoüberprüfungen durchgeführt werden. Die Beschäftigten der Bank entschieden selbst, ob und wie Kontrollen durchgeführt werden. Auch war die Bank nicht in der Lage, uns mitzuteilen, warum im konkreten Fall der Verdacht auf missbräuchliche Girokontonutzung bestand. Wir haben die Bank aufgefordert, für Girokontoüberprüfungen klare und nachvollziehbare Regelungen zu schaffen.

Die Überprüfung der tariflichen Einstufung von Girokonten sollte transparent und nach festen Compliance-Regeln erfolgen.

13.2 Andere Wirtschaftsunternehmen

13.2.1 Datenschutzprobleme bei Auskunfteien

Bei der Kontrolle zweier Auskunfteien haben wir verschiedene Datenschutzverstöße festgestellt. Beiden Auskunfteien wurde aufgegeben, Verfahrensänderungen vorzunehmen.

Auskunfteien sind berechtigt, einen Datensatz mit statistischen Wahrscheinlichkeitsdaten (Schätzdaten) anzureichern. Seit 2010 ist ausdrücklich geregelt, dass geschätzte Daten als solche deutlich zu kennzeichnen sind.[228] Es gelang uns in Verhandlungen, bei allen größeren Auskunfteien die Kennzeichnungspflicht durchzusetzen.

227 Erkenntnisse bei Geldwäscheprüfungen dürfen z.B. nicht für andere Zwecke genutzt werden.
228 § 35 Abs. 1 Satz 2 BDSG

Weiterhin verbesserungsbedürftig ist die glaubhafte Darstellung des vorgeschriebenen berechtigten Interesses der Kunden vor der Übermittlung der Daten.[229] Die anzukreuzenden stichwortartigen Gründe sind häufig nicht aussagekräftig. Sie sollten zumindest in den allgemeinen Geschäftsbedingungen näher erläutert werden.

Es ist sicherzustellen, dass die Kunden der Auskunfteien nur Daten des Unternehmens bzw. der Person erhalten, zu der nachgefragt wurde. Eine Suche mittels Trunkierung (Abkürzung eines Suchbegriffes bei Recherche in einer Datenbank), wie sie eine Auskunftei anbot, ist unzulässig, soweit es hierdurch ermöglicht wird, über die Ergebnisliste ohne weitere Darstellung eines berechtigten Interesses sämtliche Eintragungen, die zu dem verkürzten Datensatz vorliegen, abzurufen. Das Unternehmen hat inzwischen diese automatische Vervollständigung der Suchbegriffe aufgegeben. Ähnliche Probleme bestehen bei der von dieser Auskunftei angebotenen Geschäftsführersuche, bei der alle Geschäftsführer mit dem gesuchten Namen (einschließlich etwaiger Namenszusätze), Adresse und Geburtsdatum abgefragt werden können. Bei häufig vorkommenden Namen erhält der Abfragende teilweise mehr als 500 Datensätze. Da nicht für alle diese Geschäftsführerdaten ein berechtigtes Interesse bestehen kann, ist die Geschäftsführersuchfunktion rechtswidrig. Wir haben das Unternehmen darauf hingewiesen.

Teilweise bieten Auskunfteien einen sog. Nachtragsservice an. Kunden werden darüber informiert, dass eine Veränderung bei einem abgefragten Unternehmen stattgefunden hat, gleichzeitig wird der Grund der Änderung mitgeteilt. Nähere Informationen erhält der Kunde dann bei Benutzung eines Links, bei dem das berechtigte Interesse abgefragt wird. Wir haben darauf hingewiesen, dass jedenfalls die Weitergabe des Änderungsgrundes schon das Vorliegen eines berechtigten Interesses voraussetzt. Der Änderungsservice sollte sich deshalb auf die Tatsache des Vorliegens einer Änderung beschränken. Die Kunden der Auskunftei sollten außerdem vertraglich verpflichtet werden, bei Wegfall des berechtigten Interesses den Nachtragsservice zu deaktivieren.

Auskunfteien sind verpflichtet, bei Abfragen im automatisierten Abrufverfahren das berechtigte Interesse ihrer Kunden an den übermittelten Daten einzel-

229 § 29 Abs. 2 Satz 1 Nr. 1 BDSG

fallbezogen in einem Stichprobenverfahren zu überprüfen.[230] Nicht akzeptiert haben wir ein Überprüfungsverfahren, welches von den betrieblichen Datenschutzbeauftragten der anfragenden Unternehmen durchgeführt wurde, die dann gegenüber der Auskunftei nur ihre Ergebnisse mitteilten. Ein Outsourcing der Stichprobenüberprüfung ist nicht möglich, da der Gesetzgeber ausdrücklich geregelt hat, dass die Prüfung von der übermittelnden Stelle durchgeführt wird. Bei Auskunfteien, die Bonitätsdaten übermitteln, ist eine Stichprobe von zwei Promille geboten. Bei Auskunfteien, die nur Adressinformationen weitergeben, wird man einen etwas geringeren Prüfungsumfang akzeptieren können. Allerdings haben wir bei einem Adressermittlungsunternehmen, welches nur jede 10.000ste Anfrage überprüft hat, eine zu geringe Kontrollquote festgestellt.

Auskunfteien sind grundsätzlich verpflichtet, Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.[231] Da dies einen gewissen Verwaltungsaufwand verursacht, versuchen Auskunfteien teilweise, die Benachrichtigungspflicht zu umgehen. Nicht akzeptiert haben wir das Argument einer Auskunftei, bei ihrer Marktdurchdringung müsse jedes Unternehmen damit rechnen, sich im Datenbestand der Auskunftei zu befinden. Die Auskunftei hat sich inzwischen unserer Auffassung angeschlossen. Das Adressermittlungsunternehmen verzichtet auf die Benachrichtigung der Betroffenen mit der Begründung, ihre Kunden – meist Unternehmen – vertraglich zur Benachrichtigung zu verpflichten. Dies ist grundsätzlich möglich.[232] Allerdings hat die Auskunftei nie kontrolliert, ob die Unternehmen ihre vertragliche Verpflichtung auch erfüllen. Wir haben die Auskunftei aufgefordert, ihren Kunden einen genauen Informationstext vorzugeben und die vertragliche Informationspflicht stichprobenartig zu überprüfen.

Zwei Auskunfteien haben nach unserer Kontrolle ihr Datenschutzniveau erhöht.

230 § 29 Abs. 2 Satz 4 BDSG
231 § 33 Abs. 1 Satz 2 BDSG
232 § 33 Abs. 2 Satz 1 Nr. 1 BDSG

13.2.2 Berichterstattung über IHK-Wahlen

Ein Verein, der sich für die Abschaffung der Pflichtmitgliedschaft bei den Industrie- und Handelskammern einsetzt, veröffentlichte auf seiner Internetseite detaillierte Ergebnisse der Vollversammlungswahl, insbesondere die Stimmanteile aller gewählten und nichtgewählten Bewerberinnen und Bewerber. Die Daten habe der Verein mit Hilfe einer anonymen Quelle aus der Verwaltung der IHK zusammengestellt.

Das Wahlverfahren in den IHKs regelt die Vollversammlung in einer Wahlordnung.[233] In Berlin wurde festgelegt, dass nur die Namen der gewählten Bewerberinnen und Bewerber bekannt gegeben werden.[234] Insbesondere die Nichtgewählten mussten nicht damit rechnen, dass ihr genaues Wahlergebnis veröffentlich wird. Die Bekanntgabe des detaillierten Wahlergebnisses durch den Verein erfolgte ohne Einwilligung der Betroffenen oder einer rechtfertigenden Rechtsvorschrift und war somit rechtswidrig.[235] Der Verein kann sich nicht auf berechtigte Interessen an einer Veröffentlichung der Daten berufen, da die Betroffenen im Hinblick auf die Wahlordnung überwiegende Interessen an dem Ausschluss der Veröffentlichung haben.[236]

Der Verein hat sich zu Unrecht auf das sog. Medienprivileg berufen.[237] Nicht jede Internet-Veröffentlichung fällt unter das Medienprivileg, sondern nur die Veröffentlichung von Unternehmen oder Hilfsunternehmen der Presse. Außerdem kann die Veröffentlichung von Wahlergebnissen nicht als eigene journalistisch-redaktionelle Tätigkeit angesehen werden.

Wir haben das rechtswidrige Verhalten des Vereins beanstandet. Hierbei haben wir auch darauf hingewiesen, dass die Datenerhebung nur möglich war, weil mindestens ein Beschäftigter der IHK datenschutzrechtliche Pflichten verletzt hat.

233 § 5 Abs. 3 IHKG
234 § 14 Abs. 2 Wahlordnung der IHK zu Berlin
235 § 4 Abs. 1 BDSG
236 § 28 Abs. 1 Satz 1 Nr. 2 BDSG
237 § 41 Abs. 1 BDSG

Dritte sind nicht berechtigt, Wahlergebnisse zur Vollversammlung der IHK detaillierter zu veröffentlichen, als es die Wahlordnung vorgibt.

13.2.3 Reality-TV bei den Wasserbetrieben

Nachdem die Berliner Wasserbetriebe (BWB) einem Kunden auf dessen Privatgrundstück wegen angeblichen Zahlungsverzugs das Wasser abgestellt hatten, teilte er den BWB unverzüglich telefonisch mit, etwaige Rückstände sofort bezahlen zu wollen. Gleichzeitig bat er, das Wasser wieder anzustellen. Am selben Tag erschienen ein sog. Sperrkassierer der BWB sowie drei Mitarbeiter eines Filmteams. Diese fertigten ohne Einverständnis des Betroffenen Film- und Tonaufnahmen von seinem Grundstück sowie von seinen Familienangehörigen an, um die Aufnahmen für eine ZDF-Reportage in der Sendung „hallo deutschland“ zu verwenden.

Die Vorgehensweise war zu beanstanden.[238] Für eine Anstalt des öffentlichen Rechts wie die BWB ist die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.[239] Es lagen weder eine Einwilligung des Petenten noch eine entsprechende Rechtsvorschrift vor, die eine Übermittlung von Daten an das Filmteam erlaubt hätten. Die Verfahrensweise widersprach auch einem Beschluss des Abgeordnetenhauses, wonach Film- oder Fernsehaufnahmen nicht mit öffentlicher Unterstützung zu einer Verletzung von Persönlichkeitsrechten führen dürfen.[240] Bei Aufnahmen im häuslichen Bereich in Begleitung von Amtspersonen ist laut Beschluss die Einwilligung der Betroffenen spätestens am Vortag der Film- oder Fernsehaufnahmen einzuholen. Dies gilt insbesondere auch für die Herausgabe personenbezogener Daten zur Vorbereitung der Film- oder Fernsehaufnahmen.

Die BWB haben uns mitgeteilt, dass durch Verfahrensanweisungen nunmehr sichergestellt sei, dass bei einer künftigen Einbindung von Dritten (Filmteams) bei Inkassomaßnahmen vorab eine Zustimmung der betroffenen Kunden eingeholt wird. Mit Einholung der Zustimmung würden die Betroffenen auch über den Umfang der Datenübermittlung informiert sowie über die übrigen Umstände aufgeklärt, die mit der Einbeziehung des Dritten verbunden sind. Natürlich ist die Zustimmung nur rechtswirksam, wenn die Kunden im Fall ihrer Verweigerung keine Nachteile befürchten müssen.

Bei Datenübermittlungen an Stellen außerhalb des öffentlichen Bereichs - insbesondere an Medien - ist das Schutzbedürfnis der Betroffenen und die Pflicht zur Wahrung ihrer Persönlichkeitsrechte besonders groß.

13.2.4 Die indiskrete Warteschlange

Eine Petentin beschwerte sich über die Praxis bei einem Computerreparaturbetrieb. Dieser verlangte von seiner Kundschaft, den Namen, das Anliegen und die Gerätebezeichnung auf einem Terminal einzutippen, um auf zwei Großbildschirmen im Service-Bereich die Anzeige der noch verbleibenden Wartezeit zu ermöglichen. Als Grund für dieses Vorgehen gab der Betrieb an, dass es in der Vergangenheit Streitigkeiten hinsichtlich der Reihenfolge innerhalb der Kundschaft gegeben habe.

Die Anzeige von Kundennamen auf Monitoren im Service-Bereich ist eine Übermittlung von personenbezogenen Daten an Dritte. Eine Einwilligung der Betroffenen für diese Übermittlung hat der Betrieb nicht eingeholt. Die Übermittlung konnte nicht auf eine Rechtsgrundlage gestützt werden.[241] Eine Anzeige der Namen der Betroffenen auf den Monitoren war für den Reparaturauftrag nicht erforderlich.[242] Zwar konnte der Betrieb als berechtigtes Interesse an der Veröffentlichung dieser Daten die Vermeidung von Streitereien und Unstimmigkeiten anführen; bei den Kundinnen und Kunden überwogen jedoch die schutzwürdigen Interessen, diese Daten nicht jedem beliebigen Dritten zugänglich zu machen.[243]

238 § 26 Abs. 1 Satz 1 Nr. 3 BlnDSG
239 § 2 Abs. 1 i.V. m. § 13 BlnDSG
240 Beschluss vom 13. Mai 2004: Wahrung der Persönlichkeitsrechte bei Film- und Fernsehaufnahmen, siehe Anlage 3 des Plenarprotokolls, S. 4304
241 § 4 Abs. 1 BDSG
242 § 28 Abs. 1 Satz 1 Nr. 1 BDSG
243 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Der Reparaturbetrieb hat das Verfahren inzwischen datenschutzgerecht gestaltet: Neben der Möglichkeit der Nutzung eines Pseudonyms holt der Betrieb eine Einwilligung der Betroffenen für die Namensanzeige auf den Monitoren ein.

Die Veröffentlichung von personenbezogenen Kundendaten auf Anzeigemonitoren im Service-Bereich stellt eine Übermittlung dar, die nur durch eine Einwilligung der Betroffenen gerechtfertigt werden kann.

13.2.5 Bankdatenabfrage durch Unbekannte

Bei der Registrierung einer Prepaid-Karte einer Mobilfunkfirma wurde die Petentin nach ihren Kontoverbindungsdaten für weitere Aufladungen gefragt. Auf Nachfrage gab der Call-Center-Agent an, dass er nicht bei der Mobilfunkfirma beschäftigt sei, sondern bei einem dritten Unternehmen, und zudem von zu Hause aus arbeite. Die Petentin hielt dies für rechtswidrig.

Unternehmen können externe Dienstleister weisungsgebunden mit der Datenerhebung, -verarbeitung und -nutzung beauftragen, soweit es sich hierbei um Hilfsfunktionen handelt.[244] In diesem Fall bleibt die auftraggebende Stelle für den Umgang mit ihren personenbezogenen Daten beim Dienstleister verantwortlich. Datenflüsse zwischen Auftraggeber und Auftragnehmer sind keine Datenübermittlungen.[245] Vielmehr liegt eine Nutzung vor, die der Gesetzgeber privilegiert hat. Hierzu muss ein schriftlicher Auftragsdatenverarbeitungsvertrag geschlossen werden, der bestimmte Mindestbestandteile enthält.[246] Die Mobilfunkfirma hatte einen solchen Vertrag geschlossen und rechtmäßig das Call-Center mit der erforderlichen Datenerhebung beauftragt.

Die Einrichtung von Telearbeitsplätzen bedarf gesonderter technischer und organisatorischer Maßnahmen, die das Call-Center im Wesentlichen getroffen hatte. So besaßen die Call-Center-Agenten, die in Heimarbeit tätig waren,

244 § 11 BDSG
245 § 3 Abs. 8 Satz 3 BDSG
246 § 11 Abs. 2 Satz 2 BDSG

abschließbare, separate Räume, die von außen nicht einsehbar waren. Vor der Arbeitsaufnahme führte das Call-Center einen Hardwarecheck durch, um zu prüfen, ob die Infrastruktur den Anforderungen für die Heimarbeit entsprach. Während der Heimarbeitszeit durfte sich zudem keine weitere Person in dem Arbeitsraum befinden. Aufgrund unserer Anregungen hat das Call-Center mit allen in Heimarbeit Tätigen eine Vereinbarung geschlossen, die ihm eine Kontrolle der Wohnungen mit Heimarbeitsplätzen ermöglicht.

Setzt eine nicht-öffentliche Stelle einen Dritten für Hilfstätigkeiten beim Umgang mit personenbezogenen Daten ein, so kann eine Auftragsdatenverarbeitung vorliegen. Der Auftraggeber bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Es ist ein schriftlicher Auftragsdatenverarbeitungsvertrag mit bestimmten Mindestbestandteilen abzuschließen.

14 Aus der Arbeit der Sanktionsstelle

14.1 Entwicklung von Anordnungen

Stellen wir im Rahmen unserer Kontrolltätigkeit Datenschutzverstöße bei einer nicht-öffentlichen Stelle fest, so können wir nach Anhörung der verantwortlichen Stelle Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten anordnen.[247] Bei schwerwiegenden Verstößen kann das mit Mängeln behaftete Datenverarbeitungsverfahren sogar untersagt werden. Die Durchführung eines Anordnungs- und eines Bußgeldverfahrens kann gleichzeitig erfolgen, weil unterschiedliche Ziele mit den jeweiligen Verfahren verfolgt werden: Das Anordnungsverfahren wirkt in die Zukunft und führt zur Beseitigung von materiell-rechtlichen Datenschutzverstößen; mit einem Bußgeldverfahren wird hingegen eine Pflichtverletzung in der Vergangenheit sanktioniert.

