Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Datenschutz und
Informationsfreiheit
in Berlin

Datenschutz und Informationsfreiheit

Bericht 2008

Berlin

Benutzerfreundliche PDF-Datei

Zur besseren Orientierung im Dokument sind sowohl im Stichwort- als auch im Inhaltsverzeichnis alle Begriffe und Seitenzahlen verlinkt, d.h. mit einem Klick auf den Begriff oder Gliederungspunkt gelangen Sie direkt zur entsprechenden Stelle innerhalb des Dokumentes.

Auch alle Internetlinks sind - soweit dies möglich war – mit den entsprechenden Websiten verknüpft.

Auszüge, auch teilweise, sind mit dem Herausgeber abzustimmen.
Für Anregungen sind wir jederzeit dankbar.

Dr. Alexander Dix

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2008

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am **2. April 2008** vorgelegten Jahresbericht 2007 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2008 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2008“) veröffentlicht.

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

Inhaltsverzeichnis

Stichwortverzeichnis

D

E

F

G

H

I

J

K

W

Z

Einleitung

Dies ist der 30. Bericht über den Datenschutz in Berlin, seit der erste Berliner Datenschutzbeauftragte Dr. Hans-Joachim Kerkau im Januar 1980 über die Aufnahme seiner Tätigkeit berichtete. Zugleich ist es der zehnte Bericht über die Informationsfreiheit im Land Berlin, seit der Berliner Datenschutzbeauftragte 1999 auch die Funktion eines Beauftragten für Informationsfreiheit erhielt.

2008 bleibt als Jahr der Datenskandale in Erinnerung. Erstmals haben deutsche Aufsichtsbehörden Bußgelder in Rekordhöhe gegen Unternehmen verhängt, die ihre Arbeitnehmer exzessiv – teilweise mit nachrichtendienstlichen Methoden – überwacht haben. Gegen eine auch in Berlin vertretene Lebensmittelkette wurden Bußgelder in Höhe von insgesamt 1,3 Millionen Euro verhängt. Andere Formen der rechtswidrigen Ausspähung von Beschäftigten, Aufsichtsrats- und Betriebsratsmitgliedern, Gewerkschaftern und Journalisten harren noch der Aufklärung. Die unverhältnismäßigen Überwachungspraktiken bei der Deutschen Bahn AG wurden gegen Ende des Berichtszeitraums in Ansätzen bereits bekannt, werden aber noch von uns aufgearbeitet. Dieser Bericht enthält insoweit nur eine Zwischenbilanz[1].

2008 hat wie kaum ein früheres Jahr die Bedeutung einer Datenschutzkontrolle „in völliger Unabhängigkeit“ verdeutlicht, wie sie die Europäische Datenschutzrichtlinie vorschreibt. Während die Aufsichtsbehörden bisher vorwiegend präventiv tätig wurden, gehen sie nun notgedrungen dazu über, auch Sanktionen zu verhängen. Denn in den Vorstandsetagen mehrerer Unternehmen scheint man Straftaten wie Geheimnisverrat oder Korruption um nahezu jeden Preis und unter Missachtung geltenden Rechts aufdecken zu wollen.

Schon 1976 hat ein Experte der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) darauf hingewiesen, dass nach dem „Jahrhundert-Skandal Watergate“ in den USA als unmittelbare Konsequenz in Rekordzeit ein Datenschutzgesetz beschlossen worden sei. In Europa dagegen – so dieser Experte – sei der Datenschutz noch nicht als wichtiges politisches

1 Vgl. 11.1

Problem erkannt worden, weil es an großen publikumswirksamen Skandalen fehle[2]. Ob dieser Zusammenhang sich jetzt auch in Deutschland bestätigt, ist noch offen: Zwar hat die Bundesregierung wesentliche Teile der Ergebnisse des sog. Datenschutzgipfels vom 4. September als Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes auf den Weg gebracht, wozu auch eine deutliche Erhöhung des Bußgeldrahmens zählt[3]. Ob dieser Entwurf aber ebenso wie der vorangehende Entwurf zur Verbesserung des Datenschutzes bei Auskunfteien und beim Scoring noch vor dem Ende der Legislaturperiode Gesetzeskraft erlangt, ist offen. Selbst wenn dies gelingen sollte, lässt sich aber bereits jetzt sagen, dass die Korrekturen am Bundesdatenschutzgesetz unzureichend sind. Die schon 2001 als überfällig bezeichnete Modernisierung des Datenschutzrechts in Bund und Ländern darf nicht länger aufgeschoben werden und kann durch derartige Ad-hoc-Reparaturen nicht ersetzt werden. Zudem müssen die Befugnisse der Datenschutzbeauftragten ebenso wie ihre Ausstattung deutlich erweitert werden, um den gestiegenen Kontrollbedarf auch nur annähernd zu erfüllen.

Die jüngsten Datenskandale ereigneten sich ausnahmslos im Bereich der Wirtschaft. Dies wird von interessierter Seite als Argument dafür verwandt, dass die entscheidenden Risiken für die Privatsphäre heutzutage von privaten Datenverarbeitern und nicht mehr vom Staat ausgehen. Richtig ist, dass die Gefährdungen für die Freiheit des einzelnen Menschen durch Arbeitgeber, Unternehmen, Internetanbieter und andere private Datenverarbeiter zu lange unterschätzt worden sind. Es wäre aber ein Fehler zu glauben, dass die Risiken der staatlichen Datenverarbeitung künftig vernachlässigt werden können. Zum einen greifen staatliche Stellen verstärkt auf die anwachsenden Datensammlungen privater Unternehmen für ihre Zwecke zu. Auch verliert die Unterscheidung zwischen öffentlicher und nicht-öffentlicher Datenverarbeitung immer mehr an Bedeutung. Sie war für die Öffentlichkeit ohnehin nie nachzuvollziehen. Zum anderen wird weiter an der Gesetzgebungsschraube gedreht, um den Sicherheitsbehörden immer weitergehende Eingriffsbefugnisse in die Rechte Unverdächtiger einzuräumen.

2 Gassmann in: R. Dierstein/H. Fiedler/A. Schulz (Hrsg.), Datenschutz und Datensicherung, Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Informatik und der Gesellschaft für Informatik 1976, S. 11, 17 f.

3 BR-Drs. 4/09

So musste das Bundesverfassungsgericht in kurzem zeitlichem Abstand mehrfach entsprechende Gesetze auf Bundes- und Landesebene korrigieren oder aufheben. Die Regelungen im nordrhein-westfälischen Verfassungsschutzgesetz zur Online-Durchsuchung waren ebenso verfassungswidrig[4] wie die Vorschriften mehrerer Bundesländer zum Scannen von Kfz-Kennzeichen[5]. Schließlich hat das Bundesverfassungsgericht die vom Bundesgesetzgeber vorgesehene Verpflichtung von Telekommunikations- und Internetanbietern zur verdachtsunabhängigen Speicherung von Verkehrsdaten für sechs Monate in mehreren Eilentscheidungen eingeschränkt[6]. Mit einer Entscheidung in der Hauptsache ist erst nach dem Urteil des Europäischen Gerichtshofes über die Wirksamkeit der zugrunde liegenden Europäischen Richtlinie zu rechnen. Letztlich wird der Europäische Gerichtshof auch die Frage zu beantworten haben, ob eine generelle verdachtsunabhängige Speicherung sämtlicher Verkehrsdaten mit dem Grundrecht auf unbeobachtete Kommunikation vereinbar ist.

Insgesamt sollte die automatisierte Verarbeitung von personenbezogenen Daten nicht nur unter datenschutzrechtlichen, sondern auch unter ethischen Aspekten diskutiert werden. Dies war das Anliegen des aus Berlin stammenden und im März hier verstorbenen Computerwissenschaftlers und Gesellschaftskritikers Joseph Weizenbaum. Er hat schon 1976 formuliert: „Die wichtigste Grundeinsicht … ist die, daß wir zur Zeit keine Möglichkeit kennen, Computer auch klug zu machen, und daß wir deshalb im Augenblick Computern keine Aufgaben übertragen sollten, deren Lösung Klugheit erfordert.“[7] Weizenbaum hat auch darauf hingewiesen, dass Automatisierung Probleme nicht löst, sondern sie lediglich automatisiert. Die darin zum Ausdruck kommende Skepsis könnte viele Entwickler und Anwender von elektronischer Datenverarbeitung vor einer Überschätzung dieser Technik bewahren, was auch dem Datenschutz zugute käme.

4 Urteil vom 27. Februar 2008, NJW 2008, 822

5 Urteil vom 11. März 2008, NJW 2008, 1505

6 Vgl. 6.1

7 Die Macht der Computer und die Ohnmacht der Vernunft. 9. Aufl. Frankfurt am Main 1994, S. 300

Die Informationsfreiheit in Berlin ist selbst nach zehn Jahren noch im Entwicklungsstadium und hat bisher bei weitem nicht die Bedeutung wie in Skandinavien, Großbritannien oder den USA. Gleichwohl gibt es positive Entwicklungen auf Landes- und auf europäischer Ebene, die zu einer Erhöhung der Transparenz führen können[8]. Hervorzuheben ist vor allem die Fertigstellung eines Entwurfs für eine Europaratskonvention über den Zugang zu amtlichen Dokumenten, die bei ihrem Inkrafttreten der erste völkerrechtlich verbindliche Vertrag weltweit zur Informationsfreiheit sein wird.

8 Vgl. 15.1

1. Technische Rahmenbedingungen

1.1 Entwicklung der Informationstechnik

1.1.1 Computerleistung aus der Wolke

Vom Client-Server-Netz zum Terminal-Server-System

Im Jahresbericht 2006 widmeten wir dem Server Based Computing (SBC) ein eigenes Schwerpunktthema und erkannten dabei eine Rückbesinnung auf die Wurzeln der zentralen Datenverarbeitung. Viele Jahre dominierten sog. Client-Server-Systeme, die lokale Netze mit Servern für das Anbieten bestimmter informationstechnischer Leistungen und leistungsstarke Rechner an den Arbeitsplätzen (Clients) verbanden, von denen aus diese Leistungen abgerufen werden können. Ab 2005 gewannen SBC-Systeme (auch Terminal-Server-Systeme genannt) an Bedeutung, bei denen leistungsstarke Server auch die Aufgaben übernahmen, die zuvor von den Clients erbracht wurden. Diese wurden nur noch für die Darstellung der Mensch-Maschine-Schnittstelle, also der Verarbeitungsergebnisse der Server, und den Betrieb der Eingabesysteme (Tastatur, Maus) gebraucht. Konsequenterweise kamen dann auch abgespeckte Arbeitsplatzsysteme (sog. Thin Clients) zunehmend in den Einsatz.

Dieser Wandel war die Konsequenz der permanenten Leistungssteigerung der Verarbeitungs- und Speicherkomponenten. Der Bedarf an diesen Leistungen wuchs in den normalen Büroanwendungen und Fachverfahren trotz der steigenden Anforderungen moderner Softwareprodukte weniger schnell als das Angebot. Also schraubte man die Anforderungen an die Server hoch, um sie überhaupt auszulasten, und verzichtete auf normale PCs am Arbeitsplatz, deren gewaltige Kapazitäten kaum zu 10 % in Anspruch genommen wurden.

Hinzu kommt, dass es inzwischen fast völlig gleichgültig ist, wo die Server stehen, ob im Serverraum des Anwenders, in einem entfernten Rechenzentrum irgendwo in der Stadt oder irgendwo auf der Welt. Auch das IT-Dienstleistungszentrum des Landes Berlin (ITDZ) bietet den Behörden des Landes mit

dem IT-Infrastruktur-Service (ITIS) an, Fach- und Büroanwendungen auf Servern im Sicherheitsrechenzentrum über das Berliner Landesnetz in Anspruch zu nehmen.

Vom Terminal-Server-System zum Cloud Computing?

Ist es nun der „Paradigmenwechsel in der Art und Weise, wie Anbieter informationstechnische Dienste bereitstellen" und wird Informationstechnik „zum Gebrauchsgut wie Wasser und Strom"[9] oder ist es ein Wolkenkuckucksheim? Fest steht: Eines der meist gelesenen Schlagworte lautet „Cloud Computing" – Computerleistung aus der Wolke. In allen Darstellungen der Konfiguration moderner IT-Systeme findet man das Zeichen der Wolke. Die Wolke symbolisiert ein offenes Netz, in aller Regel das Internet. „Cloud Computing" ist also Computerleistung aus dem Internet. Welche Leistungen das sein können, ist von Anbieter zu Anbieter unterschiedlich. Manchmal handelt es sich um Server samt Betriebssystemen, auf denen die Kunden ihre Anwendungen installieren und betreiben können. So hat der Internet-Buchhändler Amazon seine überschüssigen Kapazitäten für diverse Plattformen inzwischen offenbar zu einem ertragreichen zweiten Standbein ausgebaut, das es mit dem Elastic-Computer-Cloud-(EC2-)Angebot Unternehmen ermöglicht, die eigenen Anwendungen auf einer solchen Infrastruktur betreiben zu können.

Grundsätzlich kann jeder IT-Dienst über das Cloud Computing genutzt werden. Der Kundschaft wird keine Systemkomponenten mehr geliefert, sondern eine zu bezahlende Dienstleistung. Da die Dienstleistungen in großer Kapazität weltweit über das Internet zu Verfügung gestellt werden, bleiben sie kostengünstig und von überall erreichbar. Die Dienstleistungen werden vielen Kundinnen und Kunden angeboten, die Ressourcen werden gemeinsam genutzt, so dass weitere Kostenvorteile entstehen.

Über den Stand der Entwicklung des Cloud Computing gibt es unterschiedliche Expertenmeinungen. Während Amazon bereits sein EC2-Angebot vermarktet, kann das Google-Angebot (Google App Engine) noch von möglicher Kundschaft getestet werden. Auch IBM und Microsoft haben Produkte zum Cloud Computing angekündigt. Man geht dennoch davon aus, dass der Trend zum Cloud Computing kein kurzzeitiger Hype sein wird, da die Vorteile für

9 W. Herrmann: Die geplante Revolution. In: Computerwoche Nr. 50/2008, S. 14 ff.

Anwender und Anbieter auf der Hand liegen. So sehr sich aber die Begeisterung für den angeblichen Megatrend[10] ausbreitet, so mehren sich warnende Stimmen, die sowohl datenschutzrechtliche als auch sicherheitstechnische Fragen anschneiden.

Datenschutz und IT-Sicherheit beim Cloud Computing

Nach den Grundsätzen der Europäischen Datenschutzrichtlinie für die Übermittlung von personenbezogenen Daten in Drittländer haben die Mitgliedstaaten in ihren nationalen Gesetzen Regelungen geschaffen, die die Zulässigkeit solcher Übermittlungen einschränken.

Cloud Computing ist eine spezielle Ausprägung der Datenverarbeitung im Auftrag[11]. Verarbeitet ein Auftragnehmer Daten für einen Auftraggeber, so gilt der Auftragnehmer nicht als Dritter im Sinne des Datenschutzrechts.[12] Der Auftragnehmer trägt keine eigene Verantwortung für die Verarbeitung der Daten (mit Ausnahme seiner Verpflichtung zur Durchführung von technisch-organisatorischen Maßnahmen[13]), der Auftraggeber bleibt datenschutzrechtlich verantwortlich für die Daten. Die Weitergabe der zu verarbeitenden Daten an den Auftragnehmer ist demzufolge keine Datenübermittlung, für die es eine Rechtsgrundlage geben müsste. Etwas anderes gilt jedoch, wenn der Auftragnehmer die Daten nicht innerhalb der EU bzw. des Europäischen Wirtschaftsraums verarbeitet. In diesem Fall ist er nach § 3 Abs. 8 Satz 3 Bundesdatenschutzgesetz (BDSG) Dritter, und die Bereitstellung der personenbezogenen Daten zum Zwecke der Auftragsdatenverarbeitung ist eine Übermittlung, deren Zulässigkeit sich an §§ 4 b und 4 c BDSG messen lassen muss.

Cloud Computing bietet Dienstleistungen mit personenbezogenen Daten, die völlig ortsunabhängig sind, also irgendwo in der Welt erbracht werden können, ohne dass die Kundin oder der Kunde wissen müsste, wo die Daten sind. Dies wäre aber nach den dargestellten datenschutzrechtlichen Ausnahmeregelungen für die Auftragsdatenverarbeitung in Drittstaaten nicht zulässig. Die datenschutzrechtlich für die Datenverarbeitung verantwortlichen, z.B. deutschen

10 Ch. Witte: Cloud Computing ist ein Megatrend, http://www.computerwoche.de/1877014
11 § 11 BDSG
12 § 3 Abs. 8 Satz 2 BDSG
13 § 9 BDSG

Kundinnen und Kunden, müssen sich davon überzeugen, dass die Datenverarbeitung nicht in einem Drittland ohne angemessenes Datenschutzniveau, z.B. in den USA, China oder Japan, stattfindet. Dies beschränkt die Ortsunabhängigkeit des Cloud Computing. Aus diesem Grunde müssen die Cloud-Computing-Provider dem Beispiel Amazons folgen, die Dienstleistungen in unterschiedlichen Regionen mit gemeinsamen Datenschutzstandards anzubieten, also zum Beispiel innerhalb der EU und anderer Länder, die nicht als Drittländer anzusehen sind.

Auch soweit Sozialdaten, zum Beispiel von Krankenkassen, verarbeitet werden, gelten diese Argumente gegen eine Auftragsdatenverarbeitung in Drittstaaten gleichermaßen. Hinzu kommt, dass § 80 Abs. 5 Sozialgesetzbuch X (SGB X) die Zulässigkeit der Verarbeitung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen zusätzlich so beschränkt, dass ein Outsourcing per Cloud Computing unwirtschaftlich sein dürfte.