Häufig beseitigen die Unternehmen ohne die Einleitung eines Anordnungsverfahrens die von uns festgestellten Mängel. Bei einem Online-Shop mussten wir allerdings tätig werden, weil er nicht die gesetzlichen Vorgaben für automatisierte Einzelentscheidungen einhielt.[248] Die Auswahl der angebotenen Zahlarten erfolgte bei diesem Online-Shop automatisiert unter Zugrundelegung einer in Echtzeit vorgenommenen Risikobewertung einer Auskunftei zur Bonität des Kunden. Das Unternehmen machte gegenüber seiner Kundschaft dieses Verfahren zur Entscheidungsfindung zunächst nicht transparent. Aufgrund unseres eingeleiteten Verfahrens hat der Online-Shop seinen Bestellvorgang umgestellt. Er informiert nunmehr die Betroffenen über das Verfahren und hat Maßnahmen ergriffen, damit sie die automatisiert getroffene Entscheidung anfechten können.

In Fällen, in denen die verantwortliche Stelle die eindeutigen Anforderungen des Datenschutzes verweigern, machen wir von der Möglichkeit der aufsichtsbehördlichen Anordnung Gebrauch.

247 § 38 Abs. 5 BDSG
248 § 6a BDSG

14.2 Ein Beispiel: Online-Arbeitsvermittlung ohne Verschlüsselung

Im Jahr 2009 beschwerte sich eine Bürgerin darüber, dass ein privater Arbeitsvermittler ihre personenbezogenen Daten mittels unverschlüsselter E-Mails an potenzielle Arbeitgeber versendet. Der Arbeitsvermittler hielt die unverschlüsselte Datenübermittlung unter Berufung auf die zuvor im Rahmen des Vermittlungsvertrags eingeholte schriftliche Einwilligung der Betroffenen für zulässig.

Der Gesetzgeber schreibt vor, dass jede datenverarbeitende Stelle technische und organisatorische Maßnahmen zur Datensicherung zu treffen hat.[249] U. a. ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[250] Dies kann insbesondere durch die Verwendung von Verschlüsselungsverfahren erfolgen.[251]

Betroffene können nicht wirksam auf diese technische und organisatorische Sicherung ihrer personenbezogenen Daten verzichten, da es sich bei der gesetzlichen Norm um eine Ordnungsvorschrift handelt, deren Adressat die verantwortliche Stelle ist.[252] Eine Einwilligung in den Verzicht auf Maßnahmen zur Datensicherheit ist gesetzlich nicht vorgesehen. Vielmehr setzt die Vorschrift eine rechtmäßige, z. B. durch Einwilligung legitimierte Datenverarbeitung voraus und verpflichtet für diesen Fall die verantwortliche Stelle zusätzlich zu bestimmten technisch-organisatorischen Maßnahmen. Wäre die Datensicherheitsvorschrift disponibel, hätte dies zur Folge, dass sich Unternehmen (insbesondere auch Betreiber sozialer Netzwerke) von Betroffenen eine umfassende Einwilligung in den Verzicht auf die Anforderungen der Norm sowie der dazugehörigen Anlage erteilen lassen und somit aus wirtschaftlichen Erwägungen gesetzlich festgelegte Datensicherheitsschranken unproblematisch umgehen könnten. Dies würde den Zweck der Vorschrift in erheblichem Maß beeinträchtigen.

249 § 9 Satz 1 BDSG
250 Nr. 4 der Anlage zu § 9 Satz 1 BDSG
251 Satz 3 der Anlage zu § 9 Satz 1 BDSG
252 Siehe auch 6.2 und 12.1.3

Nachdem wir den Arbeitsvermittler hierauf hingewiesen und erfolglos aufgefordert hatten, seine Praxis der unverschlüsselten Datenübermittlung zu ändern, erließen wir im Jahr 2010 eine Anordnung, mit der wir ihm aufgaben, im Rahmen seiner Tätigkeit Bewerberdaten, soweit diese per E-Mail an potenzielle Arbeitgeber versendet werden, zu verschlüsseln oder derart zu pseudonymisieren, dass von den Daten nicht auf die Identität der betroffenen Person geschlossen werden kann.

Gegen diese Anordnung hat der Arbeitsvermittler Klage erhoben, der zunächst vom Verwaltungsgericht Berlin stattgegeben wurde. Zur Begründung führte das Gericht u. a. an, die Anordnung sei nicht verhältnismäßig, weil der finanzielle Aufwand zur Anschaffung von Verschlüsselungssoftware angesichts der Möglichkeit einer Einwilligung der Betroffenen in eine unverschlüsselte Datenübermittlung zu hoch sei.

Unsere Berufung gegen dieses Urteil hat das Oberverwaltungsgericht (OVG) Berlin-Brandenburg mit der Begründung zugelassen, dass der Rechtssache grundsätzliche Bedeutung zukomme, weil die Frage nach der Disponibilität des § 9 BDSG entscheidungserheblich, einer fallübergreifenden Klärung zugänglich und bislang weder obergerichtlich noch höchstrichterlich entschieden sei.

Während des Berufungsverfahrens gab der Arbeitsvermittler seine Vermittlungstätigkeit endgültig auf, weshalb die Hauptsache übereinstimmend für erledigt erklärt wurde. Das Verfahren wurde eingestellt, das Urteil des Verwaltungsgerichts Berlin für wirkungslos erklärt und die Kosten des Verfahrens den Beteiligten jeweils zur Hälfte auferlegt. Das OVG begründete die Kostenentscheidung damit, dass der Ausgang des Rechtstreits ohne das erledigende Ereignis offen gewesen wäre.

Eine Einwilligung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten entbindet die verantwortliche Stelle nicht von der Pflicht, durch technische und organisatorische Maßnahmen sicherzustellen, dass die Datensicherheit während der Verarbeitung gewährleistet ist.

14.3 Entwicklung von Ordnungswidrigkeitenverfahren

Wir haben 16 Bußgeld- oder Verwarnungsbescheide erlassen und Geldbußen von insgesamt 44.235 € festgesetzt. In fünf Fällen haben wir einen Strafantrag gestellt. Häufig war die Einleitung eines Bußgeldverfahrens notwendig, weil die nicht-öffentliche Stelle unserer Behörde die erforderlichen Auskünfte nicht erteilt hat.[253]

So haben wir ein fünfstelliges Bußgeld festgesetzt, weil ein Unternehmen bei dem Verkauf einer Abonnementzeitschrift, die das ankaufende Unternehmen nur noch als Kioskzeitschrift weiterführte, die dazugehörigen Kundendaten einschließlich Kontoverbindungsdaten ohne Einwilligung der Betroffenen übermittelt hatte; der Empfänger der Daten wollte die Kunden mit einer anderen Zeitschrift beliefern, eine zivilrechtliche Zustimmung zum Vertragsübergang lag jedoch nicht vor. Die Datenübermittlung bei dieser Unternehmenstransaktion konnte auf keine Rechtsgrundlage gestützt werden. [254]

Ein vierstelliges Bußgeld setzten wir gegen einen Arzt fest,[255] der seiner Informationspflicht nicht rechtzeitig und nicht richtig nachgekommen ist. Die Arztpraxis hatte Unterlagen, die sensitive personenbezogene Daten[256] der Patienten enthielten (u. a. Diagnosen, Laborwerte und Überweisungsträger), ungeschreddert im Hausmüll entsorgt. Dank des Hinweises eines Anwohners konnten wir die Unterlagen sicherstellen. Erst nach längerer Zeit und mehrfacher Aufforderung kam der Arzt seiner Pflicht nach, seine Patienten darüber zu informieren, dass ihre Patientendaten unrechtmäßig mindestens einer dritten Person zur Kenntnis gelangt waren.[257]

Gegen ein Wohnungsunternehmen setzten wir ein Bußgeld im vierstelligen Bereich fest,[258] weil die Verantwortlichen es versäumt hatten, einen Auftragsdatenverarbeitungsvertrag mit einem externen Dienstleister zu schließen. Das Unternehmen hatte Daten seiner Mieter inklusive Kontodaten und Angaben

253 § 43 Abs. 1 Nr. 10 BDSG
254 § 43 Abs. 2 Nr. 1 BDSG
255 § 43 Abs. 2 Nr. 7 BDSG
256 § 3 Abs. 9 BDSG
257 § 42a Satz 1 Nr. 1 und 2 BDSG
258 § 43 Abs. 1 Nr. 2b BDSG

zu offenen Forderungen einem Dienstleister übermittelt, der u. a. die Mahnungen an säumige Mieter fertigte. Dieser Dienstleister stellte die Daten seinerseits weiteren Unterauftragnehmern zur Verfügung. Für solche Datenverarbeitungen ist ein Vertrag zu schließen,[259] der die Einhaltung der gesetzlich gebotenen Mindeststandards beim ausgelagerten Datenumgang sicherstellt.

Ein weiterer Bußgeldbescheid erging aufgrund einer unberechtigt getätigten Kfz-Halterabfrage,[260] die uns das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) meldete. Die Betroffene hatte einen Schuldner, gegen den sie einen gerichtlichen Vollstreckungsbescheid wegen einer Forderung ohne Bezug zum Straßenverkehr besaß, zufällig mit seinem Fahrzeug im Fernsehen gesehen und sich das Kennzeichen notiert. Mit dieser Information beantragte sie beim LABO im Online-Verfahren eine einfache Fahrzeug- und Halterauskunft nach dem Straßenverkehrsgesetz.[261] Bei der Antragstellung wird darauf hingewiesen, dass rein zivilrechtliche Ansprüche, die nicht in Verbindung mit dem Straßenverkehr stehen, keinen Auskunftsanspruch darstellen. Um sich die Auskunft auch ohne Vorliegen eines berechtigten Interesses zu erschleichen, gab die Betroffene als Auskunftsgrund fälschlicher Weise einen Tankbetrug an.

Die Verhängung von Bußgeldern stellt ein wirksames Mittel dar, Datenschutzverstöße zu ahnden.

259 § 11 Abs. 2 Satz 2 BDSG
260 § 43 Abs. 2 Nr. 4 BDSG
261 § 39 Abs. 2 Nr. 1 StVG

15 Europäischer und internationaler Datenschutz

15.1 Neue Entwicklungen

Im Dezember ist das neue europäische Grenzüberwachungssystem **EUROSUR**[262] gestartet, an dem sich zunächst 18 EU-Mitgliedstaaten mit Außengrenzen beteiligen.[263] Mit High-Tech wie Offshore-Sensoren und Aufklärungsgeräten sollen „problematische Menschenströme" – so die offizielle Terminologie – frühzeitig erkannt werden. Drohnen und Satelliten stellen die Überwachung aus der Luft[264] bzw. dem Weltall sicher. Damit sollen grenzüberschreitende Kriminalität und illegale Einwanderung in die EU verhindert, ggf. aber auch Rettungsaktionen in Bezug auf Flüchtlinge in Seenot erleichtert werden. Im Vordergrund steht aber eindeutig die Abschottung der „Festung Europa" vor außereuropäischen Flüchtlingen. Bezweckt wird eine bessere Kooperation zwischen den nationalen Grenzschutzbehörden. Deren Koordinierungszentren sollen ihre Informationen an die EU-Grenzschutzagentur Frontex liefern, die hieraus ein europäisches Lagebild erstellt. Auch wenn im Rahmen von EUROSUR selbst die Verarbeitung personenbezogener Daten einzelner Menschen die Ausnahme sein soll, macht diese Entwicklung nur allzu deutlich, welche Dimension der Überwachung der europäischen Außengrenzen und ihres Vorbereichs mittlerweile erreicht worden ist.

In diesem Zusammenhang sind auch die Vorschläge der Kommission für „intelligente Grenzen" vom Februar zu sehen, die ein **Einreise-/Ausreisesystem (EES)**, ein **Registrierungsprogramm für Reisende (RTP)** für den Schengen-Raum und für einen geänderten Schengener Grenzkodex umfassen. Die

262 **Euro**pean **Bor**der Surveillance; siehe EU-Verordnung Nr. 1052/2013 des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zur Errichtung eines Europäischen Grenzüberwachungssystems (EUROSUR), ABl. L 295 vom 6. November 2013, S. 11 ff.
263 Das sind die Mittelmeerländer, die osteuropäischen Staaten sowie Norwegen. Andere Länder – auch Deutschland – werden Ende 2014 teilnehmen.
264 Siehe hierzu das Arbeitspapier der "Berlin Group" zum Datenschutz bei Überwachung aus der Luft, vom 2./3. September 2013, Dokumentenband 2013, S. 180; siehe 17.5

Vorschläge, die noch vom Europäischen Parlament und vom Rat angenommen werden müssen, sehen die zentrale Speicherung aller Ein- und Ausreisedaten von Nicht-Europäern auch dann vor, wenn sie kein Visum für den Schengen-Raum benötigen. Diese zentrale Speicherung soll das Abstempeln der Reisepässe an der Grenze ersetzen. Auf diese Weise soll überprüft werden, ob Betroffene die höchstens zulässige Aufenthaltsdauer überschritten haben. Nach zwei Jahren soll geklärt werden, ob Strafverfolgungsbehörden und Drittstaaten der Zugriff auf das EES ermöglicht wird, nach drei Jahren sollen auch biometrische Daten von Einreisenden erfasst werden.

Die Art. 29-Datenschutzgruppe hält die im EES geplante Datenverarbeitung für unverhältnismäßig und sieht in ihr einen Verstoß gegen Art. 8 EMRK.[265] Die geplante zentrale Datenbank würde nur einen geringen Anteil der Reisenden an den Schengen-Grenzen erfassen und gegenüber dem schon existierenden Visa-Informationssystem VIS keinen zusätzlichen praktischen Nutzen bei der Überwachung der Höchstaufenthaltsdauer bewirken. Insbesondere bemängelt die Art. 29-Gruppe, dass der Vorschlag der Kommission nicht die Ursachen der illegalen Migration und Beschäftigung bekämpft und stattdessen auf eine neue zentrale Datenbank setzt, mit der lediglich Einzelfälle illegaler Aufenthalte ermittelt werden können. Andere Alternativen, etwa Sanktionen gegen Arbeitgeber illegaler Migranten, seien von der Kommission nicht ausreichend durchgesetzt worden.

Keine neuen Entwicklungen gibt es in Bezug auf das Abkommen zwischen der EU und den USA von 2010 zur Übermittlung von Zahlungsverkehrsdaten[266] (sog. **SWIFT[267]-Abkommen**). Nach den Enthüllungen über die umfassende NSA-Überwachung[268] der weltweiten Online-Kommunikation entstanden Zweifel an der Sicherheit europäischer Bankdaten. Den USA war seinerzeit gestattet worden, zur Aufdeckung von Finanzströmen mit terroristischem Hintergrund Auskunftsverlangen an das Bankennetzwerk SWIFT, eine 1973 gegründete Genossenschaft belgischen Rechts, zu richten. Angesichts des NSA-Überwachungsskandals hat das Europäische Parlament Ende Oktober

265 Stellungnahme 5/2013 zu intelligenten Grenzen vom 6. Juni 2013 (WP 206), siehe Dokumentenband 2013, S. 114

266 **T**errorist **F**inance **T**racking **P**rogram (TFTP) II-Abkommen

267 Society for Worldwide Interbank Financial Telecommunication

268 Siehe 2.2 und 3.3

die Kommission aufgefordert, das Abkommen vorübergehend auszusetzen. Die Europäische Kommission ist dem nicht gefolgt mit der Begründung, dass eine Prüfung ergeben habe, dass die USA im Zuge der Terrorismusbekämpfung nicht gegen das Abkommen verstoßen hätten. Allerdings würde die Kommission die Angelegenheit weiterhin aufmerksam verfolgen. Dessen ungeachtet haben die Aufsichtsbehörden Belgiens und der Niederlande angekündigt, in einer gemeinsamen Aktion bei SWIFT zu prüfen, ob es unberechtigte Zugriffe der USA auf die Banktransaktionsdaten europäischer Bürgerinnen und Bürger gegeben hat.[269]

15.2 Weitere Ergebnisse aus Brüssel

Das Verfahren zur gegenseitigen **Anerkennung von verbindlichen Unternehmensregelungen** in der EU (Mutual Recognition), das vor zehn Jahren u. a. auf Berliner Initiative aus der Taufe gehoben wurde, ist weiter auf dem Erfolgskurs.[270] Inzwischen haben die Aufsichtsbehörden in Europa in diesem Verfahren Unternehmensregelungen von fast 50 global tätigen Konzernen als mit ausreichenden Datenschutzgarantien versehen anerkannt.[271] Während diese sog. Binding Corporate Rules (BCR) vornehmlich die Eigenverarbeitung innerhalb der jeweiligen Konzerne betreffen, können seit Jahresbeginn auch Unternehmensregelungen für Auftragsdatenverarbeiter von ebensolchen Firmen den Aufsichtsbehörden vorgelegt werden; aufgrund der technischen Entwicklungen insbesondere im Bereich des Cloud Computing wird hierfür in der Wirtschaft ein großer Bedarf gesehen. Das hat die Art. 29-Datenschutzgruppe, in der wir die Bundesländer vertreten, bereits im letzten Jahr erkannt und in einem Arbeitspapier die notwendigen Bestandteile solcher Konzernregelungen aufgelistet.[272] Zusätzlich hat sie für die Unternehmen ein Musterantragsformular für die Anerkennung ihrer Regelungen durch die europäischen Datenschutzauf-

269 Gemeinsame Presseerklärung vom 13. November 2013, abrufbar unter www.dutchdpa.nl/Pages/en_pb-20131113-swift-bank-data-security.aspx

270 JB 2011, 10.1 (S. 158)

271 Eine Liste der Konzerne ist abrufbar unter ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

272 Arbeitsdokument 2/2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter vom 6. Juni 2012 (WP 195), Dokumentenband 2013, S. 35

sichtsbehörden entworfen[273] und ein erläuterndes Papier für diese neue Art von Unternehmensregelungen verabschiedet.[274] Zudem verhandelt die französische Datenschutzkommission im Auftrag der europäischen Datenschutzbehörden mit dem Datenschutzgremium der Asiatisch-pazifischen Wirtschaftsgemeinschaft (APEC) über eine Angleichung der Regeln über den grenzüberschreitenden Datenverkehr im Bereich der Wirtschaft. Käme es hier zu einer Einigung, so wäre ein weltweit einheitlicher Standard für grenzüberschreitende Datenflüsse denkbar. Dabei wird es darauf ankommen, dass die geltenden europäischen Standards nicht abgesenkt werden.