Neben diesen datenschutzrechtlichen Aspekten, die beim Cloud Computing zu beachten sind, wird eine Reihe von Sicherheitsaspekten diskutiert, die bei Anwendung dieser neuen Betriebsform beachtet werden sollten[14]:

- Bei der Datenverarbeitung im eigenen Hause existieren für den privilegierten Zugriff auf sensitive Daten durch Systemverwalter physische, logische und von Mitarbeitenden gesteuerte Kontrollmechanismen der IT-Abteilungen. Diese verlieren bei der Auslagerung „in die Wolke“ dadurch ihre Funktion, dass fremde Administratoren den Zugriff auf die sensitiven Daten erhalten. Die Kundenunternehmen müssen sich daher detaillierte Informationen über die Systemadministratoren beim Anbieter verschaffen, über die Auswahlkriterien bei ihrer Einstellung, über die auf sie wirkende Aufsicht sowie die eingesetzten Verfahren und die Zugriffskontrolle.
- Auch wenn die Datenverarbeitung ausgelagert wurde, behalten die Kunden wie bei der „normalen“ Datenverarbeitung im Auftrag ihre volle datenschutzrechtliche Verantwortung für ihre eigenen Daten[15]. Zur Aufrechterhaltung der „Compliance“, also der Einhaltung der gesetzlichen Bestimmungen

14 K. Friedmann: Wo die Gefahren lauern, http://www.computerwoche.de/1867951

15 §§ 11 Abs. 1 BDSG bzw. § 3 Abs. 1 BlnDSG gelten natürlich auch bei Cloud Computing.

bei der Verarbeitung von Daten, sollten die Kunden darauf achten, dass sich die Anbieter externen Audits und Zertifizierungen unterwerfen.

- Cloud Computing bedeutet auch, dass mehrere Kunden in der gleichen Umgebung verarbeiten lassen. Damit entstehen Risiken, die in einer nicht hinreichenden Trennung der gespeicherten Daten liegen. Die Kunden müssen sich daher vor der Auftragsvergabe absichern, welche Methoden zur Trennung der Daten unterschiedlicher Auftraggeber angewandt werden. Sofern dies durch Verschlüsselung erfolgt, muss der ordnungsgemäße Entwurf der Verschlüsselungssysteme geprüft werden, um sicherzugehen, dass die Verfügbarkeit der Daten gewährleistet ist.
- Die Kunden sollten sich genau darüber informieren, welche Maßnahmen im Falle des Ausfalls der Speichersysteme beim Dienstleister für die vollständige Wiederherstellung von Daten und Anwendungsverfahren vorgesehen sind, bevor man ihm die Daten anvertraut.
- Die Entdeckung ungewöhnlicher oder illegaler Aktivitäten ist beim Cloud Computing erschwert, da der Kunde nicht immer weiß, wo die Daten verarbeitet werden, und dies sich auch unbemerkt ändern kann. Die Provider sind daher vertraglich zu verpflichten, dass spezielle Überprüfungen auf ungewöhnliche oder illegale Aktivitäten möglich sind und durchgeführt werden.
- Die Kunden müssen vor Auftragsvergabe klären, dass die eigenen Daten auch dann verfügbar bleiben, wenn der Cloud-Computing-Provider insolvent oder von einem anderen Unternehmen übernommen wird.

1.1.2 Aktuelle informationstechnische Entwicklungen

Zu den Aufgaben der Datenschutzbehörden gehört auch, aktuelle Entwicklungstendenzen in der Informationstechnik zu beobachten und künftige Entwicklungen vorherzusehen, die sich aus den aktuellen Forschungsschwerpunkten der Informatik ableiten lassen. Nur so können künftige datenschutzrechtliche Risiken erkannt werden, sodass Regelungsbedürfnisse und technische sowie organisatorische Gestaltungsalternativen rechtzeitig geprüft werden können.

Nach 2006[16] legte der Arbeitskreis für technische und organisatorische Datenschutzfragen (AK Technik) der Datenschutzkonferenz 2008 zum zweiten Mal einen Kurzbericht über aktuelle technische Entwicklungen vor, die den Datenschutz berühren.

Der neue Bericht befasst sich neben der schon im Vorjahr behandelten Konvergenz der Informations- und Kommunikationstechnik[17] mit folgenden aktuellen Techniken:

- **Identitätsmanagement** ist das Verwalten von Identitätsdaten in informationstechnischen Systemen, also von Daten, die zu einer natürlichen Person gehören, nicht aber für alle Datenverarbeiter personenbezogen sein müssen. Bei den Identitätsdaten handelt es sich um Daten, mit denen sich eine Benutzerin oder ein Benutzer gegenüber IT-Systemen authentisiert und autorisiert, mit denen ihr oder ihm Rollen und die damit verbundenen Berechtigungen zugewiesen werden. In verschiedenen Zusammenhängen kann eine Person verschiedene Identitäten haben, aber eine Identität bezieht sich umgekehrt nur auf eine Person. Es gibt bereits viele Identitätsmanagementsysteme auf dem Markt, die sich hinsichtlich der Selbstbestimmung und Transparenz für die Nutzenden erheblich unterscheiden können. Außerdem gibt es datensparsame Techniken, bei denen Nutzende ihre Berechtigungen in Form von Zertifikaten unter verschiedenen Pseudonymen nachweisen können. Mit der Einführung des elektronischen Personalausweises gewinnt das Identitätsmanagement für alle erheblich an Bedeutung, da der Ausweis nicht nur zur Vorlage gegenüber Berechtigten, sondern auch als Hilfsmittel zur sicheren Authentisierung bei E-Government oder E-Commerce dient.
- Der Kurzbericht befasst sich auch mit dem sogenannten **Application Service Providing (ASP)** und den **serviceorientierten Architekturen (SOA).** Beim ASP handelt es sich um Geschäftsmodelle, mit denen ein Provider IT-Dienstleistungen anbietet, die nach Verbrauch abgerechnet werden („IT aus der Steckdose"). Bei SOA geht es um die Kopplung wieder verwendbarer Softwarebausteine, die gewisse Standards einhalten müssen, so dass Anwendungen schneller an geänderte Anforderungen angepasst werden können. Auch SOA wird aus dem Internet angeboten. Nutzende kennen

16 JB 2006, 1.1
17 JB 2007, 1.1

den angebotenen Dienst, wissen, welche Eingaben sie machen müssen, aber nicht, wie die Ergebnisse der Datenverarbeitung zustande kommen. Die Parallelität zu den Eigenschaften des Cloud Computing liegt bei ASP und SOA auf der Hand. Die dort beschriebenen Risiken für Compliance, Transparenz und Sicherheit sind bei ASP und SOA ebenfalls zu beachten.

- **Suchmaschinen** gehören zu den unentbehrlichen Werkzeugen für die Erschließung der riesigen Informationsangebote des Internets. Aber es gibt auch warnende Stimmen, die darauf hinweisen, dass die Präsentation der Suchergebnisse, insbesondere das Ranking, einfach beeinflusst werden kann, ohne dass die dahinter stehenden Algorithmen transparent wären. Das Ranking der Suchergebnisse prägt die Sicht auf die Wirklichkeit, die so auch manipuliert sein kann.
- Wer Suchmaschinen nutzt, hinterlässt zudem digitale Spuren über seine Interessen und Vorlieben, wie die gleichzeitig angebotene kontextbezogene Werbung deutlich macht. Mit der Integration weiterer Dienste wie z.B. E-Mail, Bezahlfunktionen, Routenplaner usw. in die Suchmaschinenumgebung können komplette Persönlichkeitsprofile entstehen.
- Zu Persönlichkeitsprofilen beisteuern können auch die **standortbezogenen Dienste (Location Based Services),** die als mobile Dienstangebote positions-, manchmal auch zeit- und personenabhängig sind. Dazu gehören Dienste im Bereich des GSM- oder UMTS-Mobilfunks zur Routenplanung, Finden bestimmter Gaststätten und Geschäfte, Positionsbestimmungen des eigenen oder von fremden Mobiltelefonen, Fahrplanauskünfte. Bewegungsprofile lassen sich hier verbinden mit Aktivitäten, Beziehungen und Vorlieben der Nutzenden.

Als mittelfristige Entwicklungen beschreibt der Kurzbericht die **Konvergenz von Videoüberwachung, Biometrie und RFID,** die wir bereits früher problematisiert hatten[18], das **Digital Rights Management (DRM)** zur Absicherung des Urheberrechts und das **Ubiquitous Computing**[19]. Als Forschungsgebiete benennt der Kurzbericht die **Quantenkryptographie**[20] und die **Nanotechnologie**[21], die wir 2006 im Schwerpunkt unserer Betrachtungen zu den technischen Entwicklungen dargestellt hatten.

18 JB 2006, 1.1; JB 2007, 11.1
19 JB 2004, 2.1
20 JB 2006, 1.1
21 JB 2006, 1.1

1.2 Datenverarbeitung in der Berliner Verwaltung

1.2.1 IT-Politik für die Berliner Verwaltung

Die Behörden in den Mitgliedstaaten der Europäischen Union stehen spätestens mit der Umsetzung der Europäischen Dienstleistungsrichtlinie (DLR) vor der immensen Aufgabe, kompatible Datenverarbeitungsinfrastrukturen zu schaffen, die es den Behörden ermöglichen, europaweit auf elektronischem Wege Informationen bereitzuhalten, Daten und Dokumente auszutauschen, Anträge entgegenzunehmen, unter Einschaltung aller zuständigen Stellen zu bearbeiten und bescheiden, und die es dadurch allen Bürgerinnen und Bürgern ermöglicht, Informationen abzurufen und Anträge zu stellen, ohne dabei auf nationale Egoismen und unüberwindliche technische Schranken zu stoßen.

Der Berliner Senat hat die prioritären IT-Projekte weiterentwickelt, über die wir in der Vergangenheit ausführlich berichtet haben[22]. Das Senats-Informations- und Dokumentationssystem (SIDOK) zur Vor- und Nachbereitung der Sitzungen des Senats ist auf der Grundlage eines marktüblichen Dokumentenmanagement- und Vorgangsbearbeitungssystems eingeführt worden. Das „Berlin-Telefon 900“ ist als einheitliches Telefonportal in die Berliner Verwaltung für die Bürger eingerichtet worden und wird der Berliner Beitrag zur bundeseinheitlichen Behördenservicenummer 115 sein – ein weiterer Schritt der Berliner Verwaltung in Richtung E-Government.