Die Art. 29-Datenschutzgruppe hat daneben weitere Papiere verabschiedet. So hat sie sich mit dem Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Entwicklung, Verbreitung und Nutzung von **Apps auf intelligenten Endgeräten** befasst und hierbei u. a. die Verpflichtung zur korrekten Aufklärung der Endnutzer betont und zur Verarbeitung der von Kindern und über Kinder erfassten Daten nach Treu und Glauben.[275] Vor dem Hintergrund der im Sommer geänderten Informationsweiterverwendungsrichtlinie[276] untersuchte die Gruppe schließlich die datenschutzrechtlichen Aspekte, die bei **Open Data und Weiterverwendung von Informationen** des öffentlichen Sektors beachtet werden müssen. Die hierzu beschlossene Stellungnahme enthält wichtige Leitlinien und praktische Beispiele zur datenschutzgerechten Bereitstellung von Informationen des öffentlichen Sektors und hebt die Bedeutung von Anonymisierungsverfahren in diesem Zusammenhang hervor.[277] Ein weiteres Arbeitspapier gibt Leitlinien dafür, wie die Einwilligung der Nutzenden zur Verwendung von **Cookies** eingeholt wird.[278]

273 Nur englische Fassung: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, adopted on 17 September 2012 (WP 195a)

274 Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter vom 19. April 2013 (WP 204), Dokumentenband 2013, S. 89

275 Stellungnahme 2/2013 zu Apps auf intelligenten Endgeräten vom 27. Februar 2013 (WP 202), Dokumentenband 2013, S. 47; siehe auch 17.3

276 Richtlinie 2003/98/EC, geändert durch die Richtlinie 2013/37/EU

277 Bislang nur englische Fassung: Opinion 6/2013 on open data and public sector information ("PSI") reuse, adopted on 5 June 2013 (WP 207)

278 Arbeitsunterlage 2/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies vom 2. Oktober 2013 (WP 208)

16 Informationspflicht bei Datenlecks

16.1 Datenlecks in der Wirtschaft

Leider kein Einzelfall: Patientenunterlagen im Müll

Im Hausmüll eines Wohngebäudes stellten wir aufgrund eines Hinweises aus der Bevölkerung Patientenunterlagen einer in diesem Gebäude untergebrachten Arztpraxis sicher. Bei den Unterlagen handelte es sich um Laborbefunde, Überweisungsscheine, Verordnungen zu Krankenhausbehandlungen oder Reha-Maßnahmen sowie Zahlungsbelege für Zuzahlungen. Diese Dokumente waren weder geschreddert noch auf andere Weise unkenntlich gemacht worden. Die Mülltonnen waren von der Straße aus zugänglich.

Leider stellen solche Aktenfunde keine Seltenheit dar.[279] Hier verwies der Praxisinhaber darauf, dass es sich bei den meisten Unterlagen „nur" um Fehldrucke gehandelt habe und im Übrigen Unterlagen in seiner Praxis grundsätzlich geschreddert oder geschwärzt würden. Wir mussten den Arzt darauf hinweisen, dass auch die sichergestellten Fehldrucke Angaben zur Gesundheit[280] enthielten. Schon der Hinweis darauf, dass sich eine Person in ärztlicher Behandlung befindet, stellt eine sensitive Information dar, die zudem der ärztlichen Schweigepflicht[281] unterliegt. Schließlich kam der Arzt unserer Aufforderung nach, die Betroffenen zu unterrichten. Leider erweckten die dafür verwendeten Benachrichtigungsschreiben den Eindruck, dass die Unterlagen aus dem Hausmüll durch die Sicherstellung „gestohlen" worden seien. Der Arzt ging nicht darauf ein, dass die Papierunterlagen in dem frei zugänglichen Hausmüll unzulässig entsorgt worden waren und sie daher von fremden Personen zur Kenntnis genommen werden konnten. Dieser Umstand begründete die Pflicht zur Unterrichtung der Betroffenen nach § 42a BDSG. Aufgrund der fehlerhaften Benachrichtigung der Betroffenen leiteten wir gegen den Arzt ein Bußgeldverfahren ein, der ein Bußgeld in vierstelliger Höhe entrichten musste.

279 Siehe zuletzt JB 2012, 15.2.1

280 Dabei handelt es sich um besonders schutzwürdige personenbezogene Daten nach § 3 Abs. 9 BDSG.

281 Die Verletzung der ärztlichen Schweigepflicht ist nach § 203 Strafgesetzbuch strafbar.

Die sichergestellten Unterlagen holte er ab und bestätigte, dass diese durch ein professionelles Unternehmen vernichtet wurden.

Die ordnungsgemäße Mitteilung nach § 42a BDSG ist bußgeldbewehrt. Wer eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht, kann mit einer Geldbuße von bis zu 300.000 € belegt werden, wenn dies vorsätzlich oder fahrlässig geschieht.

Pflicht zur Recherche der aktuellen Adressen der Betroffenen?

Aus einer Steuerberatungspraxis verschwand eine externe Festplatte. Auf dieser waren zur Sicherung Datensätze gespeichert, die mit einer speziellen Steuerberatungssoftware angelegt worden waren. Die Datensätze enthielten Namen und Anschriften von Mandanten, Bankverbindungsdaten, Steuernummern sowie Informationen aus der Beratungstätigkeit. Da die Steuerberatungspraxis zum Teil die Lohnbuchführung für Mandanten durchführte, waren außerdem Sozialversicherungs- und Kontonummern von Beschäftigten der Mandanten auf der Festplatte gespeichert.

Die daraufhin verschickten Schreiben, mit denen die Mandanten von dem Verlust benachrichtigt wurden, kamen zum Teil zurück, da z. B. die Adressen nicht mehr aktuell waren. Die Steuerberatungspraxis stellte sich zunächst auf den Standpunkt, dass der Benachrichtigungspflicht nach § 42a BDSG durch den Versuch, die Betroffenen zu informieren, genüge getan worden sei. Eine Pflicht zur Recherche der Adressen bestehe nicht. Wir wiesen darauf hin, dass nach dem Gesetz die Information der Öffentlichkeit an die Stelle der Benachrichtigung der Betroffenen tritt, wenn diese einen unverhältnismäßigen Aufwand erfordern würde. Auf den Einwand, dass die Veröffentlichung des Vorfalles aufgrund der unverhältnismäßigen Kosten nicht gerechtfertigt sei, teilten wir mit, dass Erwägungen zum Aufwand zwar bei der Auswahl des Unterrichtungsinstruments eine Rolle spielen dürften, nicht aber bei der Frage, ob überhaupt zu informieren ist. Letzteres ist im Rahmen der nach § 42a Satz 1 BDSG erforderlichen Gefahrenprognose festzustellen: Kommt die verantwortliche Stelle zu dem Ergebnis, dass schwere Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, muss sie diese entweder benachrichtigen oder eine in ihrem Wirkungsgrad gleich geeignete Unterrichtungsmaßnahme ergreifen. Die Steuerberatungspraxis kam zu dem Ergebnis, dass in den meisten Rückläuferfällen aufgrund des Alters und der Art der Daten keine schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohten. Wir hatten keine Anhaltspunkte, an dieser Gefahrenprognose zu zweifeln. In insgesamt sechs Fällen waren die Daten hingegen so aktuell, dass eine Benachrichtigungspflicht angenommen wurde und die Steuerberatungspraxis die Adressdaten nachrecherchierte.

Bei unverhältnismäßigem Aufwand tritt gem. § 42a Satz 5 BDSG an die Stelle der individuellen Benachrichtigung der Betroffenen die Information der Öffentlichkeit durch eine Maßnahme, die in ihrer Wirksamkeit ebenso geeignet ist wie die direkte Benachrichtigung. Dazu zählt die Veröffentlichung durch Anzeigen mit mindestens einer halben Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen.

Missbräuchlicher Datenzugriff im Ausland

Eine Interessenvertretung der deutschen Wirtschaft teilte uns mit, dass bei einem Hackerangriff auf die Netzwerke von Niederlassungen (Delegationen) in Osteuropa Dokumente abgezogen und an anderer Stelle im Internet veröffentlicht wurden. Die Interessenvertretung hatte vom Landeskriminalamt den Hinweis erhalten, dass die Dokumente im Internet verfügbar seien. Bei einer Delegation gehörten zu den betroffenen Daten insbesondere Kreditkartenabrechnungen und Passdaten des Leiters des Delegiertenbüros und seiner Ehefrau. Ansonsten waren Personaldaten der Beschäftigten der Büros und Daten von Beschäftigten der Interessenvertretungen aus Sitzungsprotokollen betroffen sowie Lebensläufe von Bewerbern für die Auslandsbüros.

Für die Informationspflicht nach § 42a BDSG sind wir grundsätzlich von einer Anwendbarkeit des deutschen Datenschutzrechts ausgegangen. Die ausländischen Niederlassungen der Interessenvertretung sind rechtlich unselbständig, sodass die bei diesen Stellen gespeicherten Daten der Interessenvertretung in Deutschland zugerechnet wurden.[282] Für die Rechte und schutzwürdigen

282 Art. 4 Abs. 1 a) Europäische Datenschutzrichtlinie 95/46/EG, § 1 Abs. 2 Ziff. 3 BDSG

Interessen der Beschäftigten der Auslandsbüros drohten nach der Prognose der Interessenvertretung keine schwerwiegenden Beeinträchtigungen. Nur in Ausnahmefällen waren hier über den Namen der Beschäftigten hinaus weitere Daten abhanden gekommen. Gleichwohl wurden die Beschäftigten der Büros von der Interessenvertretung oder den jeweiligen Büroleitungen mündlich informiert. Auf unsere dringende Empfehlung hin wurden auch die betroffenen Bewerber, deren Lebensläufe zu den vom Angriff betroffenen Dokumenten gehörten, nachträglich benachrichtigt. Im Hinblick auf die personenbezogenen Daten von Beschäftigten und Mitgliedern der Interessenvertretung bestand keine Benachrichtigungspflicht, da es sich bei den Daten aus den Sitzungsprotokollen nicht um Angaben handelte, die von den Kategorien des § 42a Satz 1 BDSG erfasst waren. Nachteilige Folgen wurden von der Interessenvertretung für den Büroleiter und für seine Ehefrau gesehen, deren Pass- und Kreditkartendaten gehackt worden waren. Diese waren bereits über den Zugriff informiert.

Im Rahmen der Prüfung des Vorfalles stellte sich heraus, dass keine einheitlichen Vorgaben für die Auslandsbüros zu den erforderlichen technisch-organisatorischen Maßnahmen existierten. Wir haben der Interessenvertretung daher als Sofortmaßnahme aufgegeben, entsprechende Empfehlungen zur Absicherung der Systeme zu erstellen und die Umsetzung dieser Maßnahmen durch die Auslandsbüros zu überprüfen.

Verantwortliche Stellen müssen dafür Sorge tragen, dass technisch-organisatorische Vorgaben für die gesamte Datenverarbeitung ihrer Organisation umgesetzt werden, d. h. auch in rechtlich unselbständigen Niederlassungen.

Trojaner im Anhang

Durch die Mitteilung eines Online-Shopping-Portals und Hinweisen in der Presse sowie aufgrund von Beschwerden von Betroffenen wurden wir darauf aufmerksam, dass die Kunden des Portals E-Mails mit gefälschten Rechnungen erhalten hatten. Die Anhänge zu den E-Mails waren mit einem sog. „Trojaner“ versehen, sodass beim Öffnen der Anlage ein „Downloader-Virus“ ausgeführt wurde. Damit konnte das Computersystem der Betroffenen unter die Kontrolle von Dritten gebracht und für böswillige Zwecke missbraucht werden. Die Betroffenen teilten teilweise mit, dass ihre E-Mail-Adressen nicht „sprechend“ waren, d. h. keine Hinweise auf Vor- und Nachnamen enthielten. Gleichwohl waren sie in den E-Mails mit korrektem Vor- und Zunamen adressiert worden, sodass die Rechnungsstellung per E-Mail durchaus glaubwürdig war. Erstaunlich war zudem, dass die Trojaner-E-Mails an E-Mail-Adressen gesendet worden waren, die die Betroffenen speziell für die Nutzung des Online-Shopping-Portals angelegt hatten, ohne diese sonst zu verwenden. Diese Umstände deuteten darauf hin, dass die verwendeten E-Mail-Adressen und Namen durch ein Datenleck bei dem Online-Shopping-Portal abhanden gekommen waren.

Die Kunden des Portals wurden per E-Mail benachrichtigt, dass die Betreiberin nicht Absenderin der gefälschten Rechnungsmails gewesen sei und auch zukünftig keine solche E-Mails versenden werde. Den Kunden wurde dringend empfohlen, weder die gefälschte Rechnungsmail noch die Anhänge zu öffnen. Ähnliche Informationen wurden von der Betreiberin auch telefonisch im Ansagetext der Kundenhotline geschaltet sowie auf dem Blog des Portals und in den Profilseiten des Portals bei sozialen Netzwerken eingestellt. Die Betreiberin des Portals engagierte zudem ein auf forensische Untersuchungen und IT-Sicherheit spezialisiertes Unternehmen zur Analyse der Vorkommnisse. Weder bei der eigenen noch bei der durch die externe Firma durchgeführten Analyse konnten nach Angaben der Betreiberin Nachweise für eine Verletzung der Datensicherheit, der Zugänglichmachung von Daten an Dritte oder für einen Hackerangriff auf die Systeme des Portals gefunden werden. Die Betreiberin legte die ergriffenen Maßnahmen zur Analyse ausführlich dar. Wir hatten keine Anhaltspunkte, an der Effektivität oder Eignung der ergriffenen Maßnahmen zu zweifeln. Es blieb daher ungeklärt, wo und wie die missbrauchten E-Mail-Adressen und Kundendaten gewonnen worden waren und ob diese bei der Betreiberin des Online-Shopping-Portals abgegriffen wurden. Die Betreiberin kündigte fortlaufende Untersuchungen an und wird uns über diese informieren.

Auch wenn nicht feststeht, ob eine Pflicht zur Mitteilung nach § 42a BDSG oder § 15a TMG besteht, kann es sinnvoll sein, die Betroffenen zeitnah zu benachrichtigen. Letztlich können wenige Stunden oder gar Minuten für die Wirksamkeit von Abwehrmaßnahmen und die Verhinderung größeren Schadens entscheidend sein.

Unschöne Urlaubsüberraschung

Hacker bemächtigten sich des Servers eines Dienstleisters in Nordrhein-Westfalen, der bundesweit für verschiedene (Online-)Reisebüros tätig war. Sie lasen eine Vielzahl von Datensätzen mit Kreditkartentypen, Kreditkartennummern, Verifikationsnummern, Ablaufdaten, Anschriftendaten, Telefonnummern und E-Mail-Adressen aus. Als Auftraggeber dieses Dienstleisters meldete sich bei uns ein Berliner Unternehmen, das über zwei Online-Portale Reiseleistungen an Endkunden vermittelt. Insgesamt waren 96 Kunden dieser Berliner Online-Portale von dem Hackerangriff betroffen.

Diese Kunden wurden von der Betreiberin der Berliner Reiseportale per E-Mail informiert, zusätzlich telefonisch kontaktiert und im Falle erfolgloser telefonischer Kontaktversuche auf dem Postwege angeschrieben. Zum Teil hatte der Dienstleister bereits die Kreditkartenunternehmen betroffener Kunden informiert, sodass die Karten gesperrt und die Kunden von den Kreditkartenunternehmen unterrichtet worden waren. Dies war nicht in allen Fällen möglich, da die Kreditkartendaten bei Reiseantritt gelöscht werden und dem Dienstleister nicht mehr vorlagen.

In der praktischen Umsetzung war die Tätigkeit des Dienstleisters für die Online-Reisebüros als Verarbeitung im Auftrag zu qualifizieren. Der zur Vereinbarung der Dienstleistung eingesetzte Mustervertrag musste allerdings an die Anforderungen des § 11 BDSG angepasst werden. Dies hatte eine Prüfung des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ergeben.

Für einen Verlust von Daten, die beim Auftragnehmer im Auftrag des Auftraggebers gespeichert waren, ist der Auftraggeber verantwortlich. Dieser muss bei Vorliegen der Voraussetzungen nach § 42a BDSG benachrichtigen.