Der durch die DLR vorgeschriebene nächste Schritt stellt den Übergang von der Papierakte zur verbindlichen elektronischen Akte dar. Soweit überhaupt schon Dokumentenmanagementsysteme[23] eingesetzt werden, werden sie in der Regel „nur“ zur Arbeitsunterstützung und inhaltlichen Qualitätsverbesserung aufgrund komfortabler Suchmöglichkeiten verwendet. Die führende Akte blieb zumindest bisher stets die Papierakte, schon deshalb, weil nur sie den notwendigen Beweiswert bei gerichtlichen Auseinandersetzungen bieten konnte. Dies muss sich ändern, wenn Anträge elektronisch gestellt, bearbeitet

22 JB 2006, 1.2

23 Ausführlich dazu JB 2006, 2.6 und die Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“, http://www.datenschutz-berlin.de/attachments/3/OH-DMS.pdf?1161158417

und beschieden werden sollen, wie es die DLR vorsieht. Der Übergang von der führenden Papierakte zur führenden und damit verbindlichen elektronischen Akte – vom papierlosen Büro wollen wir dabei noch nicht sprechen – wird mit großen Umwälzungen in den Behörden und in den Köpfen ihrer Dienstkräfte verbunden sein.

Die Senatsverwaltung für Inneres und Sport hat zum Ende des Jahres einen Zwischenbericht zur „Schaffung der Rahmenbedingungen für einen flächendeckenden Einsatz eines DMS/VBS-Systems in der Berliner Verwaltung“ vorgelegt. Den Schwerpunkt der Schaffung geeigneter rechtlicher Rahmenbedingungen soll eine überarbeitete Gemeinsame Geschäftsordnung der Berliner Verwaltung (GGO I) bilden. Sie wird vorsehen, dass die elektronisch gestützten Verwaltungsprozesse keinen höheren rechtlichen Anforderungen unterliegen als die traditionell papiergebundenen Prozesse, dass die elektronische Akte und der elektronische Geschäftsgang explizit zugelassen wird und dass das Scannen des Schriftguts und der rechtssichere und wirtschaftliche Einsatz der qualifizierten digitalen Signatur sowie die Aussonderungsverfahren abgesichert werden. Ferner wird der Bedarf nach einem Rahmenaktenplan geprüft. Die Schaffung der technischen Rahmenbedingungen soll die Erfahrungen des Projekts SIDOK einbeziehen, damit die rechtssichere Ablage von Dokumenten aus IT-Fachverfahren, die Registratur, die rechtssichere elektronische Akte und Vorgangsbearbeitung möglich werden.

1.2.2 IT-Sicherheit in Berlin

Seit dem Inkrafttreten der ersten Datenschutzgesetze in den 70er Jahren des letzten Jahrhunderts müssen alle öffentlichen und privaten Organisationen technische und organisatorische Maßnahmen ergreifen, um die Ausführung der Vorschriften des Datenschutzes sicherzustellen. Technische Hindernisse darf es nicht geben, wenn z.B. eine Person wissen will, welche Daten über sie gespeichert sind. Das Löschen, Sperren und Korrigieren von Daten muss technisch möglich sein. Zudem müssen unbefugte Kenntnisnahmen, Verarbeitungen, Speicherungen, Änderungen, Löschungen und Übermittlungen verhindert werden. Dies betrifft sowohl das Handeln von unbefugten Dritten als auch nicht autorisiertes Handeln von Beschäftigten der Daten verarbeitenden Stellen.

Mit der Novellierung des Berliner Datenschutzgesetzes im Jahre 2001 ist der Gesetzgeber den Anregungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gefolgt, die statischen Kontrollanforderungen des alten Gesetzes durch Zielvorgaben zu ersetzen, deren Verfehlungen schon länger als „Grundbedrohungen der IT-Sicherheit“ bekannt waren. Die im IT-Sicherheitshandbuch des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) bereits 1992 beschriebenen Grundbedrohungen der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Programmen und Systemen wurde ergänzt durch die im Internet erhöhte Gefahr für die Authentizität von Daten, Programmen und Systemen sowie die Ziele der Revisionsfähigkeit und Transparenz der Verfahren, um die Beherrschbarkeit und Kontrolle der IT-Systeme sicherzustellen.

Außerdem sind vor der Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung die notwendigen technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Sinn macht dies jedoch erst, wenn man eine Reihenfolge beachtet. In einer Risikoanalyse – oder bei Anwendung der aktuellen Grundschutz-Kataloge zumindest einer Schutzbedarfsanalyse – ist festzulegen, gegen was man sich in der konkreten Situation schützen muss, um dann festzulegen, was man gegen Risiken tun kann, die man nicht bewusst akzeptieren will. Damit wird gleichzeitig die geforderte Angemessenheit für den angestrebten Schutzzweck sichergestellt. Angemessen ist alles, was das Restrisiko als tragbar erscheinen lässt, entweder weil die Maßnahmen das Eintreten von Schäden hinreichend unwahrscheinlich machen, oder weil die Maßnahmen im Falle eines Schadens diesen ausreichend begrenzen.

Die IT-Sicherheitsgrundsätze des Senats[24] legen fest, dass die IT-Grundschutz-Kataloge des Bundesamtes für die Sicherheit in der Informationstechnik (BSI)[25] bei der Erarbeitung von Sicherheitskonzepten zu verwenden sind. Um dies zu vereinfachen, hat das IT-Kompetenzzentrum bei der Senatsverwaltung für Inneres ein „Modellsicherheitskonzept” erstellt und aktualisiert es laufend. Nur mit vergleichbaren und fachlich abgesicherten Vorgehensweisen lässt sich sicher-

24 Grundsätze zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsgrundsätze) vom 11. Dezember 2007

25 http://www.bsi.de/gshb/index.htm

stellen, dass die Risikoanalysen so vollständig wie möglich sind und es nicht Zufälligkeiten unterliegt, welche Risiken man entdeckt. Die Sicherheitsgrundsätze verlangen auch, dass alljährlich ein IT-Sicherheitsbericht aus Einzelberichten der Berliner Behörden zusammengestellt wird. Der aktuell vorliegende IT-Sicherheitsbericht 2008 stellt die Situation zum Zeitpunkt der Erhebung im Jahre 2007 dar. Die folgenden Angaben stützen sich also auf die Selbstdarstellungen der Behörden und geben nicht Ergebnisse unserer Kontrollen wieder:

Von den 71 Behörden, die mit ihren Mitteilungen am Bericht teilgenommen haben, gaben 47 an, dass ein behördliches Sicherheitskonzept vorliegt. Die übrigen 24 Behörden arbeiteten zum Termin der Abfrage an einem Sicherheitskonzept. Immerhin ist daraus zu schließen, dass die nach 2001 zunächst geübte Zurückhaltung bei der Erarbeitung von Sicherheitskonzepten inzwischen aufgegeben wurde. Keine Behörde scheint mehr am Sinn von Sicherheitskonzepten zu zweifeln. Auch die methodischen Vorgaben (Grundschutz-Kataloge oder Modellsicherheitskonzept) werden erfreulicherweise beachtet. Von den 47 gemeldeten Sicherheitskonzepten waren 37 von der Behördenleitung bestätigt. Für die übrigen zehn Behörden muss also angenommen werden, dass eine Umsetzung in konkrete Maßnahmen noch nicht die Billigung der Leitungen hat und daher offen bleibt.

Erfreulich ist auch, dass in der Mehrzahl der Behörden der vorgeschriebene IT-Sicherheitsprozess angelaufen ist, der für die permanente Überprüfung und Ergänzung der Sicherheitskonzepte gebraucht wird. In 32 Behörden wurde sogar ein IT-Sicherheitsmanagement eingerichtet. Dies gilt allerdings nicht für jene sieben Behörden, die angaben, für die IT-Sicherheit keinerlei Ressourcen zur Verfügung zu haben. Da die Bereitstellung von Ressourcen auch in Zeiten der Mittelknappheit stets eine Prioritätenabwägung darstellt, ist es diesen Behörden offenbar gleichgültig, ob die Informationstechnik sicher und zuverlässig funktioniert.

Der sichere Einsatz der Informationstechnik in der Berliner Verwaltung ist längst keine Selbstverständlichkeit, auch wenn die Zahl an bekannt gewordenen Sicherheitsvorfällen gering und die Schadenshöhe verschmerzbar zu sein scheint. Wenn durch das aufkommende E-Government die Verwaltungsverfahren den Gefahren des Internets ausgesetzt werden, darf die IT-Sicherheit jedoch nicht länger mit niedriger Priorität behandelt werden.

1.2.3 Aktuelle IT-Projekte des Landes

RFID in den öffentlichen Bibliotheken

Der Einsatz modernster Technologien in der Verwaltung findet stets Aufmerksamkeit im politischen Bereich. So hat der Plan der für kulturelle Angelegenheiten zuständigen Senatskanzlei, die Verwaltung der Medien in öffentlichen Bibliotheken mit Hilfe der RFID-Technik zu revolutionieren, die Aufmerksamkeit des für Datenschutz zuständigen Unterausschusses des Abgeordnetenhauses von Berlin erregt, der das Thema im November 2007 behandelte. In diesem Zusammenhang wurden wir erstmals über das Projekt informiert, was angesichts der Tatsache, dass auch heute noch keine Realisierung in Sicht ist, nicht kritisiert werden kann. Damals lag ein Prüfgutachten zu den Einsatzmöglichkeiten von RFID in den Bibliotheken vor, das hinsichtlich des Datenschutzes zum Ergebnis kam, dass dieser zwar berührt wird, aber im untersuchten Bereich unproblematisch sei. Allerdings hält es das Gutachten für notwendig, dass die verantwortlichen Stellen Maßnahmen zur Vermeidung von Sicherheitslücken treffen müssten, auch um eventuell kriminelles Handeln zu erschweren. Wir haben daher auf die Notwendigkeit eines IT-Sicherheitskonzepts hingewiesen, das auch auf die Potienziale der eingesetzten Technik eingehen muss. Wir werden das Projekt, für das im kommenden Haushalt Mittel vorgesehen werden sollen, weiter intensiv begleiten.

MODESTA – Modernisierung der Staats- und Amtsanwaltschaft

Nachdem wir durch Veröffentlichungen im Internet davon gehört hatten, dass die Generalstaatsanwaltschaft Berlin die Modernisierung ihrer IT-Anwendung anstrebt, haben wir um die gesetzlich vorgeschriebene Unterrichtung[26] gebeten.

Mit dem Projekt MODESTA soll die elektronische Registratur der Staatsanwaltschaften, die seit 1984 mit dem Verfahren ASTA (Amts- und Staatsanwaltschaften) betrieben wurde, durch ein modernes Vorgangsverwaltungs- und -bearbeitungssystem ersetzt werden. Dazu sind die bisher in ASTA gespeicherten Daten nach MODESTA zu migrieren.

In der ersten Ausbaustufe bleibt das primäre Bearbeitungsmedium bei den Strafverfolgungsbehörden die Papierakte. Es entsteht aber bereits eine elektronische Akte, die jedoch nur die bei der Behörde erstellten Dokumente aufnimmt.

26 § 24 Abs. 3 Satz 3 BlnDSG

Die erste Stufe beinhaltet die automatisierte Schriftguterstellung und einen parallel zum Papierfluss eingerichteten Workflow der elektronischen Akte. In der zweiten Stufe werden die Akten vollständig elektronisch geführt und ausschließlich elektronisch bearbeitet. Papiereingänge müssen gescannt werden. In dieser Stufe werden auch die in POLIKS vorhandenen Dokumente der Vorgänge neben den Metadaten an MODESTA übertragen.

Das vorgelegte Pflichtenheft sieht nur Schnittstellen von MODESTA zum Verfahren POLIKS der Berliner Polizei, AULAK (Registratur-Fachanwendung der ordentlichen Gerichte) und JUKOS (Fachanwendung zur Geldstrafenvollstreckung) vor. Alle übrigen Schnittstellen müssen weiter über ASTA abgewickelt werden, so dass das Altverfahren in Betrieb bleiben und über eine Schnittstelle aus MODESTA befüllt werden muss. Bei den weiteren Schnittstellen handelt es sich um die Verbindungen zum BZR (Bundeszentralregister), VZR (Verkehrszentralregister), GZR (Gewerbezentralregister), StaLA (Statistik), ZStV (Zentrales Staatsanwaltschaftliches Verfahrensregister), LABO (Melde- und Ausländerangelegenheiten) und zu ZEDA/S (Namensdatei in Strafsachen des AG Tiergarten). Vorgesehen ist ein Server-Based-Computing-Betrieb mit mehreren Server-Parks im ITDZ und mit Thin Clients an den Arbeitsplätzen. Dies ist aus IT-Sicherheitsgründen zu begrüßen, da dadurch fast alle Risiken, die von Clients und ihren Benutzerinnen und Benutzern ausgehen, unterbunden werden.

In einer ersten rechtlichen Bewertung des Verfahrens sind wir zu dem Ergebnis gekommen, dass die von der Generalstaatsanwaltschaft angegebenen Rechtsgrundlagen aus der Strafprozessordnung zwar auf die Speicherung, Änderung und Nutzung von personenbezogenen Daten, nicht jedoch auf alle denkbaren Übermittlungsvorgänge anwendbar sind. MODESTA soll nicht nur die Datenübermittlung nach § 487 Abs. 1 StPO unterstützen, der lediglich die Datenübermittlung zu Zwecken des Strafverfahrens, der internationalen Rechtshilfe in Strafsachen und von Gnadensachen erlaubt. Soweit eine Datenübermittlung zu anderen Zwecken erfolgt, richtet sich dies nach bereichsspezifischem Recht, zu dem jedoch noch nachvollziehbare Angaben fehlen.

Eine abschließende Bewertung des Verfahrens kann erst erfolgen, wenn der Entwurf der Errichtungsanordnung nach § 490 Strafprozessordnung (StPO), die Risikoanalyse und das Sicherheitskonzept nach § 5 Abs. 3 Satz 1 Berliner

Datenschutzgesetz (BlnDSG) sowie das Ergebnis der nach § 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG vom behördlichen Datenschutzbeauftragten der Generalstaatsanwaltschaft durchzuführenden Vorabkontrolle nach § 5 Abs. 3 Satz 2 BlnDSG vorliegen.

Zeitmanagementsystem für Behörden

Bürgerfreundlichkeit ist eines der Ziele, die mit der Automatisierung der Verwaltungsvorgänge und insbesondere dem E-Government erreicht werden sollen. Ein Beispiel für eine bürgerfreundliche Verfahrensweise ist das Projekt des Zeitmanagements bei Behörden. Das Verfahren enthält zwei Komponenten, die einzeln oder auch integriert eingesetzt werden können:

Zunächst leistet es die elektronische Terminverwaltung durch Sachbearbeitung von Ämtern inkl. E-Appointment, also die Option für Bürgerinnen und Bürger, bei Ämtern auf elektronischem Wege Termine zu reservieren. Solche Wege wären z.B. das Internet oder fernmündlich das Behörden-Call-Center in ITDZ (künftig: 115). Die Reservierung könnte auch unter Pseudonym erfolgen. Weiter soll die bisherige Organisation der Warteschlangen mittels Ziehung von Bearbeitungsnummern durch ein IT-gestütztes Verfahren abgelöst werden, bei dem die Bürgerin oder der Bürger per SMS oder E-Mail zeitnah über den voraussichtlichen Zeitpunkt ihrer/seiner Bedienung informiert wird.

Offen war zunächst die Rechtsgrundlage für die Verarbeitung der Bürgerdaten, da die vom Landesamt für Bürger- und Ordnungsangelegenheiten als Rechtsgrundlage herangezogene Einwilligungslösung nicht hinreichend trägt. Die Betroffenen kennen nicht alle Verfahrensschritte in voller Konsequenz, so dass die Voraussetzungen der „informierten" Einwilligung nicht gegeben sind. Als Rechtsgrundlage kommt hier jedoch das Gesetz über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit (Informationsverarbeitungsgesetz (IVG)) in Betracht. Dieses Gesetz regelt die Verarbeitung personenbezogener Daten bei der manuellen und automatisierten allgemeinen Verwaltungstätigkeit, soweit hier keine besonderen gesetzlichen Vorschriften gelten oder im Hinblick auf das informationelle Selbstbestimmungsrecht erforderlich sind. Die öffentlichen Stellen des Landes Berlin dürfen personenbezogene Daten bei der Wahrnehmung ihrer Aufgaben ohne Einwilligung der Betroffenen verarbeiten, soweit dies für die allgemeine Verwaltungstätigkeit erforderlich ist und schutzwürdige Belange der

Betroffenen wegen der Art der Daten, wegen der Art der Verwendung oder wegen ihrer Offenkundigkeit nicht entgegenstehen.

§ 4 IVG verlangt zwar eine Risikoanalyse vor der Entscheidung über den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens der allgemeinen Verwaltungstätigkeit, ob und in welchem Umfang mit der Nutzung der Informationstechnik Gefahren für die Rechte der Betroffenen oder für die Funktionsfähigkeit der Verwaltung verbunden sind, jedoch wird diese Forderung von der weitergehenden Anforderung aus § 5 Abs. 3 BlnDSG abgedeckt, wonach grundsätzlich vor der Entscheidung über den Einsatz oder die wesentliche Änderung der automatisierten Datenverarbeitung die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln sind.

Ende April ging das Verfahren in eine Erprobungsphase, über deren Ergebnisse wir noch nicht informiert wurden.

Software zur Unterstützung der ESF- und EFRE-Verwaltung

ESF steht für den Europäischen Strukturfonds und EFRE für den Europäischen Fonds für Regionale Entwicklung. Die Durchführung der Förderungsmaßnahmen von Berliner Projekten erfolgt durch zwei Verwaltungsbehörden im Hause der Senatsverwaltung für Wirtschaft, Technologie und Frauen. Die Arbeit dieser Verwaltungsbehörden soll durch eine neue Software unterstützt werden.