16.2 Datenlecks in der Verwaltung

Wir werden immer wieder gefragt, ob für öffentliche Stellen, die am Wettbewerb teilnehmen, die Informationspflicht des § 18a BlnDSG oder die des § 42a

gilt. Letzteres ist richtig. Zwar wird die Anwendbarkeit des § 18a BlnDSG für solche Stellen nicht ausgeschlossen,[283] und es wird sogar explizit auf die Informationspflicht nach BDSG verwiesen.[284] Eine parallele Anwendung der beiden Informationspflichten ergibt aber keinen Sinn, da die Normen sich in ihren Anwendungsvoraussetzungen unterscheiden: § 42a BDSG ist nur einschlägig, wenn Daten der in § 42a Satz 1 BDSG genannten Kategorien abhandenkommen. Entsprechende Einschränkungen sind in § 18a BlnDSG nicht enthalten. Vor diesem Hintergrund ist davon auszugehen, dass aufgrund eines gesetzgeberischen Redaktionsversehens die Anwendbarkeit des § 18a BlnDSG für öffentliche Stellen, die am Wettbewerb teilnehmen, nicht ausgeschlossen wurde. Unsere Anregung, das BlnDSG entsprechend anzupassen, wurde bisher nicht aufgegriffen.

Schulungsunterlagen mit personenbezogenen Daten

Bei der Veröffentlichung von Schulungsunterlagen zum Aufbau von Honorarunterlagen für Ärzte kam es bei der Kassenärztlichen Vereinigung Berlin (KV) zu einem Fehler: Die Unterlagen enthielten Musterbeispiele, die aus unterschiedlichen Original-Honorarunterlagen von Ärzten zusammengestellt worden waren. In der Papierversion der Schulungsunterlagen waren personenbezogene Informationen geschwärzt worden. Bei der Erstellung der für die Veröffentlichung vorgesehenen PDFs war diese Schwärzung technisch nur vordergründig vorgenommen worden, sodass die Unterlagen bei einer bestimmten Einstellung der Druckoptionen ohne Schwärzung ausgedruckt werden konnten. Die Kassenärztliche Vereinigung nahm die Unterlagen vom Netz und informierte die betroffenen Ärzte per Post.

Bei der Durchsicht der uns übersandten Unterlagen stellten wir fest, dass nicht nur Daten von Ärzten, sondern auch Patientendaten in den Übersichten vorhanden waren. Auf Nachfrage erklärte die KV, dass Unterlagen mit Patientendaten nicht als "Portable Document Format" (PDF) ins Internet eingestellt worden seien. Im PDF-Format können zwar Daten per Mausklick geschwärzt, aber mit entsprechender Software wieder sichtbar gemacht werden. In diesen

283 § 2 Abs. 3 Satz 1 BlnDSG
284 § 2 Abs. 3 Satz 2 BlnDSG

Fällen seien vielmehr die geschwärzten Papierübersichten gescannt und dann ins Netz gestellt worden, sodass es nicht zu dem Fehler gekommen sei. Die Richtigkeit dieser Darstellung konnten wir im Nachhinein nicht mehr überprüfen. Die Patienten wurden von der KV nicht benachrichtigt. Die Unterlagen enthielten auch die Versichertennummer eines Versicherten, ohne dass diese geschwärzt war. Da der Rückschluss von der Versichertennummer auf eine bestimmte Person nicht ohne Weiteres möglich ist und die Informationen im Zusammenhang mit der Versichertennummer keinen Aufschluss über gesundheitliche Aspekte im Detail ergaben, sah die Kassenärztliche Vereinigung keine drohenden schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Versicherten. Eine Benachrichtigung erfolgte dementsprechend nicht. Wir hatten keine Anhaltspunkte, an dieser Gefahrenprognose zu zweifeln.

Wer Schulungsunterlagen im Internet veröffentlicht, muss sicherstellen, dass sie keine personenbezogenen Daten – weder in pseudonymisierter Form noch als Klardatensatz – enthalten oder die personenbezogenen Daten so geschwärzt sind, dass sie nicht wieder sichtbar gemacht werden können.

Datenweitergabe an die Mitglieder eines Ausschusses

Die Senatsverwaltung für Gesundheit und Soziales hat vom Ausschuss für Gesundheit und Soziales des Abgeordnetenhauses den Auftrag erhalten, in einem Bericht darzustellen, wie viele der laufenden Ermittlungsverfahren gegen unseriöse ambulante Pflegedienste privatwirtschaftlich organisierte Dienste betreffen. Hierfür hat die Senatsverwaltung eine Excel-Tabelle erstellt, die die Namen der Pflegedienste enthielt, gegen die ein Ermittlungsverfahren anhängig war. Zusammen mit dem Bericht wurde die nicht anonymisierte Excel-Datei an die Mitglieder des Ausschusses weitergeleitet. Die Senatsverwaltung schrieb daraufhin den Vorsitzenden des Ausschusses an und bat um vertrauliche Behandlung der nicht-anonymisierten Übersicht. Die Pflegedienste waren nach Ansicht der Senatsverwaltung schon deshalb nicht zu benachrichtigen, da dadurch die Strafverfolgung hätte gefährdet werden können.

Die Senatsverwaltung bat uns um Beratung zur Frage der Informationspflicht nach § 18a BlnDSG. Sie stellte insbesondere die unrechtmäßige Kenntniserlangung durch die Abgeordneten in Frage, da diese aufgrund ihrer besonderen Rechtsstellung und des Kontrollrechts gegenüber dem Senat berechtigte Interessen an den Daten haben könnten. Für die Übermittlung von personenbezogenen Daten durch öffentliche Stellen an die Abgeordneten enthält das BlnDSG eine eigene Rechtsgrundlage[285], die diese Weitergabe grundsätzlich von einer Abwägung mit den Interessen der Betroffenen abhängig macht. Diese Einschränkung steht allerdings im Widerspruch zu dem verfassungsrechtlich gewährleisteten Einsichtsrecht der einzelnen Abgeordneten in Akten und sonstige amtliche Unterlagen der Verwaltung, welches wiederum nur versagt werden darf, wenn überwiegende öffentliche Interessen einschließlich des Kernbereichs exekutiver Eigenverantwortung oder überwiegende private Interessen an der Geheimhaltung dies zwingend erfordern.[286] Unter Berücksichtigung dieses weitgehenden verfassungsrechtlichen Informationsanspruches der Abgeordneten wäre auch eine personenbezogene Übermittlung an die Abgeordneten des Fachausschusses grundsätzlich gerechtfertigt gewesen, sodass nicht von der unrechtmäßigen Kenntniserlangung i. S. d. § 18a BlnDSG auszugehen war. Dies teilten wir der Senatsverwaltung mit, wiesen allerdings darauf hin, dass auch die Vernichtung der Liste vom Ausschussvorsitzenden eingefordert werden sollte. Vorliegend war keine namentliche Nennung der Pflegedienste verlangt worden. Die Darstellung der Anteile der Ermittlungsverfahren gegen private ambulante Pflegedienste in anonymisierter Form wäre zur Erfüllung des Berichtsauftrags ausreichend gewesen.

Die Möglichkeit, die Benachrichtigung nach § 18a BlnDSG aus Strafverfolgungsgründen aufzuschieben, betrifft allerdings nur solche Fälle von Strafverfolgung, die infolge des Vorfalls der unrechtmäßigen Kenntniserlangung angestoßen bzw. durchgeführt werden.

Nimmt eine Senatsverwaltung überschüssige personenbezogene Daten in einen Bericht an das Abgeordnetenhaus auf, so muss sie vor dem Hintergrund des Informationsrechts der Abgeordneten prüfen, ob sie zur Benachrichtigung der Betroffenen verpflichtet ist.

285 § 20 Abs. 1 BlnDSG

286 Art. 45 Abs. 2 Satz 1 und 2 VvB; § 20 Abs. 1 BlnDSG ist deshalb verfassungskonform auszulegen.

Veröffentlichung der Mitgliedschaft in der Waffen-SS

In mehreren Zeitungen wurden Artikel zur Mitgliedschaft eines kürzlich verstorbenen Schauspielers in der Waffen-SS veröffentlicht. Die Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen deutschen Wehrmacht (WASt) meldete sich bei uns und teilte mit, dass sie für ein Forschungsprojekt Auskünfte zu den Einheiten des Schauspielers und Dienstzeiten in der Waffen-SS an die anfragende Universität erteilt hatte. Eine Einwilligung der Angehörigen zur Weitergabe dieser Daten lag zu diesem Zeitpunkt nicht vor.

Ob die Angaben durch die Universität bzw. den das Forschungsprojekt leitenden Professor an die Presse weitergegeben wurden, konnte nicht abschließend festgestellt werden. Die WASt hat erläutert, dass sie gegenüber einer anfragenden Zeitung darauf hingewiesen habe, dass die Bestätigung und Veröffentlichung der WASt-Auskunft nur mit Zustimmung der nächsten Angehörigen möglich sei. Gleichwohl sei der Artikel erschienen. Nach Bekanntwerden der Veröffentlichung hatte die WASt umgehend Kontakt mit dem nächsten Angehörigen des Schauspielers aufgenommen und dessen nachträgliche Einwilligung zur Weitergabe der Daten an die Universität erhalten. Im Hinblick auf die Meldepflicht nach § 18a BlnDSG war damit nichts weiter zu veranlassen. Vor dem Hintergrund, dass die WASt nach dem WASt-Datenverarbeitungsgesetz und der WASt-Verordnung nur sehr eingeschränkte Übermittlungsbefugnisse hat, muss nun generell geprüft werden, wie die WASt mit Anfragen von Forschungsinstituten verfährt.[287] Diese Prüfung war im Berichtszeitraum noch nicht abgeschlossen.

Angaben zu Verstorbenen können zugleich personenbezogene Daten von lebenden Angehörigen darstellen, sodass diese als Betroffene nach § 18a BlnDSG bzw. § 42a BDSG zu benachrichtigen sind.

287 Zum Verhältnis des IFG zu den Vorschriften über die WASt siehe 18.3.4

17 Telekommunikation und Medien

17.1 Reform der Bestandsdatenauskunft

Am 1. Juli ist das Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft in Kraft getreten.[288] Die Neuregelung war erforderlich geworden, nachdem das Bundesverfassungsgericht (BVerfG) dem Gesetzgeber aufgegeben hatte, die Regelungen zur Bestandsdatenauskunft im Telekommunikationsgesetz (TKG) bzw. in den Fachgesetzen für die Tätigkeit der Strafverfolgungsbehörden und Geheimdienste so zu verändern, dass sie eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen.[289] Die bestehenden Regelungen dürften insbesondere nicht zur Zuordnung dynamischer IP-Adressen verwendet werden, da es insoweit an einer normenklaren Regelung für solche Eingriffe in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG fehle.

In unserer Stellungnahme zu dem Gesetzentwurf der Bundesregierung[290] zur Reform der Bestandsdatenauskunft haben wir den Senat insbesondere auf Folgendes hingewiesen:

Anders als vom BVerfG in der Entscheidung zur Vorratsdatenspeicherung[291] gefordert, sah der Entwurf eine Erteilung von Auskünften über die zu bestimmten Zeitpunkten einem Nutzer zugewiesenen IP-Adressen zur Verfolgung jedweder Ordnungswidrigkeiten vor. Demgegenüber fordert das BVerfG die Beschränkung solcher Auskünfte auf „(...) auch im Einzelfall (...) besonders gewichtige Ordnungswidrigkeiten (...), die der Gesetzgeber ausdrücklich benennen muss.“ [292] Außerdem schreibt das BVerfG im Falle der Identifizierung von IP-Adressen Benachrichtigungspflichten vor.[293] Auch diese Forderung war in dem Entwurf nicht umgesetzt.

288 BGBl. I, S. 1602
289 Entscheidung vom 24. Januar 2012 – 1 BvR 1299/05, BVerfGE 130, 151
290 BR-Drs. 664/12 vom 2. November 2012
291 Entscheidung vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260
292 Siehe dort Absatz Nr. 262
293 Siehe dort Absatz Nr. 263

Darüber hinaus haben wir den geplanten Wegfall der Bußgeldvorschrift[294] kritisiert, die das Verbot betraf, Zugriffscodes wie PINs an andere als die gesetzlich bestimmten öffentlichen Stellen oder an nicht-öffentliche Stellen zu übermitteln.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit war im weiteren Verlauf des Gesetzgebungsverfahrens als Sachverständiger zu einer Anhörung im Innenausschuss des Deutschen Bundestages geladen und hat dort die o. g. Forderungen bekräftigt. Im Hinblick auf ein mögliches größeres Eingriffsgewicht durch die zukünftig verstärkte Nutzung statischer IP-Adressen – etwa auf Basis des Internet-Protokolls Version 6[295] – hat er darüber hinaus eine Befristung der Regelung des § 112 TKG bis zum 31. Dezember 2014 und dessen unabhängige, wissenschaftliche Evaluation gefordert.

Zwar hat der Gesetzgeber im Gesetzgebungsverfahren einigen der von uns erhobenen Bedenken Rechnung getragen: So sind zumindest für die Nutzung von Bestandsdaten im Zusammenhang mit dynamischen IP-Adressen und für die Nutzung von Daten zum Zugriff auf Endgeräte oder auf Speichereinrichtungen für Zwecke der Strafverfolgung oder durch das Bundesamt für Verfassungsschutz nachträgliche Benachrichtigungen von Betroffenen eingeführt worden. Auch die oben erwähnte Bußgeldvorschrift ist erhalten geblieben. Zur Internet-Protokoll Version 6 und deren Auswirkungen auf Ermittlungsmöglichkeiten und den Schutz der Grundrechte soll die Bundesregierung dem Bundestag zum 31. Dezember 2015 berichten.

Jedoch ließ auch der im Mai dem Bundesrat zugeleitete Gesetzentwurf noch eine Auskunftserteilung über die hinter einer IP-Adresse stehende Person zum Zwecke der Verfolgung von Ordnungswidrigkeiten jedweder Art zu. Wir haben die Senatsverwaltung für Inneres und Sport nochmals auf unsere diesbezüglichen verfassungsrechtlichen Bedenken hingewiesen und auf die Gefahr, dass das Gesetz auch in seiner neuen Fassung mit hoher Wahrscheinlichkeit erneut vom BVerfG aufgehoben wird. Wir haben den Senat deswegen darum gebeten, sich im Bundesrat dafür einzusetzen, dass der Gesetzentwurf dort abgelehnt wird. Dieser Bitte ist er jedoch nicht nachgekommen. Der Gesetzentwurf ist

294 § 149 Abs. 1 Nr. 34 TKG a. F.
295 JB 2011, 12.7

in diesem Punkt unverändert geblieben. Unmittelbar nach Inkrafttreten des Gesetzes wurden erneut Verfassungsbeschwerden gegen die Regelungen zur Bestandsdatenauskunft erhoben. Eine Entscheidung lag bei Redaktionsschluss des Berichts noch nicht vor.

Auch nach der Novellierung der Regelungen zur Bestandsdatenauskunft bleiben Zweifel an der Verfassungsmäßigheit der Nutzung von Daten über Inhaber von dynamischen IP-Adressen zur Verfolgung selbst geringfügiger Ordnungswidrigkeiten.

17.2 Soziale Netzwerke

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Orientierungshilfe „Soziale Netzwerke“ erarbeitet.[296] Sie soll deren Betreiber und die solche Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung dieser Angebote unterstützen. Die Orientierungshilfe enthält neben Erläuterungen zur Datensicherheit und zur Verantwortlichkeit der einzelnen Akteure auch Informationen zu einzelnen Aspekten der rechtlichen Grundlagen. Zusätzlich sind datenschutzfreundliche Ansätze für Bereiche enthalten, in denen der Regulierungsrahmen Schutzlücken in Bezug auf das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist.

In einer Begleitentschließung[297] wies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Betreiber sozialer Netzwerke auf ihre Verpflichtung hin, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Sie hielt darüber hinaus die Weiterentwicklung des vorhandenen Rechtsrahmens zum Schutz der Privatsphäre bei sozialen Netzwerken für notwendig.

296 Orientierungshilfe vom 14. März 2013 (Version 1.1), abrufbar unter www.datenschutz-berlin.de/content/deutschland/konferenz
297 Entschließung vom 13./14. März 2013: Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor, Dokumentenband 2013, S. 15

Diese Forderungen an den Gesetzgeber haben in der Zwischenzeit nochmals an Bedeutung gewonnen, da die Bemühungen der Freiwilligen Selbstkontrolle Multimedia (FSM), mit einigen Betreibern von sozialen Netzwerken aus dem In- und Ausland einen Kodex zur Selbstregulierung ihrer Nutzer zu erarbeiten, unterdessen eingestellt worden sind. Die FSM war auf Initiative des Bundesministeriums des Innern tätig geworden; die beteiligten Unternehmen konnten sich jedoch nicht auf einen solchen gemeinsamen Kodex einigen.[298] Die Beauftragten für Datenschutz und Informationsfreiheit der Länder Berlin und Nordrhein-Westfalen waren an diesem Prozess beteiligt und haben stets betont, dass ein Verhaltenskodex, der hinter den Vorgaben des deutschen Rechts zurückbleibt, nach dem Bundesdatenschutzgesetz nicht hätte anerkannt werden können.

Betreiber sozialer Netzwerke sind verpflichtet, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Die Orientierungshilfe „Soziale Netzwerke" soll sie bei der datenschutzgerechten Gestaltung ihrer Angebote unterstützen.

17.3 Apps auf Smartphones

Nach wie vor kommen in großem Umfang Apps für die verschiedenen Smartphone-Betriebssysteme neu auf den Markt. Über damit zusammenhängende Datenschutzprobleme hatten wir bereits früher berichtet.[299]

Die Art. 29-Datenschutzgruppe hat eine Stellungnahme zu Apps auf intelligenten Endgeräten verabschiedet.[300] Darin erläutert die Gruppe den europäischen Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Entwicklung, Verbreitung und Nutzung von Apps, insbesondere Anforderungen an die Einwilligung, die Grundsätze von Zweckbindung und Datenminimierung sowie Verpflichtungen zu Sicherheitsmaßnahmen und zur Aufklärung von Endnutzern.

298 Siehe den „Closing Report" der FSM vom April, http://www.fsm.de/ueber-uns/veroeffentlichungen/FSM_Closing_Report_SocialCommunities.pdf

299 Zuletzt JB 2012, 16.5

300 Stellungnahme 2/2013 zu Apps auf intelligenten Endgeräten vom 27. Februar 2013 (WP 202), Dokumentenband 2013, S. 47

Auch die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre hat sich mit dem Thema befasst und eine Erklärung verabschiedet.[301] Darin weisen Datenschutzbehörden aus aller Welt auf bestehende Defizite des Schutzes personenbezogener Daten hin und fordern die verschiedenen Akteure (App-Entwickler, aber auch Betreiber von App-Stores und Hersteller von Betriebssystemen) zu deren Beseitigung auf. Die Nutzenden sollen insbesondere – auch innerhalb einer App – vor der Erhebung personenbezogener Daten klare und verständliche Informationen über die beabsichtigte Datenverarbeitung erhalten.

App-Entwickler sollten den Schutz der Privatsphäre bereits zu Beginn der Entwicklung einer App berücksichtigen. Auch Betreiber von App-Stores und Hersteller von Smartphone-Betriebssystemen müssen zur Verbesserung des Schutzes der Privatsphäre beitragen.

17.4 Internet Sweep Day

Im Mai fanden erstmalig international koordinierte Datenschutz-Prüfungen von 1883 Unternehmen am gleichen Tag, dem Internet Sweep Day, statt. An der Prüfaktion beteiligten sich weltweit 18 Datenschutzaufsichtsbehörden. Wir haben ebenfalls teilgenommen und eine Zufallsstichprobe aus großen und kleinen Unternehmen geprüft, darunter einige Startups. Organisiert wurde die Aktion vom Global Privacy Enforcement Network, einem Netzwerk zur internationalen Kooperation der Datenschutzaufsichtsbehörden.

Geprüft wurden die Online-Auftritte und Smartphone-Apps von Unternehmen nach einem einheitlichen Kriterienkatalog. Fokus war dabei die Trans-

301 Erklärung von Warschau zur „Appifikation" der Gesellschaft vom 24. September 2013, Dokumentenband 2013, S. 147

parenz der Datenverarbeitung, d. h. die Information der Betroffenen, die die Webseiten aufrufen. Konkret wurde auf Vorhandensein, Auffindbarkeit, Vollständigkeit und Verständlichkeit der Datenschutzerklärung oder vergleichbarer Hinweise geprüft und darauf, ob eine Kontaktmöglichkeit für Datenschutzfragen angegeben wurde.

International zeigte die Aktion teilweise erschreckende Ergebnisse:

- 21 % der Webangebote hatten überhaupt keine Datenschutzerklärung.
- Ein Teil beschränkte sich auf sehr kurze und allgemeine Aussagen, die keine konkrete Auskunft erteilten, welche Daten zu welchen Zwecken gesammelt werden.
- Ca. 38 % der Datenschutzerklärungen waren schwer verständlich oder zitierten nur einschlägige Ausschnitte aus den jeweiligen Datenschutzgesetzen.
- Smartphone-Apps hatten in über 50 % der Fälle keine oder zumindest keine auf die App bezogene Datenschutzerklärung. Oft wurde einfach nur die für das Webangebot der App-Ansichten vorgesehene Erklärung auch in der App verlinkt, wobei eine App in der Regel weitere oder andere Daten in anderen technischen Verfahren sammelt.

Im Gegensatz zu den internationalen Ergebnissen fiel unsere Prüfung vergleichsweise positiv aus. Nur ein Webangebot hatte eine sehr kurze, wenig aussagekräftige Datenschutzerklärung, was nach Aussage der Firma daran lag, dass man die interaktiven Dienste, die eine Datenerhebung erfordern, gerade erst eingeführt hatte. Mittlerweile ist diese Datenschutzerklärung zufriedenstellend.

Auch bezüglich der anderen Kriterien schnitten die von uns geprüften Angebote relativ gut ab. Kleinere Mängel fanden sich bei ca. 10 % der Webangebote. Die betroffenen Firmen wurden angeschrieben und die Mängel behoben. Dieses Jahr noch nicht geprüft wurde die tatsächliche Datenverarbeitung der einzelnen Unternehmen. Der Sweep Day 2014, an dem wir wieder teilnehmen werden, wird einen anderen Schwerpunkt setzen.

Berliner Unternehmen brauchen den internationalen Vergleich bezüglich der Information der Betroffenen nicht zu scheuen. Weltweit besteht allerdings erheblicher Verbesserungsbedarf.

17.5 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 15.-16. April in Prag und am 2.-3. September in Berlin insgesamt vier Arbeitspapiere verabschiedet:

Das Arbeitspapier zum **Recht auf vertrauliche Telekommunikation**[302] nimmt Bezug auf die bekannt gewordenen Aktivitäten von Nachrichtendiensten[303] und erinnert an die Bedeutung des Telekommunikationsgeheimnisses als Menschenrecht. Die Unterscheidung zwischen nationaler und internationaler Telekommunikation ist heutzutage überholt, da Telekommunikation meist grenzüberschreitend stattfindet. Eine Überwachung der Kommunikation durch staatliche Behörden und insbesondere durch Nachrichtendienste kann für legitime Zwecke notwendig sein, sie muss aber die Ausnahme bleiben. Schon zuvor hatte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit der Bundesregierung vorgeschlagen, sich auf der Ebene der Vereinten Nationen für eine völkerrechtlich verbindliche Regelung zum Schutz der Privatsphäre im digitalen Zeitalter einzusetzen. Auf Vorschlag Deutschlands und anderer Staaten hat die Vollversammlung der Vereinten Nationen im Dezember eine Entschließung verabschiedet, in der sie die Menschenrechtsbeauftragte mit entsprechenden Vorarbeiten betraut.[304]

Das Arbeitspapier zum **Webtracking**[305] beschreibt gängige Methoden der Sammlung, Analyse und Verwendung von Daten über Nutzung von Diensten der Informationsgesellschaft im Internet mit Hilfe von Computern oder anderen Geräten (z. B. Smartphones). Solche Nutzungsdaten werden zunehmend zu verschiedenen Zwecken zusammengeführt und analysiert; diese reichen von wohltätigen bis zu kommerziellen Zwecken der verschiedenen Akteure. Modernes Webtracking ermöglicht, beinahe jeden einzelnen Aspekt des Nutzerverhaltens im gesamten Internet zu beobachten – es birgt das Potenzial für die Erstellung einer vollständigen Übersicht über die Nutzung des Internets

302 Dokumentenband 2013, S. 178
303 Siehe 2.2 und 3.3
304 Dokumentenband 2013, S. 151
305 Arbeitspapier Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar, Dokumentenband 2013, S. 155

einer Einzelperson über potenziell unbegrenzte Zeitspannen. Diese Entwicklung enthält eine beispiellose Gefahr für die Privatsphäre in der Informationsgesellschaft. Die Gruppe gibt Empfehlungen zur Minimierung dieser Gefahren an die verschiedenen Interessenvertreter, die beim Webtracking eine Rolle spielen.

Daraufhin hat sich auch die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre mit dem Thema befasst.[306] Darin fordert die Konferenz wirksame Maßnahmen zur Verbesserung des Schutzes der Privatsphäre der Betroffenen einschließlich der Förderung technischer Standards für eine bessere Nutzerkontrolle (z. B. eines wirksamen Do-Not-Track Standards[307]) und ruft zum Verzicht auf die Nutzung unsichtbarer Trackingelemente zu anderen Zwecken als zur Gewährleistung von Datensicherheit, zur Betrugsaufdeckung oder zum Netzwerkmanagement auf.

Das Arbeitspapier der „Berlin Group“ zum **Datenschutz bei Überwachung aus der Luft**[308] beschreibt Risiken für den Schutz der Privatsphäre, die beim Einsatz von fliegenden Überwachungsplattformen wie Drohnen[309] entstehen können. Hier ist eine angemessene Balance zwischen den Bedürfnissen von Strafverfolgung und öffentlicher Sicherheit auf der einen Seite und den legitimen Interessen der Individuen am Schutz ihrer Privatsphäre auf der anderen Seite sicherzustellen. Die Gruppe empfiehlt, die Überwachung aus der Luft auf spezifische Zwecke zu beschränken (wie die Suche nach vermissten Personen, die Überwachung von Landesgrenzen oder legitime private Zwecke, wie den Zugriff auf Informationen durch Journalisten). Die Öffentlichkeit sollte über Maßnahmen zur Überwachung aus der Luft im größtmöglichen Ausmaß unterrichtet werden. Dies kann z. B. dadurch sichergestellt werden, dass Drohnen Informationen über die für sie verantwortliche Stelle an eine Behörde senden, die diese Informationen in Echtzeit als Open Data veröffentlicht.

In einem weiteren Arbeitspapier weist die Gruppe auf **Risiken für die Privatsphäre durch die Veröffentlichung personenbezogener Daten im Internet** hin.[310] Administratoren von Websites können zum Schutz der Privatsphäre Betroffener beitragen, indem sie die existierenden Möglichkeiten zur Kontrolle der Indexierung solcher Inhalte durch Suchmaschinen anwenden (z. B. durch Nutzung des „robots.txt“-Protokolls oder der Verwendung von speziellen Attributen auf den betreffenden Seiten eines Internet-Angebots). Das Arbeitspapier enthält auch Empfehlungen für Betreiber von Suchmaschinen.

306 Entschließung zu Webtracking und Datenschutz vom 23.-26. September 2013, Dokumentenband 2013, S. 143

307 Siehe hierzu JB 2012, 16.4.1 (S. 174)

308 Dokumentenband 2013, S. 180

309 Siehe 15.1

310 Arbeitspapier und Empfehlungen zu der Veröffentlichung personenbezogener Daten im Web, der Indexierung des Inhalts von Websites und dem Schutz der Privatsphäre, Dokumentenband 2013, S. 168

18 Informationsfreiheit

18.1 Internationale und europäische Informationsfreiheit

Im September haben wir zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die 8. Internationale Konferenz der Informationsfreiheitsbeauftragten – zehn Jahre nach ihrer Gründung in Berlin – ausgerichtet. Auf der dreitägigen Veranstaltung im Plenarsaal des Abgeordnetenhauses diskutierten über 150 Teilnehmende aus 35 Staaten aus Politik, Wissenschaft, Verwaltung und Nicht-Regierungsorganisationen aktuelle Fragen zu Transparenz und Offenheit staatlichen Handelns. In der „Berliner Erklärung" unterstützten die Informationsfreiheitsbeauftragten die Anerkennung der Informationsfreiheit als internationales Grundrecht und hoben die Bedeutung von Art. 19 des Internationalen Pakts über bürgerliche und politische Rechte vom 16. Dezember 1966 hervor.[311] Zudem haben sie empfohlen, dass alle Staaten der Konvention des Europarats über den Zugang zu amtlichen Dokumenten vom 18. Juni 2009 (Tromsø-Konvention) beitreten. Die Bundesrepublik Deutschland gehört zu den Staaten, die der Konvention bisher nicht beigetreten sind. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit betonte, dass auch Geheimdienste nicht pauschal von Transparenzpflichten ausgenommen bleiben dürfen. Effektive Kontrolle von Geheimdiensten setze ein Mindestmaß an Transparenz voraus. Nur so werde es möglich sein, die unter exzessiver Geheimhaltung stattfindende exzessive Überwachung[312] zu begrenzen.

Für mehr Transparenz auf europäischer Ebene hat der EuGH mit einem Urteil gesorgt, das gegen den Rat der Europäischen Union ergangen ist.[313] Danach ist der Rat nicht berechtigt, die Namen von EU-Mitgliedstaaten geheim zu halten, die gewisse Vorschläge im Rahmen von EU-Gesetzgebungsverfahren unterbreitet haben. Im konkreten Fall ging es ausgerechnet um Vorschläge zur Änderung der EU-Verordnung zum Informationszugang. Der Rat hatte die

311 Berliner Erklärung zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013: „Transparenz – der Treibstoff der Demokratie", siehe Dokumentenband 2013, S. 198

312 Siehe 2.2 und 3.3

313 EuGH, Urteil vom 17. Oktober 2013, Az. C-280/11 P

Namen der Mitgliedstaaten in den geänderten Legislativvorschlägen geschwärzt. Die Menschenrechtsorganisation Access Info Europe hat mit Unterstützung des Europäischen Parlaments diesen wichtigen Erfolg errungen, der zu mehr Licht im Dunkelfeld der europäischen Entscheidungsprozesse führen wird. In der Tat ist die Position eines einzelnen EU-Mitgliedstaats in bestimmten europäischen Gesetzgebungsverfahren durchaus von allgemeinem Interesse.

18.2 Informationsfreiheit in Deutschland

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) tagte in diesem Jahr unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, der seit 2013 beide Aufgaben wahrnimmt. Mit einer Entschließung forderte die IFK, die bestehenden Informationsfreiheitsrechte um aktive Veröffentlichungspflichten weiterzuentwickeln.[314] Zur Umsetzung von Open Data – also der proaktiven Veröffentlichung von Informationen durch den Staat im Internet – seien klare gesetzliche Grundlagen im Rahmen der Informationsfreiheitsgesetze erforderlich.[315] Einen Nachbesserungsbedarf hat die IFK auch bei der Veröffentlichung von Hygieneverstößen im Lebensmittelbereich gesehen. Bundesweit hatten Verwaltungsgerichte solche Veröffentlichungen auf dafür eigens vorgesehenen Internetplattformen gestoppt. Hier gilt es, die gesetzliche Grundlage[316] zu überarbeiten und im Dialog mit den Ländern ein einheitliches Transparenzsystem zu schaffen.[317] Angesichts der Entscheidung des Bundesverwaltungsgerichts,[318] nach der die Landespressegesetze keine Verpflichtung von Bundesbehörden zur Auskunftserteilung an Journalisten begründen, sprach sich die IFK für die Schaffung der notwendigen gesetzlichen Grundlage für eine effektive journalistische Recher-

314 Entschließung vom 27. Juni 2013: Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!, siehe Dokumentenband 2013, S. 189

315 Positionspapier vom 27. Juni 2013: Informationsfreiheit und Open Data, siehe Dokumentenband 2013, S. 190

316 § 40 Abs. 1a LFGB

317 Entschließung vom 27. Juni 2013: Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!, siehe Dokumentenband 2013, S. 193

318 Urteil vom 20. Februar 2013, Az. 6 A 2/12

che aus.[319] Schließlich hat die IFK vor dem Hintergrund der Enthüllungen des US-Geheimdienstes NSA[320] die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheits- und Transparenzgesetze als nicht länger hinnehmbar bezeichnet.[321] Dass die Informationsrechte der Menschen in Deutschland in der neuen Legislaturperiode gestärkt werden müssen, hat die IFK ebenfalls gefordert.[322]

18.3 Informationsfreiheit in Berlin

18.3.1 Neu: Fortbildungen an der Verwaltungsakademie

Aufgrund zahlreicher Nachfragen aus der Berliner Verwaltung boten wir erstmals Fortbildungen zum IFG an der Verwaltungsakademie (VAk) Berlin an. Im Rahmen der zwei gut besuchten eintägigen Veranstaltungen im April und September vermittelten wir interessierten Beschäftigten der Berliner Verwaltung die Grundlagen des IFG. Neben einer Einführung in die grundlegende Systematik des IFG wurden detailliert der Umfang des Anspruchs auf Informationszugang, die Reichweite der Ausschlussgründe sowie die Verfahrensvorschriften erläutert. Daneben wurde dargestellt, wie die Gebühren für den Informationszugang im Einzelnen berechnet werden. Dank der zahlreichen Erfahrungen, die wir in unserer Funktion als Schiedsstelle[323] gesammelt haben, konnten wir gezielt auf die immer wiederkehrenden Unsicherheiten und Fehler in der Anwendung des IFG eingehen und praxisgerechte Lösungsvorschläge anbieten. Die Teilnehmenden machten dabei ausgiebig von der Möglichkeit Gebrauch, nicht nur konkrete Nachfragen an uns zu richten, sondern auch untereinander über die „Alltagsprobleme“ bei der Handhabung des IFG zu diskutieren. Im Nachgang zu den Fortbildungen machten sie mehrfach von unserem Angebot Gebrauch, sich bei weiterem Beratungsbedarf zu konkreten Anwendungsproblemen an uns zu wenden. Wegen der weiterhin zunehmenden Nachfrage nach entsprechenden Fortbildungen sowie der überaus positiven Rückmeldungen der Teilnehmenden sind für die Zukunft mindestens drei Fortbildungen im Jahr geplant.