Im Zentrum der datenschutzrechtlichen Betrachtungen dieser Software lag die Frage, in welchen Phasen der Datenflüsse zwischen Fördermittelempfängern und entscheidenden, steuernden und kontrollierenden Instanzen der Personenbezug der Daten erforderlich ist, soweit überhaupt personenbezogene Daten anfallen. Wir haben folgende Datenflüsse als zulässig angesehen:

Die Antrag stellenden Personen liefern die notwendigen, ggf. auch personenbezogenen Daten zu sog. Zwischengeschalteten Stellen (ZGS), die über die Anträge entscheiden müssen und daher alle Daten benötigen. Dies sind Bezirksämter, ggf. auch private Stellen wie z.B. die Beratungs- und Servicegesellschaft Umwelt GmbH. Die ZGS leiten die Daten dann – soweit erforderlich – in personenbezogener Form an die Senatsverwaltung zwecks Einstellung in die Datenbank weiter. Unter Umständen gibt es noch weitere zwischengeschaltete

Stellen, die Fachaufsicht über Entscheider ausüben. Diese benötigen personenbezogene Daten zwar nicht, sie laufen aber bei ihnen durch, weil die Senatsverwaltung sie braucht.

Die Senatsverwaltung für Wirtschaft, Technologie und Frauen benötigt die personenbezogenen Daten jedoch nicht, soweit sie Kontrollaufgaben bei den geförderten Projekten ausübt, z.B. die Kontrolle des Mittelabflusses. Hier reicht es, dass sie die Projekte über Pseudonyme identifizieren kann. Sie braucht die personenbezogenen Daten allerdings für die Aufnahme in das sog. Begünstigtenverzeichnis. Es ist durch eine entsprechende rollenbasierte Zugriffssteuerung darauf hinzuwirken, dass die Dienstkräfte der Senatsverwaltung, die die Projekte steuern und kontrollieren, nur auf die pseudonymisierten Daten zugreifen können.

Europäische Stellen, die ebenfalls für Kontrollaufgaben und ggf. Aufgaben der Korruptionsbekämpfung Zugang zu den Daten erhalten, müssen sich in der Regel auf pseudonymisierte Daten beschränken. Die identifizierenden Daten wären im konkreten Einzel-(Verdachts-)fall explizit und mit Begründung anzufordern. Die wissenschaftliche Begleitforschung und planende Stellen benötigen für ihre Aufgaben nur anonymisierte Daten.

Die Leistungsbeschreibung zu der Software enthält auch die Anforderung eines Sicherheitskonzepts, das bisher jedoch noch nicht vorliegt.

2. Schwerpunkte

2.1 Datenmafia, Call-Center und Unschuldslämmer

Wer kennt nicht diese Situation zu Hause? Man sitzt beim Abendessen, das Telefon klingelt und am Telefon ist ein netter junger Mann, der ein interessantes Angebot unterbreitet. Angeboten wird die Teilnahme an einem Glücksspiel, ein günstiger Telefontarif oder eine besonders gewinnversprechende Finanzanlage. Möglich ist auch, dass der Anrufer daran erinnert, es sei wieder an der Zeit, Geld für einen wohltätigen Zweck zu spenden. Die Telefonnummer des Anrufers ist in der Regel unterdrückt, bei kritischen Nachfragen ist der nette junge Mann plötzlich gar nicht mehr so freundlich ... Die Anzahl der lästigen und unzulässigen Werbeanrufe, die einen „kalt erwischen" (Cold Calls), hat sich in den letzten Jahren deutlich erhöht. Leider muss man feststellen, dass sich Berlin zu einer Hochburg rechtswidrig arbeitender Call-Center entwickelt hat.

Das Zauberwort in der Call-Center-Szene lautet „Opt-in-Qualität" oder „Opt-in-Daten". Ein Datensatz hat Opt-in-Qualität, wenn die Betroffenen sich damit einverstanden erklärt haben, Werbeanrufe zu erhalten. Bei der großen Anzahl der angebotenen Opt-in-Dateien müsste man allerdings davon ausgehen, dass fast alle ausdrücklich mit Telefonwerbung einverstanden wären. Es liegt auf der Hand, dass diese Annahme nicht zutrifft. Wie ist dieses Phänomen jedoch zu erklären? Opt-in-Daten werden auf dem Markt von Datenhändlern angeboten und von den Call-Centern aufgekauft, wenn der Händler ihnen noch einmal bestätigt, dass der gekaufte Datensatz die hohen Weihen der Opt-in-Qualität erfüllt. Dies reicht den Call-Centern in der Regel aus. Eine Überprüfung des Datensatzes nimmt man sicherheitshalber nicht vor. So verkaufte der Adresshändler einem Lotterieunternehmen Opt-in-Daten für einen fünfstelligen Geldbetrag und später stellte sich heraus, dass der inzwischen in Polen untergetauchte Adresshändler nur Telefonbücher abgeschrieben hatte. In einem anderen Fall, in dem bei einer von uns durchgeführten Stichprobe kein Datum Opt-in-Qualität hatte, teilten uns die für den Adresshändler zuständigen niedersächsischen Kollegen mit, dass gegen den Betroffenen so viele Strafverfahren laufen, dass das von uns festgestellte Datenschutzdelikt von der Staatsanwaltschaft wohl kaum weiterverfolgt würde.

Auch bei den etwas seriöseren Adresshändlern haben die Daten selten Opt-in-Qualität. Viele Daten werden bei Glücksspielen akquiriert. Im Kleingedruckten und nicht im Text hervorgehoben findet sich der Hinweis, dass die Daten für Telefonwerbung verwendet werden. Der Einwilligungstext ist in der Regel so unbestimmt, dass die Betroffenen, selbst wenn sie den Text gelesen haben, nicht die Reichweite der Frage „Wer darf mich anrufen?" erkennen können. Bei der Akquise von „Opt-in-Daten" im Internet können die Adresshändler oft nicht einmal mit Sicherheit sagen, ob die Betroffenen selbst die Einwilligung gegeben haben.

Eine wirksame Opt-in-Erklärung setzt grundsätzlich Schriftlichkeit voraus. Die Einwilligung ist im Text hervorzuheben[27] und der Einwilligungstext muss ausreichend bestimmt sein. Eine generelle Einwilligung in Telefonwerbung ist demgegenüber unwirksam. Die konkret erfolgende Telefonwerbung muss sich im Rahmen der gegebenen Einwilligung bewegen. Legt man diese durch gefestigte Rechtsprechung definierten Kriterien zugrunde, dürfte nur ein Promillesatz der zurzeit im Markt befindlichen „Opt-in-Daten" Opt-in-Qualität haben.

Bei der Prüfung eines Call-Centers, das sich auf Lose der Süddeutschen Klassenlotterie spezialisiert hatte, stellten wir fest, dass wir nicht die einzigen Prüfer waren. Gleichzeitig prüften das Landeskriminalamt und der Zoll, u.a. wegen des Verdachts der Schwarzarbeit. Aufsichtsrechtliche Maßnahmen gegen Call-Center lassen sich insbesondere deshalb schwer durchsetzen, weil viele nur kurz am Markt sind und anschließend mit anderem Namen und mit neuem Management als neue juristische Person (teilweise auch an anderen Orten) weiterarbeiten. Das geprüfte Call-Center leitete in regelmäßigen Abständen im Zusammenwirken mit der Muttergesellschaft seine Insolvenz ein. Hierdurch ersparte man sich nicht nur die Probleme mit datenschutzrechtlicher oder gewerberechtlicher Aufsicht. Auch die Zahlung der Mitarbeitergehälter ließ sich so umgehen.

Wer ist verantwortlich für die immer weiter steigende Zahl der rechtswidrigen Cold Calls? Klassenlotterien oder große Telefongesellschaften, für die regelmäßig Werbung gemacht wird, würden die Verantwortung weit von sich weisen.

27 § 4 a Abs. 1 letzter Satz BDSG

Die Süddeutsche Klassenlotterie etwa hatte selbst keinerlei Verträge mit Call-Centern abgeschlossen, dies erledigte die zuständige Lotterieeinnahmestelle. Diese wiederum ließ sich von den Call-Centern bestätigen, dass keine Cold Calls durchgeführt werden. Die geforderten oder für die Rentabilität erforderlichen Fallzahlen setzten allerdings rechtswidrige Werbeanrufe nahezu zwingend voraus. Nach ähnlichem Muster laufen die Werbeanrufe für die Telekommunikationsbranche ab. Kurz zusammengefasst kann man sagen, dass sich die großen Unternehmen und Institutionen gerne die Hände in Unschuld waschen.

In vielen Fällen liegt aber eine Auftragsdatenverarbeitung vor, wenn etwa eine Telefongesellschaft ihre Kundschaft anrufen lässt, um sie in einen neuen Tarif zu drängen (auch dies ist ohne Einwilligung rechtswidrig). Dabei werden zwar die Kundendaten dem Call-Center zur Verfügung gestellt. Dieses muss sich aber vertraglich verpflichten, die Daten nur entsprechend den Weisungen des Auftraggebers zu verarbeiten. Er hat die Rechtmäßigkeit der Datenverarbeitung beim Auftragnehmer durch entsprechende Verträge und Kontrollen sicherzustellen. Die Einschaltung von Call-Centern ist insbesondere dann üblich, wenn Produkte vermarktet werden, die überflüssig sind (Glücksspiel) oder für die ein harter Wettbewerb besteht. Nachdem die Umsätze im Zeitungsgewerbe zurückgegangen sind, haben beispielsweise neuerdings viele Zeitungen damit begonnen, per Telefon für neue Abonnements zu werben.