319 Entschließung vom 27. Juni 2013: Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden – auch des Bundes, siehe Dokumentenband 2013, S. 195
320 Siehe 2.2 und 3.3
321 Entschließung vom 27. Juni 2013: Transparenz bei Sicherheitsbehörden, siehe Dokumentenband 2013, S. 194
322 Entschließung vom 28. November 2013: Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!, siehe Dokumentenband 2013, S. 196
323 § 18 IFG

18.3.2 Altes Thema im neuen Gewand: Aktenpläne

Immer wieder hatten wir festgestellt, dass nur wenige Verwaltungen der gesetzlichen Pflicht[324] nachkommen, Aktenpläne zu führen und diese allgemein zugänglich zu machen.[325] Daran konnte auch ein Hinweisschreiben der Senatsverwaltung für Inneres und Sport[326] nichts ändern, das aufgrund einer entsprechenden Aufforderung des Abgeordnetenhauses an die öffentlichen Stellen geschickt worden war.[327] Dass diese gesetzliche Verpflichtung offenbar nicht leicht in den Griff zu bekommen ist, zeigten später mehrere Kleine Anfragen der Piratenfraktion, die sich der Thematik angenommen hat.[328] Die Antworten des Senats offenbarten den wahren Missstand im Hinblick auf fehlende Aktenpläne und die Gründe dafür. Als erfreuliche Folge hat das Abgeordnetenhaus beschlossen, den Senat aufzufordern, einheitliche Richtlinien für das Führen und die öffentliche Zugänglichmachung von Aktenverzeichnissen zu schaffen.[329] Der Senat betrachtete diesen Beschluss mit seinem – bereits vorher herausgegebenen – Rundschreiben[330] und mit dem Hinweis auf das geplante Berliner E-Government-Gesetz[331] als erledigt.[332] Letzteres soll die einheitliche Veröffentlichung aller Aktenpläne über ein zentrales Datenportal sicherstellen.

324 § 17 Abs. 5 IFG
325 Siehe schon JB 2007, 13.2 (S. 230); zuletzt JB 2012, 18.3 (S. 201, 206)
326 Hinweise zur Anwendung des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin vom 24. Februar 2009 (I A 12 – 0201/48), zwischenzeitlich ergänzt durch Rundschreiben I InnSport Nr. 14/2013 vom 5. Juni 2013
327 Plenarprotokoll des Abgeordnetenhauses vom 25. Juni 2009, Anlage 3, S. 4721
328 Drs. 17/10962 vom 12. September 2012, Drs. 17/11312 vom 4. Dezember 2012, Drs. 17/12063 vom 13. Mai 2013
329 Plenarprotokoll vom 29. August 2013, S. 3405
330 Rundschreiben I InnSport Nr. 14/2013 vom 5. Juni 2013
331 Siehe 1.7
332 Mitteilung zur Kenntnisnahme vom 17. Dezember 2013, Drs. 17/1375

18.3.3 Verhältnis des IFG zu grundstücksbezogenen Vorschriften

Wiederholt erreichten uns Anfragen, in welchem Verhältnis das IFG zu grundstücksbezogenen Vorschriften steht. Häufig ging es dabei um die Einsicht in das Baulastenverzeichnis, das Liegenschaftskataster sowie das Grundbuch.

Die Akteneinsicht in das **Baulastenverzeichnis** war ursprünglich in der **Bauordnung für Berlin**[333] geregelt. Danach konnte diejenige Person, die ein berechtigtes Interesse darlegte, in das Baulastenverzeichnis Einsicht nehmen oder sich Abschriften erteilen lassen. Im Rahmen der Neufassung der Bauordnung 2005 hat der Gesetzgeber diese Regelung gestrichen und zur Begründung ausgeführt, dass das IFG ein umfassendes Akteneinsichtsrecht gewährt. Seitdem richtet sich die Einsicht in das Baulastenverzeichnis[334] nur noch nach dem IFG. Dementsprechend sind auch die Gebühren allein nach der für IFG-Fälle geltenden Tarifstelle 1004 des Gebührenverzeichnisses zur Verwaltungsgebührenordnung zu berechnen und insbesondere für Kopien o. Ä. je nach Format nicht mehr als die in Tarifstelle 1001 genannten 4,60 € je Seite. Die Tarifstelle 9.2 des Gebührenverzeichnisses zur Baugebührenordnung für Abschriften je Grundstück i. H. v. 29 € ist nicht mehr anzuwenden.

Der Informationszugang zum **Liegenschaftskataster** richtet sich allein nach dem **Gesetz über das Vermessungswesen in Berlin**.[335] Danach werden auf Antrag bestimmte Angaben aus dem Liegenschaftskataster zur Verfügung gestellt,[336] wobei Eigentümerangaben nur dann herausgegeben werden dürfen, wenn die antragstellende Person ein berechtigtes Interesse darlegt.[337] Demgegenüber ist der Antrag auf Informationszugang nach dem IFG voraussetzungslos und nicht zu begründen, insbesondere muss auch kein Informationsinteresse dargelegt werden. Der Eigentümer eines Grundstücks wäre nach dem IFG in der Regel zu offenbaren.[338] Dadurch würde aber die Regelung im VermGBln unterlaufen, nach der ein berechtigtes Interesse darzulegen ist.

333 § 73 Abs. 5 BauO Bln a. F.
334 § 82 BauO Bln
335 § 17 VermGBln i. d. F. von 2009
336 § 17 Abs. 1 Satz 1 VermGBln
337 § 17 Abs. 1 Satz 2 Nr. 2
338 § 6 Abs. 2 Satz 1 Nr. 1 d) IFG

Die Akteneinsicht in das **Grundbuch** richtet sich allein nach der **Grundbuchordnung**,[339] die dem IFG als bundesrechtliche Spezialvorschrift vorgeht.[340]

18.3.4 Verhältnis des IFG zu den Vorschriften über die WASt

Wir wurden häufig gefragt, ob nach dem IFG Auskunftsansprüche gegen die Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen deutschen Wehrmacht (WASt) bestehen. Das ist nicht der Fall, denn das Gesetz über die WASt (WAStG) von 1993 i. V. m. dem 2. Kapitel (Schutz der Sozialdaten) des SGB X geht als Spezialgesetz dem IFG vor.

Dafür spricht nicht nur der Verweis im WAStG auf das vorgenannte Bundesrecht als Auffangrecht (solche bundesrechtlichen Regelungen gehen dem IFG nach dessen § 17 Abs. 4 vor), sondern auch die Ausgestaltung der „Datenübermittlungsbefugnis an Stellen außerhalb des öffentlichen Bereichs“ in § 6 Abs. 1 WAStVO: Die Anforderungen an das Auskunftsinteresse (glaubhafte Darlegung und Interesse an der Aufklärung des Einzelschicksals) sind höher als nach dem IFG, denn danach spielt das Auskunftsinteresse grundsätzlich keine Rolle. Auch werden die Belange der Betroffenen nach unterschiedlich ausgerichteten Regelbeispielen als nicht schutzwürdig angesehen: Während § 6 Abs. 3 WAStVO einen archivrechtlichen Ansatz hat (u. a. je nachdem, wie lange der Betroffene bereits verstorben ist), knüpft § 6 Abs. 2 IFG an eine bestimmte rechtliche Stellung des Betroffenen (zumeist in Verwaltungsverfahren) an.

Diese Wertungen in den Rechtsvorschriften zur WASt dürfen durch das IFG nicht unterlaufen werden. Selbst wenn dieses anwendbar wäre, dürften nicht mehr als die in 6 Abs. 2 Satz 1 Nr. 1 IFG genannten Daten herausgegeben werden. Dass solche Informationen Gegenstand von Auskunftsbegehren gegen die WASt sind, ist eher unwahrscheinlich.

339 § 12 GBO erfordert hierfür grundsätzlich ein berechtigtes Interesse der antragstellenden Person.
340 § 17 Abs. 4 IFG

18.3.5 Transparenz beim neuen Stadtwerk

Bereits im letzten Jahr haben die Regierungsfraktionen SPD und CDU einen Antrag auf Änderung der Landeshaushaltsordnung in das Parlament eingebracht, mit dem u. a. das Berliner Betriebe-Gesetz geändert werden sollte.[341] Hintergrund war das Bestreben, die Berliner Klimaschutzstrategie und Energiewende durch einen eigenen Energieerzeuger und -vertrieb für erneuerbare Energien umzusetzen und das Stromnetz transparent auszuschreiben. Dieses Ansinnen wurde mit dem im November in Kraft getretenen geänderten Berliner Betriebe-Gesetz realisiert.[342] Nun wird unter der bestehenden Anstalt des öffentlichen Rechts BSR eine gesellschaftsrechtlich selbstständige Tochter, ein Öko-Stadtwerk, gegründet. Im Gesetz erfolgt der ausdrückliche und begrüßenswerte Verweis auf die analoge Geltung des Berliner Informationsfreiheitsgesetzes.[343]

18.4 Einzelfälle

Zähes Ringen mit der Senatsverwaltung für Finanzen

Der Verein Bund der Steuerzahler Berlin bat die Senatsverwaltung für Finanzen um Auskunft zu der Frage, an welchem Datum und in welchem Umfang nach dem Kenntnisstand der Senatsverwaltung im Sport- und Erholungszentrum (SEZ) ein Hallenbad- bzw. Schwimmbetrieb im „baurechtlichen Sinne“ wieder aufgenommen wurde. Hintergrund war, dass ansonsten ein Wiederkaufsrecht des Landes Berlin in Bezug auf das für den symbolischen Kaufpreis von 1 € veräußerte Grundstück bestanden hätte. Die Senatsverwaltung antwortete darauf zunächst, dass der Käufer des SEZ ein Konzept eingereicht und im Dezember 2007 anlässlich einer Objektbesichtigung einen dem Nutzungskonzept entsprechenden Badebereich präsentiert habe.

341 Drs. 17/0705 vom 5. Dezember 2012

342 GVBl., S. 578 und S. 645

343 § 3 Abs. 5 Nr. 3 Berliner Betriebe-Gesetz; der letzte Satz („Das Nähere regelt die Satzung.“) darf nicht zu einer Beschränkung des gesetzlichen Informationszugangsanspruchs führen, sondern nur zu einer Erweiterung (siehe § 3 Abs. 3 IFG).

Wir wiesen die Senatsverwaltung darauf hin, dass der Verein einen Anspruch auf Beantwortung der konkreten Frage anhand aller bei der Senatsverwaltung vorhandenen Akten hat, und baten um Prüfung, ob die Frage nach Aktenlage detaillierter beantwortet werden kann. Die Senatsverwaltung teilte dem Verein daraufhin mit, dass einerseits eine baurechtliche Definition für ein Hallenbad- bzw. Schwimmbetrieb nicht bekannt, andererseits der Kaufvertrag zwischenzeitlich auf der Webseite des SEZ veröffentlicht worden sei. Dem Verein wurde empfohlen, Einsicht in die Dokumente zu nehmen und diese selbst zu bewerten.

Wir erklärten der Senatsverwaltung, dass der Auskunftsanspruch zu der gestellten Tatsachenfrage nicht durch rechtliche Ausführungen erfüllt werden kann, und empfahlen, die Antwort nachzuholen. Die Senatsverwaltung erwiderte, dass unsere Ausführungen nicht nachvollziehbar seien und die Beantwortung der Frage schon deshalb nicht möglich sei, weil es keinen Hallenbad- bzw. Schwimmbetrieb im baurechtlichen Sinne gebe. Der Verein teilte uns hierzu auf Nachfrage mit, dass er den Begriff „Hallenbad- bzw. Schwimmbetrieb im baurechtlichen Sinne“ einer Antwort auf eine Kleine Anfrage aus 2010[344] entnommen habe, in der die Senatsverwaltung selbst erklärt habe, dass zu diesem Zeitpunkt noch kein Hallenbad im baurechtlichen Sinne betrieben werde.

Hiermit konfrontiert erklärte die Senatsverwaltung, dass zunächst eine Rückmeldung der für die Beantwortung der Kleinen Anfrage zuständigen Referentin abgewartet werden müsse, sodann werde man sich erneut an uns wenden. Wir teilten der Senatsverwaltung mit, dass dem Verein zur Beantwortung seiner Frage auch die Auskunft genügen würde, dass sich bezüglich des SEZ seit dieser Antwort kein neuer Sachstand ergeben hat.

Die Senatsverwaltung hat sich trotz mehrfacher Erinnerung fast drei Monate nicht gemeldet. Der Verein musste fristwahrend Klage erheben. Erst im Zuge des Prozesses hat sich die Senatsverwaltung weiter mit der Sache befasst und eine schriftliche Auskunft in Aussicht gestellt. Wir haben darauf gedrungen, diese Auskunft einsehen zu dürfen, bevor sie an das Verwaltungsgericht übersandt wird. Den Gerichtsprozess hätte die Finanzverwaltung sich und der Allgemeinheit buchstäblich ersparen können.

344 Drs. 16/14490 vom 24. Juni 2010, siehe Antwort zu Frage 5

Das IFG gewährt jedem Menschen nach seiner Wahl ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten.[345] Wenn eine konkrete Information in den Akten der öffentlichen Stelle vorhanden ist, kann der Auskunftsanspruch nicht durch Herausgabe von anderen – nicht verlangten – Informationen als erfüllt angesehen werden.

Bevorratung des Grippemedikaments Tamiflu

Der Verein Transparency International Deutschland begehrte bei der Senatsverwaltung für Gesundheit und Soziales Informationszugang zur Bevorratung des Grippemedikaments Tamiflu. Neben verschiedenen Fragen hinsichtlich der Beschaffung, Vernichtung und Wiederbeschaffung der Einzeldosen, der hierfür entstandenen Kosten sowie etwaiger geplanter Bevorratungen im Jahr 2013 bat er um Auskunft über den Lagerort der Einzeldosen sowie um Einsicht in die Kaufverträge mit dem Hersteller. Die Auskünfte wurden ihm auf unser Tätigwerden hin zwar überwiegend gewährt, jedoch wurde die Auskunft über den Lagerort unter Verweis auf die Gefährdung des Gemeinwohls[346] sowie die Einsicht in die Kaufverträge unter Verweis auf den Schutz des behördlichen Entscheidungsprozesses[347] und die Gefährdung des Gemeinwohls[348] verweigert.

Soweit es den Lagerort des Grippemedikaments betraf, teilten wir die Einschätzung der Senatsverwaltung, dass das Arzneimittel vor gezieltem Zugriff oder Fremdeinwirkung geschützt werden muss, um den Einsatz während einer Pandemie oder Epidemie jederzeit zu gewährleisten, und der Lagerort hierzu geheim gehalten werden muss. Die Bewertung der Senatsverwaltung hinsichtlich der Kaufverträge war jedoch unzutreffend. So sprach nichts dafür, dass die vertrauensvolle Zusammenarbeit mit anderen Bundesländern durch die Offenlegung der Verträge überhaupt gefährdet werden könnte. Zum einen hatten bereits der Bund und verschiedene Bundesländer ihrerseits die Kaufverträge offengelegt, zum anderen hatten sich die ablehnenden Bundesländer weit überwiegend auf Vertraulichkeitsvereinbarungen berufen.[349]

345 § 3 Abs. 1 IFG
346 § 11 IFG
347 § 10 Abs. 3 Nr. 2 IFG
348 § 11 IFG
349 Vertraulichkeitsvereinbarungen wären in Berlin nach § 4 Abs. 2 IFG unzulässig.

Dies teilten wir der Senatsverwaltung mit und empfahlen, vor der Entscheidung über den Widerspruch zunächst bei den übrigen Bundesländern nachzufragen, ob aus deren Sicht eine Offenlegung der Verträge überhaupt geeignet wäre, die vertrauensvolle Zusammenarbeit mit dem Land Berlin zu gefährden. Kurz darauf erhielt der Petent die gewünschten Kaufverträge mit der Begründung, dass die anderen Bundesländer keine Einwände gegen die Herausgabe hätten.

Der Informationszugang darf wegen der Gefährdung des Gemeinwohls nur dann abgelehnt werden, wenn die schwerwiegenden Nachteile bzw. Gefährdungen mit einer gewissen Eintrittswahrscheinlichkeit drohen, an die jedoch umso geringere Anforderungen zu stellen sind, je schwerer die möglichen Folgen sind.

Überzogene Gebührenforderung für einen Kontoauszug

Ein Petent begehrte vom Finanzamt für Körperschaften II die Übersendung eines 24-seitigen Kontoauszugs. Nachdem das Finanzamt zunächst die Anwendbarkeit des IFG bestritten hatte, teilte es dem Petenten mit, dass der Kontoauszug nach Zahlung einer Gebühr von 262 € übersandt werde. Auf Nachfrage teilte das Finanzamt dem Petenten Folgendes mit: Der Kontoauszug habe für ihn als Insolvenzverwalter einen außerordentlich hohen Nutzen, da es im Wesentlichen um die Ausforschung von Anfechtungstatbeständen gehe und die Auskunft ihm die Darlegungslast erleichtere. Auch sei der entstandene Verwaltungsaufwand hoch und hindere das Finanzamt an der normalen Aufgabenerfüllung. Schließlich seien die wirtschaftlichen Verhältnisse der Gläubiger und die beabsichtigte Mehrung der Insolvenzmasse durch Anfechtung zu berücksichtigen, die als besonders hoch einzuschätzen seien.

Wir wiesen das Finanzamt darauf hin, dass es sich bei dem Ausdruck eines einzelnen Kontoauszugs in jedem Fall nur um einen einfachen Fall der Aktenauskunft handelt und der Gebührenrahmen daher von 5 bis 100 € reicht.[350] Auch knüpfen die maßgeblichen Tarifstellen für Informationszugang tatbestandlich

350 Tarifstelle 1004 a) Nr. 2 des Gebührenverzeichnisses zur VGebO

an den entstandenen Verwaltungsaufwand an, sodass nur dieser im Rahmen der Gebührenermittlung zugrunde gelegt werden darf.[351] Allenfalls dürfen die wirtschaftlichen Verhältnisse[352] des Antragstellers (zu dessen Gunsten) berücksichtigt werden, nicht der wirtschaftliche Nutzen[353] (zu seinen Lasten). Schließlich darf eine Gebühr in keinem Missverhältnis zur öffentlichen Leistung stehen. Bei der Gebührenerhebung gilt der Grundsatz des staatlichen Gewinnerzielungsverbots.