Anfang des Jahres hat der illegale Adresshandel eine neue sogar strafrechtlich relevante Qualität erreicht, als plötzlich bundesweit Datensätze mit Bankverbindung angeboten wurden. Die Ermittlungen der Staatsanwaltschaft hierzu sind noch nicht in allen Fällen abgeschlossen. Diese illegal vermarkteten Daten betrafen viele Betroffene, die an einer staatlichen Klassenlotterie teilgenommen hatten. Seit Anfang 2008 ist der Verkauf von Lotterie-Losen über das Telefon verboten. Ein Großteil der Call-Center dürfte allerdings auch für größere Unternehmen wie z.B. die Deutsche Telekom AG Auftragsdatenverarbeitung betrieben haben. Mit Hilfe der vorhandenen Kontonummern hofften die Call-Center, neue Geschäftsfelder zu erschließen.

Im August übergab uns der Verbraucherzentrale Bundesverband e. V. (vzbv) Datenträger mit rund sechs Millionen Datensätzen, die er von einem Dritten erhalten hatte. Wir haben Strafantrag gestellt und die Datenträger der Staatsanwaltschaft zugeleitet. Gegen den bald darauf festgenommenen

Adresshändler hat das Amtsgericht Münster lediglich einen Strafbefehl über 900 Euro verhängt.

In einem besonders krassen Fall gaben sich die Anrufer als Datenschützer aus, die davor warnten, die Daten der Angerufenen seien im Internet auffindbar. Für 60 Euro würde man einen umfangreichen Schutz anbieten. Zum Beweis für die Datenschutzproblematik nannte man den Betroffenen die genaue Bankverbindung. Die Täter benutzten zuerst die Daten der über 70-Jährigen, weil sie davon ausgingen, dass diese ängstlicher seien und sich eher zu einem Vertragsschluss verleiten ließen. Als Verbraucherschützer durch eine einstweilige Verfügung das Verfahren stoppten, wurde ein neues Unternehmen gegründet, welches zwar die gleiche Masche anwandte. Die Anrufer nannten sich jetzt jedoch „Verbraucherschützer", offenbar eine kleine Rache wegen der Untersagungsverfügung. Man hatte inzwischen auch dazugelernt. So gaben die „Verbraucherschützer" keine Firmenadresse mehr an. Sie waren nur noch über Fax erreichbar. Offenbar war bei beiden Unternehmen die erhoffte Akquisequote jedoch nicht groß genug. So ging man dazu über, den Betroffenen unter Verweis auf das Telefongespräch fertige Verträge (Mitgliedschaften) zuzuleiten, auch wenn die Betroffenen am Telefon nur die Zusendung von Informationsmaterial akzeptiert hatten. Wir haben gegen die Verantwortlichen beider Unternehmen Strafantrag gestellt. Angesichts der Schnelllebigkeit der „Branche" sind langfristig angelegte aufsichtsbehördliche Maßnahmen hier fehl am Platz.

Inzwischen wurde das Geschäft mit den illegalen Datensätzen weiter verfeinert. Call-Center kamen zu dem Ergebnis, dass man sich die arbeitsintensiven Cold Calls sparen kann. So versandte das Call-Center eines großen deutschen Medienunternehmens ohne vorheriges Telefongespräch gleich fertige Verträge für eine Clubmitgliedschaft. Da man über die Bankverbindung der Betroffenen verfügte, konnte man das Geld per Lastschrift abbuchen. Als die Sache aufflog, hat der Medienkonzern „eine Rückabwicklung" der angeblichen Verträge akzeptiert.

Die Bundesregierung hat im Dezember die beim sog. Datenschutzgipfel am 4. September gegebene Zusage insoweit eingelöst, als sie den Entwurf zu einer weiteren Änderung des Bundesdatenschutzgesetzes (BDSG) beschlossen hat[28],

28 BR-Drs. 4/09

der die überfällige Streichung des „Listenprivilegs“ für den Adresshandel vorsieht. Künftig setzt danach der Handel mit Adressdaten in aller Regel die ausdrückliche schriftliche Einwilligung der Betroffenen voraus. Allerdings enthält der Regierungsentwurf nicht die zwingend gebotene Pflicht zur Kennzeichnung über die Herkunft der Daten. Wer Werbebriefe erhält, sollte jeweils durch einen kurzen Zusatz auf die Datenquelle hingewiesen werden. Nur so lässt sich der illegale Datenhandel auch praktisch erkennen und eindämmen. Dieser Mangel des Gesetzentwurfs wird hoffentlich – neben anderen Defiziten – während der parlamentarischen Beratung noch behoben.

Es bleibt zu hoffen, dass durch die neuen gesetzlichen Regelungen das rechtswidrige Verhalten der Call-Center, ihrer Auftraggeber und der Adresshändler eingeschränkt werden kann. Der Gesetzgeber sollte zudem prüfen, ob die Regelung zur Auftragsdatenverarbeitung dem illegalen Datenhandel nicht Vorschub leistet. Überdies ist eine Pflicht zur Kennzeichnung der Herkunft von Daten wichtig, um die Rechtmäßigkeit von Werbeschreiben überprüfen zu können.

2.2 Soziale Netzwerke – Die Illusion der Intimität

Soziale Netzwerkdienste (Online- oder Social Communities) bieten den Teilnehmenden Interaktionsmöglichkeiten auf der Basis von selbst erstellten persönlichen Profilen. Über die große Popularität, aber auch die sich abzeichnenden Risiken für die Privatsphäre haben wir im letzten Jahr berichtet[29]. Die Nutzerzahlen dieser Netzwerke sind national und international weiter stark angestiegen. Nicht nur bei Jugendlichen ist ihre Beliebtheit ungebrochen. Die Entwicklung hat dazu geführt, dass auch „privateste Daten“ einzelner Personen – einschließlich großer Mengen digitaler Fotos und Videos – in einem bisher unbekannten Maß öffentlich – und global – zugänglich sind.

Für die Nutzenden besteht die Gefahr, dass sie die Kontrolle über die Verwendung ihrer Daten verlieren, wenn sie erstmals im Netzwerk veröffentlicht sind. Viele sind sich nicht darüber im Klaren, dass die Veröffentlichung ihrer

29 JB 2007, 12.3

persönlichen Daten in einem sozialen Netzwerk eben nicht dasselbe ist wie die Mitteilung dieser Informationen unter Freunden von Angesicht zu Angesicht: Je nach den Umständen des Einzelfalls können Profildaten tatsächlich für alle Mitglieder eines sozialen Netzwerkdienstes verfügbar sein – deren Anzahl kann je nach Anbieter in die Millionen gehen. Zudem kann sich jede Person mit geringem Aufwand bei dem betreffenden Netzwerk anmelden. Soziale Netzwerke bieten deshalb nur die Illusion der Intimität.

Auch Nutzende, die von den vielfach zur Verfügung gestellten Einstellmöglichkeiten zur Privatsphäre Gebrauch machen, müssen mit bestimmten Restrisiken leben. So eröffnen zwar viele Anbieter die Möglichkeit, den Zugang zu Fotos auf registrierte Freunde zu beschränken. Häufig ist aber nicht bekannt, dass sich eine solche Zugangsbeschränkung gleichwohl von der Situation unterscheidet, bei der man Freunden ein Fotoalbum im heimischen Wohnzimmer zeigt. Es ist nämlich so, als würde man jedem dieser Freunde eine digitale Kopie des eigenen Fotoalbums in die Hand drücken. Denn derzeit existiert praktisch keine Möglichkeit zu verhindern, dass Profildaten jeder Art durch andere zugriffsberechtigte Mitglieder des Netzwerkes (oder im Fall von Sicherheitslücken auch durch unbefugte netzwerkfremde Dritte) kopiert werden können. Dritte können diese Daten dann grundsätzlich für beliebige Zwecke weiterverwenden, z.B. indem sie sie an anderer Stelle im Internet veröffentlichen oder zum Aufbau von Persönlichkeitsprofilen verwenden. Digitale Bilder können zudem manipuliert oder in einen negativen Kontext gestellt werden.

Nationale und internationale Gremien der Datenschutzbeauftragten haben sich auf unsere Initiative mit Fragen rund um soziale Netzwerke befasst. So hat der Düsseldorfer Kreis (das Gremium der obersten Aufsichtsbehörden für die Privatwirtschaft) in einem Beschluss zur datenschutzkonformen Gestaltung sozialer Netzwerke Stellung bezogen[30] und daran erinnert, dass Anbieter in Deutschland zur Einhaltung des hiesigen Regulierungsrahmens zum Datenschutz verpflichtet sind. Dies betrifft insbesondere folgende Einzelfragen:

Anbieter sozialer Netzwerke sind verpflichtet, ihre Mitglieder umfassend über die Verarbeitung ihrer personenbezogenen Daten einschließlich vorhandener Wahl- und Gestaltungsmöglichkeiten zu unterrichten. Dazu zählen vor allem

30 Beschluss vom 17./18. April 2008, vgl. Dokumentenband 2008, S. 34

Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in persönlichen Profilen einhergehen können, sowie eine Aufklärung darüber, wie Nutzende mit personenbezogenen Daten Dritter verfahren müssen. Eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke ist nach dem Telemediengesetz (TMG) nur zulässig, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten ist den Betroffenen nach dem BDSG mindestens eine Widerspruchsmöglichkeit einzuräumen. Die Aufsichtsbehörden empfehlen den Anbietern, die Nutzenden selbst darüber entscheiden zu lassen, ob und ggf. welche Profil- oder Nutzungsdaten zur zielgerichteten Werbung genutzt werden.