Das Finanzamt reduzierte daraufhin die Gebühr zwar auf 112 €, blieb jedoch bei der irrigen Auffassung, dass die wirtschaftlichen Verhältnisse und der wirtschaftliche Nutzen zum Nachteil des Petenten zu berücksichtigen seien. Wir stellten dem Petenten daher den Schriftwechsel mit dem Finanzamt als Argumentationshilfe für eine mögliche Klage beim Verwaltungsgericht zur Verfügung.

Bei der Bemessung der Gebühren für Informationszugang darf nur der tatsächlich entstandene Verwaltungsaufwand berücksichtigt werden. Allenfalls dürfen die wirtschaftlichen Verhältnisse der antragstellenden Person zu deren Gunsten berücksichtigt werden.

Starrsinn bei der Apothekerkammer

Ein Petent begehrte bei der Apothekerkammer Akteneinsicht in verschiedene Vorgänge zu Rezeptfälschungen, Beschwerden sowie Arzneimittelrückrufen der Arzneimittelkommission der Deutschen Apotheker. Die Apothekerkammer teilte dem Petenten mit, dass für die Akteneinsicht eine Gebühr i. H. v. 227,40 € im Voraus zu entrichten sei und er die gewünschten Unterlagen nach Eingang der Gebühr erhalten werde.

Die Gebührenhöhe war nicht zu beanstanden und wurde von der Apothekerkammer auch nachvollziehbar begründet. Zur Vorauszahlung der vermutlich entstehenden Gebühr[354] baten wir die Apothekerkammer um Stellungnahme und wiesen darauf hin, dass die generelle Entscheidung, dass immer eine Vorauszahlung erfolgen müsse, ermessensfehlerhaft und damit rechtswidrig ist.[355] Die Apothekerkammer meinte, dass die Verwaltung so ein effizientes Gebührenmanagement sicherstellen würde und dies in allen Bereichen der Verwaltung gängige Praxis sei. Bei dem Grundprinzip der Gebührenvorauszahlung handle es sich um eine antizipierte Ermessensentscheidung, von der nur in begründeten Fällen abgewichen werde. Dem Petenten stehe es frei, den Rechtsweg zu beschreiten.

Wir erklärten der Apothekerkammer, dass die umgekehrte Rechtsauffassung zutreffe: Die Festsetzung der Vorauszahlung komme nur in begründeten Ausnahmefällen in Betracht, etwa bei Anhaltspunkten, dass die antragstellende Person die Gebühr nicht, nicht vollständig oder nicht rechtzeitig entrichten wird. Da die Apothekerkammer an ihrer Auffassung festhielt, stellten wir dem Petenten unseren Schriftwechsel mit der Apothekerkammer als Argumentationshilfe für eine mögliche Klage beim Verwaltungsgericht zur Verfügung.

Die Vorauszahlung einer vermutlich entstehenden Gebühr darf nur ausnahmsweise verlangt werden. Generell so vorzugehen, ist ermessensfehlerhaft und damit rechtswidrig.

Langwierige Aktenauskunft bei der Humboldt-Universität

Ein Petent begehrte von der Humboldt-Universität Auskunft zu einer Vielzahl von Fragestellungen zum Studiengang Gender Studies. Die Universität stellte die Beantwortung einiger Fragen in Aussicht, lehnte die Beantwortung der übrigen Fragen jedoch ab. Zur Begründung führte sie aus, dass die Beantwortung der Fragen eine Wertung erfordern würde und diese daher nicht nach dem Akteninhalt beantwortet werden könnten. Auch habe der Petent seine wissenschaftlichen Qualifikationen nicht nachgewiesen, und angesichts seines Wohnorts in Bayern seien Zweifel angebracht, welche Teilhabe er geltend machen wolle in Angelegenheiten, die nach der Kompetenzordnung des Grundgesetzes Sache der Bundesländer seien.

351 § 5 Nr. 2 VGebO
352 § 5 Nr. 3 VGebO
353 § 5 Nr. 1 VGebO
354 § 17 GebBeitrG
355 § 40 VwVfG i.V. m. § 1 Abs. 1 VwVfG Bln

Unsere Prüfung ergab, dass die meisten Fragen tatsächlich nicht nach dem IFG zu beantworten waren, da sie sich nicht auf konkrete Akteninhalte bezogen, sondern Wertungen und Beurteilungen der Universität verlangten. Diese teilte uns mit, dass die in Aussicht gestellten Antworten noch nicht gegeben worden seien, da noch nicht alle benötigten Informationen vorlägen. Wir empfahlen daher, die Beantwortung „abzuschichten" und dem Petenten die bereits vorhandenen Informationen zur Verfügung zu stellen, woraufhin die Universität von den zu beantwortenden Fragen alle bis auf zwei beantwortete.

Zwei Monate später wandte sich der Petent erneut an uns, da er immer noch keine Antwort erhalten hatte. Erst auf mehrmalige Nachfrage unsererseits wurde dem Petenten weitere drei Monate später eine der beiden offenen Fragen beantwortet. Zu der verbleibenden Frage wurde ihm mitgeteilt, dass zunächst die Zustimmung des Bundesministeriums für Familie, Senioren, Frauen und Jugend eingeholt werden müsse.[356] Die noch offenen Fragen wurden daraufhin fast weitere vier Monate später endlich so weit beantwortet, wie dies aufgrund der eingeschränkten Zustimmung möglich war.

Zwar wurden die nach dem IFG zu beantwortenden Fragen schließlich in dem erforderlichen Umfang beantwortet. Zwischen der ursprünglichen Antragstellung und der Beantwortung der letzten noch offenen Fragen lag jedoch ein Zeitraum von insgesamt acht Monaten.

Über Anträge auf Informationszugang ist unverzüglich[357] zu entscheiden, also ohne schuldhaftes Zögern.[358] Soweit die öffentliche Stelle den Antrag zurückweisen will, ist der Antragsteller innerhalb von zwei Wochen nach Antragstellung zu bescheiden.[359] Überlange Verfahrensdauern von mehreren Monaten sind grundsätzlich nicht hinnehmbar.

356 § 10 Abs. 3 Nr. 2 IFG
357 § 14 Abs. 1 Satz 1 IFG
358 § 121 Abs. 1 BGB
359 § 15 Abs. 5 IFG

Erwerb der Bundesligarechte durch die ARD

Ein Petent begehrte vom RBB Einsicht in die Verträge über den Erwerb der Bundesligarechte durch die ARD. Der RBB lehnte die Herausgabe ab und führte zur Begründung aus, dass der RBB zwar grundsätzlich dem IFG unterliege, soweit er hoheitlich tätig werde, das IFG jedoch keine Anwendung auf den journalistisch-redaktionellen Bereich finde, zu dem auch der Erwerb von Sendelizenzen und Übertragungsrechten gehöre.

Der RBB durfte die Einsicht in die Verträge zu Recht ablehnen. Zwar handelt es sich bei dem RBB um eine Anstalt des öffentlichen Rechts, die grundsätzlich – und nicht nur bei hoheitlicher Tätigkeit – dem IFG unterliegt.[360] Der konkrete Anwendungsbereich des IFG muss jedoch durch eine verfassungskonforme Auslegung ermittelt werden, da Rundfunkanstalten durch die verfassungsrechtlich garantierte Rundfunkfreiheit[361] vor jedem fremden Einfluss auf Auswahl, Inhalt und Gestaltung der Programme geschützt sind. Es würde daher einen unzulässigen Eingriff in die Rundfunkfreiheit darstellen, wenn der RBB Informationszugang zu Akten gewähren müsste, die dem geschützten journalistisch-redaktionellen Bereich unterfallen. Der Erwerb von Sendelizenzen und Übertragungsrechten steht jedoch in unmittelbarem Zusammenhang mit der Erfüllung der Programmgestaltung und -produktion und ist demnach dem geschützten journalistisch-redaktionellen Bereich zuzurechnen.

Akten von Rundfunkanstalten unterliegen dem Informationszugangsanspruch nur, soweit sie in keinem inhaltlichen Zusammenhang mit der Erfüllung der Programmgestaltung und -produktion stehen und deren Offenbarung ohne Gefährdung der Programmfreiheit möglich ist.

360 § 2 Abs. 1 Satz 1 IFG; zum diesbezüglichen Streit mit dem RBB siehe JB 2010, 14.1
361 Art. 5 GG

Nachhilfe zu Umweltinformationen

Ein Petent begehrte beim Bezirksamt Marzahn-Hellersdorf Einsicht in die Vorgänge bezüglich der Fällung verschiedener geschützter Bäume. Das Bezirksamt teilte ihm mit, dass die Grundstückseigentümerin eine Ausnahmegenehmigung erhalten habe, die Fällung mithin rechtmäßig erfolgt sei. Im Übrigen teilte man ihm nur mit, dass er kein auf verfahrensrechtliche Vorschriften gestütztes Informationsrecht habe. Allenfalls käme eine Auskunft nach dem Umweltinformationsgesetz in Betracht, wobei er hiernach nur einen Informationsanspruch zu den objektiven Informationen hinsichtlich Anzahl und Art der Ersatzpflanzungen habe.

Diese Rechtsauffassung findet im Gesetz keine Stütze. Vielmehr hat jeder Mensch nach Maßgabe des UIG Anspruch auf freien Zugang zu Umweltinformationen,[362] über die die informationspflichtige Stelle verfügt.[363] Wir baten das Bezirksamt daher, dem Petenten die gewünschte Akteneinsicht zu ermöglichen. Vorsichtshalber wiesen wir darauf hin, dass selbst bei Vorliegen von Ablehnungsgründen nach dem UIG andere Ansprüche auf Informationszugang unberührt bleiben[364] und daher gegebenenfalls auch Ansprüche nach dem IFG zu prüfen sind – selbst wenn der Petent sich ausdrücklich auf das UIG berufen hat. Schließlich machten wir deutlich, dass für die Akteneinsicht in Umweltinformationen vor Ort keine Gebühren erhoben werden dürfen.[365] Das Bezirksamt folgte unserer Empfehlung und ermöglichte dem Petenten die gebührenfreie Akteneinsicht in die gewünschten Vorgänge.

Jeder Mensch hat wahlweise Anspruch auf Einsicht in oder Auskunft über die Umweltinformationen, die bei einer öffentlichen Stelle vorhanden sind. Umweltinformationen können vor Ort gebührenfrei eingesehen werden.

362 § 2 Abs. 3 UIG
363 § 3 Abs. 1 UIG i.V. m. § 18a Abs. 1 IFG
364 § 3 Abs. 1 Satz 2 UIG
365 § 18a Abs. 4 Nr. 1 IFG

Massive Probleme beim Bezirksamt Neukölln

Ein Petent begehrte vom Bezirksamt Neukölln Auskunft über die dort sowie beim Bezirksbürgermeister in einem bestimmten Zeitraum geführten medienrechtlichen Gerichtsverfahren. Das Bezirksamt teilte mit, dass es keinen Anspruch auf diese Auskunft gebe und das IFG keine personenbezogene Kontrolle aller Staatsorgane bezwecke. Zudem forderte das Bezirksamt den Petenten auf, das Auskunftsbegehren zu begründen, woraufhin dieser mitteilte, die Informationen für einen Aufsatz zu benötigen. Sodann erteilte es eine auf 2011 beschränkte Teilauskunft und stellte ihm gestützt auf das Gebühren- und Auslagenverzeichnis zur Informationsgebührenverordnung des Bundes pro Einzelfall eine Gebühr von bis zu 500 € in Aussicht. Abschließend wies das Bezirksamt darauf hin, dass das Recht auf Akteneinsicht oder Aktenauskunft nicht bestehe, soweit sich Akten auf die Beratung der Bezirksämter sowie deren Vorbereitung beziehen.[366] Sodann lehnte es die Auskunft hinsichtlich des übrigen Zeitraums ab und führte zur Begründung aus, dass der Petent einerseits überwiegend Privatinteressen verfolgen würde;[367] andererseits stehe der Auskunft die Verhältnismäßigkeit entgegen, zumal der Verwaltungsaufwand übermäßig und durch das Informationsinteresse nicht mehr gerechtfertigt sei. Das Bezirksamt erließ daraufhin einen Gebührenbescheid i. H. v. 250 € und stellte dem Petenten die gewünschten Auskünfte nach Entrichtung der Gebühr in Aussicht. Nach Bezahlung der Gebühr erhielt er die knappe Auskunft, dass das Bezirksamt im Zeitraum von 2006 bis 2010 insgesamt drei Verfahren mit presserechtlichem Hintergrund geführt habe.

Aufgrund der Vielzahl von Rechtsfehlern wandten wir uns in dieser Angelegenheit direkt an den Bezirksbürgermeister. Wir wiesen ihn darauf hin, dass eine Einschränkung des Rechts auf Informationszugang durch Heranziehung des Gesetzeszwecks[368] nicht in Betracht kommt und der Anspruch nach dem IFG voraussetzungslos ist und nicht begründet werden muss. Auch beziehe sich der Schutzbereich des behördlichen Entscheidungsprozesses bezüglich der Beratung des Bezirksamts[369] nur auf den absoluten Kernbereich exekutiver Eigenverantwortung, worunter keinesfalls die vom Bezirksamt bzw. vom

366 § 10 Abs. 3 Nr.1 IFG
367 § 6 Abs. 1 IFG
368 § 1 IFG
369 § 10 Abs. 3 Nr. 1 IFG

Bezirksbürgermeister geführten presserechtlichen Verfahren zählen. Die Verfolgung von Privatinteressen stünde dem Auskunftsanspruch nicht entgegen,[370] da das Informationsinteresse des Petenten Bestandteil des Informationsinteresses der Allgemeinheit[371] ist und der Informationszugangsanspruch nach dem IFG nicht durch analoge Anwendung von bundesrechtlichen Datenschutzvorschriften eingeschränkt bzw. ausgeschlossen werden kann. Auch die Gebührenberechnung für Informationszugang richte sich nicht nach bundesrechtlichen Bestimmungen, sondern nach dem Gebührenverzeichnis zur Berliner Verwaltungsgebührenordnung. Daneben wiesen wir darauf hin, dass es ausweislich der erteilten Auskünfte insgesamt nur um zehn Verfahren ging und es sich somit um einen Fall der einfachen Aktenauskunft handelt, deren Gebührenrahmen von 5 bis 100 € reicht.[372] Schließlich war zweifelhaft, ob überhaupt Gebühren nach der Tarifstelle für Informationszugang nach dem IFG erhoben werden dürfen, wenn das Bezirksamt zugleich die grundsätzliche Anwendbarkeit des IFG bestreitet. Wir baten daher darum, den Gebührenbescheid unter Beachtung dieser Rechtslage erneut zu überprüfen. Das Bezirksamt teilte bis zuletzt in keiner Hinsicht unsere Auffassungen. Damit steht zu befürchten, dass in Neukölln auch künftig eindeutig rechtswidrige IFG-Bescheide erlassen werden.

Eine derart breite Unkenntnis des Berliner Informationsfreiheitsrechts lässt keinen anderen Schluss zu als den auf einen massiven Fortbildungsbedarf[373].

370 Nach § 6 Abs. 1 IFG könnte die Verfolgung von Privatinteressen ohnehin nur der Offenbarung personenbezogener Daten entgegenstehen, nicht jedoch den Informationszugang in Gänze ausschließen.

371 § 1 IFG

372 Tarifstelle 1004 a) Nr. 2 des Gebührenverzeichnisses zur VGebO

373 Siehe 18.3.1

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

Eine Bürgerin bat um Unterstützung, da sie durch ein Gesundheitsamt aufgefordert worden war, das **Impfbuch** ihres Kindes in der Schule vorzulegen, ohne dass sie in dem Anschreiben auf die Freiwilligkeit hingewiesen worden war. Da sowohl die Impfbucheinsicht als auch die Impfung selbst freiwillig sind,[374] konnten wir beim Gesundheitsamt erreichen, dass das Elternanschreiben entsprechend geändert und nun deutlich auf die Freiwilligkeit der Impfbuchvorlage hingewiesen wird.

Ein Vater wies uns zum zweiten Mal darauf hin, dass im Rahmen eines von einem Jugendhilfeträger für Schulkinder angebotenen Bildungsangebots eine Vielzahl personenbezogener **Daten über** die **Minderjährigen** erhoben wurde. Den Sinn dieser Datenerhebung konnte der Vater nicht erkennen. Der Veranstalter gab an, dies sei notwendig, da das Projekt durch den Europäischen Sozialfonds (ESF) gefördert werde und die Förderbedingungen ihn dazu verpflichteten. Bereits in einem ähnlichen Fall hatten wir vor zwei Jahren die für ESF-Förderungen zuständige Senatsverwaltung für Wirtschaft, Technologie und Forschung darauf hingewiesen, dass die Datenerhebung unzulässig ist. Die Förderbedingungen für derartige Kinderveranstaltungen lassen eine anonyme Teilnahme ausdrücklich zu. Die Senatsverwaltung hatte uns daraufhin versichert, dass sich der Fehler nicht wiederholen werde. Leider stellte sich heraus, dass dies nicht der Fall war. Auf unsere Intervention hat die Senatsverwaltung nunmehr entsprechende Hinweise in die Handbücher und Unterlagen für die Beantragung aufgenommen und die an den Projekten beteiligten Stellen ebenfalls informiert. Wir hoffen, dass das Problem nun tatsächlich nicht mehr auftreten wird.

Ein Bürger beschwerte sich bei uns darüber, dass in einem Kino beim Kauf einer Eintrittskarte unter Vorlage des **Schwerbehindertenausweises** Inhaber-

374 JB 2011, 7.2.7

name und Nummer des Ausweises von den Beschäftigten an der Kasse notiert werden, wenn eine Begleitperson freien Eintritt erhalten soll. Der Kinobetreiber rechtfertigte dies damit, einen möglichen Missbrauch der Regelung zum freien Eintritt durch Beschäftigte vorzubeugen. Wir wiesen den Betreiber darauf hin, dass eine solche Datenverarbeitung ohne Einwilligung der Betroffenen unzulässig ist, und konnten erreichen, dass ab sofort bei Gewährung des freien Eintritts für eine Begleitperson keine Daten der Inhaberin oder des Inhabers des Schwerbehindertenausweises mehr notiert werden.

Eine Bürgerin war an uns mit dem Hinweis herangetreten, sie habe das Referat Verkehrsordnungswidrigkeiten und Bußgeldeinziehung beim Polizeipräsidenten mehrfach vergeblich gebeten, ihr das **Frontfoto**, dass der Behörde **zu Beweiszwecken für eine Ordnungswidrigkeit** diente, zuzusenden, da sie zurzeit gesundheitlich nicht in der Lage sei, das Foto bei der Behörde vor Ort einzusehen. Wir haben die Polizei gebeten, in diesem konkreten Fall, insbesondere mit Rücksicht auf die gesundheitliche Verfassung der Petentin, ausnahmsweise das gewünschte Foto zu übersenden, auch wenn ein Rechtsanspruch nicht besteht. Daraufhin hat sich die Polizei „allein zur schnellen und endgültigen Erledigung der Angelegenheit ohne Anerkennung einer Rechtspflicht“ bereit erklärt, der Petentin das gewünschte Foto zu schicken.

Ein Petent begehrte von der Senatsverwaltung für Finanzen Einsicht in das **Shareholders‘ Agreement zwischen Veolia und RWE** im Zusammenhang mit der Rekommunalisierung der Berliner Wasserbetriebe. Die Senatsverwaltung lehnte dies ab, da sie einerseits nicht Vertragspartner des Shareholders‘ Agreement und daher nicht zuständig sei, andererseits der Herausgabe ohnehin Betriebs- bzw. Geschäftsgeheimnisse[375] entgegenstünden. Wir wiesen die Senatsverwaltung darauf hin, dass das Land Berlin im Zuge des Rekommunalisierungsvertrages zumindest beabsichtigt hatte, in das Shareholders‘ Agreement einzutreten, und dieses daher jedenfalls zu diesem Zeitpunkt amtlichen Zwecken diente.[376] Zu den Betriebs- bzw. Geschäftsgeheimnissen hoben wir hervor, dass eine Abwägung mit dem Informationsinteresse der Allgemeinheit vorzunehmen ist,[377] das hier aufgrund der besonderen Materie des Shareholders‘ Agreement das schutzwürdige Interesse der betroffenen Vertragspartner an der Geheimhaltung überwiegt. Die Senatsverwaltung veröffentlichte daraufhin das Shareholders‘ Agreement in der englischen Originalfassung nebst deutscher Übersetzung im Internet.

375 § 7 IFG
376 § 3 Abs. 2 IFG
377 § 1 IFG

Ein Petent begehrte vom Bezirksamt Marzahn-Hellersdorf Akteneinsicht in verschiedene **Grundstückskaufverträge**. Das Bezirksamt lehnte dies ab, da solche Verträge nach dem Sachenrechtsbereinigungsgesetz nicht in den Anwendungsbereich des IFG fielen und das Handeln des Facility Managements auf Fiskalprivatrecht fuße. Wir wiesen das Bezirksamt darauf hin, dass das IFG nicht nur für die Verwaltungstätigkeit, sondern für die gesamte Tätigkeit des Bezirksamts gilt[378] und auch auf Grundstückskaufverträge anwendbar ist.[379] Das Bezirksamt wollte daraufhin zunächst eine Stellungnahme des Rechtsamts einholen. Als auch nach der zweiten eingeräumten Fristverlängerung noch keine Stellungnahme vorlag, wandten wir uns ausnahmsweise selbst an das Rechtsamt, das erklärte, dass eine Prüfbitte dort nicht vorliege. Es stellte sich heraus, dass der Vorgang versehentlich liegengeblieben und nicht an das Rechtsamt weitergeleitet worden war. Nach Übersendung des Vorgangs schloss sich das Rechtsamt unserer Auffassung an. Durch unsere Initiative wurde der Aktengang im Bezirksamt neu angestoßen und dem Petenten letztlich zu seinem Recht verholfen.

378 § 2 Abs. 1 IFG
379 § 3 Abs. 2 IFG

20 Aus der Dienststelle

20.1 Zusammenarbeit mit dem Abgeordnetenhaus

Der Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit hat den Jahresbericht 2011 und die Stellungnahme des Senats[380] beraten. Allerdings konnten diese Beratungen bis zum Jahresende noch nicht abgeschlossen werden. Für das kommende Jahr ist ein zusammenfassender Antrag geplant, der in das Plenum des Abgeordnetenhauses eingebracht werden soll. Darüber hinaus hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit im Ausschuss für Inneres, Sicherheit und Ordnung zur Schaffung einer Rechtsgrundlage für die Anfertigung von Übersichtsaufnahmen bei Demonstrationen Stellung genommen.[381]

20.2 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 13./14. März in Bremerhaven und am 1./2. Oktober in Bremen unter dem Vorsitz der Bremischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[382] Für 2014 hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz in der Konferenz übernommen.

Der **Düsseldorfer Kreis**, in dem unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich** zusammenarbeiten, fasste zwei Beschlüsse zur Videoüberwachung in und an Taxis und zur Datenübermittlung in Drittstaaten.[383]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 27. Juni und 28. November unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Erfurt und fasste mehrere Entschließungen zu aktuellen Fragen des Informationszugangs und der Transparenz.[384] 2014 wird der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auch diese Konferenz leiten.

Die **Arbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie**, in der Berlin traditionell die Bundesländer i.A. der deutschen Datenschutzbehörden vertritt, beteiligte sich erneut intensiv an der Debatte über den neuen europäischen Rechtsrahmen für den Datenschutz. Darüber hinaus hat die Gruppe Stellungnahmen u. a. zu Apps auf Smartphones, zu verbindlichen Unternehmensregelungen für Auftragsverarbeiter und zu intelligenten Grenzen („Smartborders“) verfasst, die z.T. in unserem Dokumentenband abgedruckt sind.[385]

Auf Einladung des polnischen Datenschutzbeauftragten fand die **35. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre** vom 23.-26. September in Warschau statt, die sich mit zentralen Fragen des Datenschutzes in der Informationsgesellschaft wie der Transparenz bei der Datenverarbeitung auch durch Nachrichtendienste, der Profilbildung, der „Appifikation“ der Gesellschaft, den notwendigen digitalen Bildungsangeboten und der Verankerung des Datenschutzes in internationalen Konventionen befassten.[386] Die Internationale Konferenz griff in einer weiteren Entschließung das Thema „Webtracking“ auf, das bereits die **Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)** bei ihrer Sitzung in Prag am 15.-16. April zum Gegenstand eines Arbeitspapiers gemacht hatte. Diese Arbeitsgruppe tagte erneut am 2.-3. September in Berlin und verabschiedete weitere Arbeitspapiere zur Luftüberwachung durch Drohnen und zum Recht auf vertrauliche Telekommunikation.[387]

Gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veranstalteten wir vom 18.-20. September die **8. Internationale Konferenz der Informationsfreiheitsbeauftragten**[388] im Abgeordnetenhaus von Berlin. Diese Konferenz war 2003 in der Bundeshauptstadt vom damali-

380 Abghs.-Drs. 17/0435
381 Siehe 3.5
382 Dokumentenband 2013, S. 10 ff.
383 Dokumentenband 2013, S. 26 ff.
384 Dokumentenband 2013, S. 189 ff.
385 Dokumentenband 2013, S. 35 ff.
386 Dokumentenband 2013, S. 133 ff.
387 Siehe 17.5, Dokumentenband 2013, S. 155 ff.
388 Siehe 18.1

gen Berliner Beauftragten für Datenschutz und Informationsfreiheit ins Leben gerufen worden.

Erneut erhielten wir Besuch von mehreren ausländischen Delegationen, die mit uns über praktische Fragen der Datenschutzkontrolle und des Informationszugangs diskutierten. Dazu gehörten Experten aus den Golfstaaten, Moldawien, der Schweiz und Usbekistan.

20.3 Öffentlichkeitsarbeit

Am 28. Januar fand auf Einladung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema „Eine Datenschutz-Grundverordnung für Europa – internationale Perspektiven" eine zentrale Veranstaltung in der Jerusalemkirche in Berlin aus Anlass des 7. Europäischen Datenschutztages statt.

Vom 16.-18. April wurde im FEZ-Berlin eine Projektwoche für Grundschüler „Sicher surfen im Internet" durchgeführt. Während dieser Projektwoche gestalteten wir am 17. April einen Workshop zum Thema „Datenschutz in sozialen Netzwerken und Chatrooms".

Im Rahmen der Vorlesungsreihe der KinderUni Lichtenberg (KUL) und der mobilen Lichtenberger KinderUni „KUL *unterwegs*" bieten wir regelmäßige Vorlesungen zum Thema „Soziale Netzwerke und Datenschutz" für Kinder ab acht Jahren an. So wurden im August zwei Klassen der Fritz-Reuter-Oberschule über den Datenschutz bei „Facebook, Twitter, Myspace & Co." informiert. Auch interessierte Eltern wurden geschult: Sie konnten im November unter dem Titel „‚Meine Freunde sind drin – Ich will das auch!' Kinder und Jugendliche in sozialen Netzwerken – Ratschläge für Eltern" einen Vortrag zu den Gefahren und Chancen sozialer Netzwerke besuchen.

Berlin, den 2. April 2014

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Anhang

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 12. September 2013 im Abgeordnetenhaus von Berlin zum Jahresbericht 2012

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren,

Ihnen liegen der Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2012 und die Stellungnahme des Senats hierzu vor.

Die ständig zunehmende Bedeutung des Datenschutzes wird jedem überdeutlich, der morgens die Zeitung aufschlägt. Auch der Regierende Bürgermeister hat hierauf bei der Eröffnung der Internationalen Funkausstellung 2013 hingewiesen.

Der Jahresbericht 2012 konzentriert sich einerseits auf Entwicklungen in Berlin, behandelt aber auch europäische und internationale Fragen, denen sich die Bundeshauptstadt gerade in einer vernetzten Welt stellen muss.

Unsere 2012 durchgeführte Prüfung der flächendeckenden **Funkzellenüberwachung** ist in diesem Haus bereits erörtert worden. Allerdings spricht der Senat in seiner Stellungnahme dem Datenschutzbeauftragten die Kompetenz dafür ab, die Maßnahmen der Staatsanwaltschaft vor einer gerichtlichen Anordnung zu bewerten. Dabei verkennt er, dass die Strafverfolgungsbehörden sich einer datenschutzrechtlichen Kontrolle der Funkzellenabfragen nicht unter Hinweis auf die Unabhängigkeit der Gerichte entziehen können. Wo kein Kläger, da kein Richter: gerade weil häufig Betroffene nicht – wie im Prinzip vorgeschrieben – benachrichtigt werden, ist eine unabhängige Kontrolle durch den Datenschutzbeauftragten im Interesse des Grundrechtsschutzes der betroffenen, meist unverdächtigen Personen zwingend geboten. Zugleich begrüße ich es, dass dieses Haus auf Empfehlung des **Ausschusses für Digitale Verwal-**

tung, Datenschutz und Informationsfreiheit den Senat aufgefordert hat, sich im Bundesrat für eine Beschränkung der Funkzellenabfragen auf das erforderliche Maß einzusetzen und darüber hinaus zu prüfen, ob die Öffentlichkeit über Funkzellenabfragen unterrichtet werden kann.

Auch in zwei weiteren Punkten besteht ein Dissens zwischen dem Datenschutzbeauftragten und der Landesregierung: 1988 hatte das Abgeordnetenhaus den Senat aufgefordert, im polizeilichen Informationssystem auf bestimmte **personengebundene Hinweise** wie „GEISTESKRANK“ und „ANSTECKUNGSGEFAHR“ zu verzichten, weil diese Merkmale dazu führen, dass Betroffene leicht abgestempelt werden. Der Senat ist dieser Forderung des Parlaments seinerzeit gefolgt. Auf den Beschluss der Innenministerkonferenz hin hat er allerdings im vergangenen Jahr der Polizei die Verwendung dieser personenbezogenen Hinweise wieder gestattet, ohne dem Parlament zu erläutern, weshalb dafür inzwischen (nach 24 Jahren !) ein zwingendes Erfordernis besteht.

In Sachen Informationsfreiheit erklärt der Senat in seiner Stellungnahme zwar einerseits, ein **Transparenzgesetz** sei in Berlin nicht erforderlich, weil das Informationsfreiheitsgesetz eines der informationsfreundlichsten Gesetze in Deutschland sei. Andererseits lehnt es der **Senat** nach wie vor ab, die **pauschale Geheimhaltung seiner Beschlüsse** aufzuheben. Dazu bleibt festzuhalten: In puncto Transparenz gerät Berlin z.B. gegenüber Hamburg ins Hintertreffen, denn dort sind die wesentlichen Teile der Senatsbeschlüsse zu veröffentlichen, wenn das Hamburgische Transparenzgesetz 2014 in Kraft tritt.

Gegenwärtig stehen wir zudem an einer entscheidenden Wegmarke: Wenn die **Geheimdienste** zweier westlicher Demokratien offensichtlich jedes Maß verloren haben und die weltweite Telekommunikation einschließlich der Telefonate und des Mail-Verkehrs auch innerhalb Berlins nahezu lückenlos und weitgehend unkontrolliert überwachen, dann müssen jetzt Konsequenzen gezogen werden. Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat hierzu in der vergangenen Woche konkrete Forderungen erhoben. Die Bundeskanzlerin hat mit Blick auf die Aktivitäten der US-amerikanischen und britischen Geheimdienste gesagt: „Deutschland ist ein Land der Freiheit.“ Der Senat von Berlin sollte sie beim Wort nehmen und auf die zügige Umsetzung des 8-Punkte-Plans der Bundesregierung drängen. Die Aufklärungsbemühungen dürfen mit der Bundestagswahl nicht enden. Jede Regierung und jedes

Parlament in Deutschland sind nach dem Grundgesetz verpflichtet, die Grundrechte der hier lebenden Menschen zu schützen, selbst wenn diese im Ausland beeinträchtigt werden. Auch die Berliner Verwaltung muss Konsequenzen ziehen. Dazu zählt etwa der konsequente Verzicht auf die Nutzung von Telekommunikations-, Cloud- und anderen Internet-Diensten, bei denen der unverhältnismäßige Zugriff ausländischer Geheimdienste nicht hinreichend sicher ausgeschlossen werden kann. Zudem braucht **Europa** jetzt einen **gemeinsamen Rechtsrahmen für den Datenschutz** mit hohem Schutzniveau, was die Vizepräsidentin der EU-Kommission jüngst gemeinsam mit dem Senator für Justiz und Verbraucherschutz mit Recht hervorgehoben hat. Auch hierzu enthält unser Jahresbericht 2012 konkrete Vorschläge.

Wenn Hersteller von Sicherheitssoftware oder Netzknotenrechnern auf Veranlassung der Geheimdienste **Schwachstellen und Hintertüren** in ihren Produkte verstecken, kann nicht verhindert werden, dass auch Kriminelle diese Schwachstellen ausnutzen. So wird statt Sicherheit systematisch Unsicherheit erzeugt und Vertrauen zerstört.

Wir müssen entscheiden, in welcher Gesellschaft wir leben wollen: in einer freien Gesellschaft, in der die heimliche Überwachung der Telekommunikation wieder zur Ausnahme wird, oder in einer unfreien Gesellschaft, in der diese Überwachung die Regel bleibt.

Herzlichen Dank für Ihre Aufmerksamkeit!

Stichwortverzeichnis

P

R / S

T

U / V

W / Z

www.datenschutz-berlin.de

Sicherheit im Berliner Landesnetz • De-Mail als Patentrezept? • EU-Datenschutzreform • Vom sicheren zum unsicheren Hafen – Datenübermittlungen in die USA • Datenverarbeitung im forensischen Bereich eines Wirtschaftsprüfungsunternehmens • Das intelligente Haus • Inernet-Wache • PRISM beim Verfassungsschutz? • Fahrzeugkameras im Straßenverkehr • Funkzellenabfragen – wie weiter? • City Tax • Forschungsprojekt Smart Senior • Vormerksystem für Kita-Plätze • „Doku-Soap" im Kreißsaal? • Personalausweiskopien in Arztpraxen • Diebstahl von Gesundheitsdaten • Datenschutzorganisation bei einer Gewerkschaft • Das Liegenschaftskataster als Marketing-Reservoir? • Lehrkräfte und Facebook • Sprachlerntagebuch • Reality-TV bei den Wasserbetrieben • Reform der Bestandsdatenauskunft • Internationale und europäische Informationsfreiheit