Eine Speicherung personenbezogener Nutzungsdaten über das Ende der Verbindung hinaus ist nur gestattet, soweit diese Daten zur Abrechnung gegenüber den Nutzenden erforderlich sind. Für die vorauseilende Speicherung von Nutzungsdaten für eventuelle zukünftige Strafverfolgungszwecke gibt es keine Rechtsgrundlage. Eine solche Speicherung wird auch nicht durch die Bestimmungen zur Vorratsdatenspeicherung[31] vorgeschrieben.

Anbieter sind nach dem TMG darüber hinaus verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Das gilt unabhängig davon, ob sich die Nutzenden gegenüber dem Anbieter des sozialen Netzwerks selbst mit ihren Echtdaten identifizieren müssen. Dieser muss auch die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit treffen und dabei insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem Angebot verhindern.

Des Weiteren fordern die Aufsichtsbehörden die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzenden möglichst umfassend geschützt wird. Diese Standardeinstellungen sind besonders restriktiv zu fassen, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf nur vorgesehen werden, soweit die Nutzenden ausdrücklich eingewilligt haben. Schließlich ist den Nutzenden die Möglichkeit einzuräumen, ihre Profile auf einfache Weise selbst zu löschen. Zusätzlich empfehlen die Aufsichtsbehörden den

31 Vgl. 6.1

Anbietern die Einführung von Verfallsdaten oder zumindest von automatischen Sperrungen, die von den Nutzenden selbst festgelegt werden können.

Bereits im März hat die unter unserem Vorsitz tagende Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation einen Bericht und Empfehlungen zum Datenschutz in sozialen Netzwerken verabschiedet[32]. Darin weist die Arbeitsgruppe auf Risiken für die Privatsphäre bei der Nutzung sozialer Netzwerkdienste hin und richtet Empfehlungen zur datenschutzkonformen Gestaltung dieser Dienste an Gesetzgeber, Anbieter und Nutzende. Insbesondere weist die Arbeitsgruppe auf Risiken hin, die sich mit der Veröffentlichung von Fotos ergeben können. Sie können zu universellen biometrischen Identifikatoren innerhalb eines Netzwerks oder sogar über Netzwerke hinweg werden. Das automatisierte Auffinden von Bildern, auf denen dieselbe Person abgebildet ist, wird bereits jetzt durch die verfügbaren Technologien zur Gesichtserkennung erleichtert. Ist einmal ein Name zu einem Bild hinzugefügt, kann dies auch die Privatsphäre und Sicherheit anderer pseudonymer Nutzerprofile gefährden, z.B. bei Profilen in Kontaktanzeigen, die häufig Bilder, aber nicht den wirklichen Namen der Betroffenen enthalten. Dem Gesetzgeber empfiehlt die Arbeitsgruppe u.a. die Einführung einer Verpflichtung für Anbieter sozialer Netzwerkdienste zur Benachrichtigung der Nutzenden bei Sicherheitsvorfällen sowie die Verbesserung der Integration von Datenschutzkenntnissen im Bildungssystem.

Gestützt auf diese Vorarbeiten hat die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre eine Entschließung zum Datenschutz in sozialen Netzwerkdiensten gefasst[33], die maßgeblich auf unseren Vorschlag zurückgeht.

Der Schutz der Privatsphäre in sozialen Netzwerken war auch Thema unserer Veranstaltung anlässlich des 2. Europäischen Datenschutztages[34] sowie eines Internationalen Symposiums, das wir am Rande der 30. Internationalen Datenschutzkonferenz veranstaltet haben[35].

32 Vgl. Dokumentenband 2008, S. 129

33 Straßburg, 15.–17. Oktober 2008, vgl. Dokumentenband 2008, S. 123

34 am 28. Januar 2008, vgl. 17.4

35 Vortragsunterlagen sind teilweise abrufbar unter http://www.datenschutz-berlin.de/content/berlin/berliner-beauftragter/veranstaltungen/symposium-2008.

Teilnehmenden an sozialen Netzwerkdiensten können wir nach dem derzeitigen Kenntnisstand folgende Empfehlungen geben, um die mit der Nutzung sozialer Netzwerke verbundenen Risiken für die Privatsphäre zu begrenzen:

- **Informieren Sie sich über den Anbieter des Dienstes** und darüber, welchen gesetzlichen Bestimmungen zum Datenschutz dieser Anbieter unterliegt. Dies ist wichtig, weil das Datenschutzniveau in verschiedenen Ländern nach wie vor sehr unterschiedlich ist und ein Anbieter in der Regel dem Rechtsrahmen des Landes unterliegt, in dem er seinen Sitz hat.
- **Seien Sie mit der Veröffentlichung eigener personenbezogener Daten** in sozialen Netzwerken **zurückhaltend**. Insbesondere Minderjährige sollten vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen. Denken Sie darüber nach, ob Sie mit den Informationen oder Bildern später konfrontiert werden möchten, z.B. bei einer Bewerbung um einen Arbeitsplatz. Laut Umfragen machen Personalverantwortliche in Unternehmen zunehmend von sozialen Netzwerkdiensten Gebrauch, um Informationen aus Bewerbungsunterlagen zu verifizieren oder zu ergänzen.
- **Nutzen Sie Pseudonyme** statt Ihres echten Namens, wo immer dies sinnvoll ist. Auch das darf Sie aber nicht zur Sorglosigkeit beim Umgang mit den eigenen Daten oder Bildern verleiten. Bedenken Sie, dass Dritte in der Lage sein könnten, Ihr Pseudonym aufzudecken. Diese Gefahr besteht beispielsweise dann, wenn Ihr Nutzerprofil Fotos enthält, auf denen Sie deutlich zu erkennen sind. Nutzen Sie für die Anmeldung eines pseudonymen Profils möglichst eine separate E-Mail-Adresse. Einige Anbieter ermöglichen ihren Mitgliedern einen Abgleich mit deren eigenem E-Mail-Adressbuch. Dadurch könnten diese Ihr Pseudonym aufdecken.
- **Respektieren Sie die Privatsphäre anderer Personen.** Überlegen Sie sich, bevor Sie Daten über Dritte veröffentlichen, ob Sie selbst mit einer Veröffentlichung gleichartiger Daten einverstanden wären, die Sie betreffen. Wir empfehlen, vor der Veröffentlichung von Daten über Dritte die Einwilligung der Betroffenen einzuholen. Bedenken Sie, dass die unbefugte Veröffentlichung von Bildern nach einer kaum bekannten Vorschrift im Kunsturhebergesetz mit Freiheits- oder Geldstrafe geahndet werden kann[36].

36 Vgl. § 33 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie (KunstUrhG)

- **Begrenzen Sie die Verfügbarkeit von Informationen** über sich selbst soweit wie möglich. Informieren Sie sich darüber, welche Einstellmöglichkeiten Ihr Anbieter hierzu bereitstellt, und machen Sie von ihnen Gebrauch. Schließen Sie eine Indexierung durch Suchmaschinen aus, soweit der Anbieter dies nicht ohnehin tut oder eine Indexierung nur aufgrund Ihrer Einwilligung ermöglicht.
- **Informieren Sie sich darüber, ob und wie der Anbieter Ihre Profil- oder Nutzungsdaten verarbeitet.** Widersprechen Sie der Nutzung für zielgerichtete Werbung.
- **Nutzen Sie keine Identifizierungsdaten** (Login und/oder Passwort), die Sie auch bei anderen Diensteanbietern (z.B. E-Mail oder Online-Banking) verwenden.
- **Trennen Sie Daten** aus verschiedenen „sozialen Rollen", z.B. aus Berufs- und Privatleben. Nutzen Sie dafür unterschiedliche Profile oder Plattformen unterschiedlicher Anbieter.
- Viele Anbieter privilegieren bei den Einstellungen für Zugriffsbefugnisse Dritter auf Profildaten „registrierte Freunde" in starkem Maße. **Überlegen Sie, bevor Sie eine Freundschaftseinladung bestätigen,** ob Sie der betreffenden Person wirklich all diese Daten zugänglich machen wollen.
- Soziale Netzwerke öffnen sich immer mehr für andere Web-Dienste, z.B. durch die Möglichkeit, Programme aus dritter Hand in die eigenen Profile zu integrieren. **Seien Sie sich bewusst,** dass dies oft zu einer Übermittlung Ihrer personenbezogenen Daten an diese Dritten führt. Dies sollten Sie nur bei vertrauenswürdigen Drittanbietern gestatten.
- **Das Internet vergisst nichts!** Es gibt bereits heute Auskunfteien und andere (Daten-)Händler, die legal oder illegal personenbezogene (Risiko-)Profile erstellen. Anbieter sozialer Netzwerke können nicht verhindern, dass auch veraltete Inhalte der selbst angelegten Profile in diesen Profilen auftauchen. Interessenten können Personalverantwortliche in Unternehmen, Banken oder Versicherungen sein.

Mit dem Anbieter der Sozialen Netzwerke „SchülerVZ", „StudiVZ" und „MeinVZ", die wir überprüft haben,[37] wurden Ergebnisse erzielt, die die Nutzenden in die Lage versetzen, ihre Daten in ausreichendem Maß zu schützen,

37 JB 2007, 12.3; JB 2006, 10.2.4

ohne den wirtschaftlichen Erfolg der Plattformen zu verhindern. So kann „feingranular“ eingestellt werden, welche Inhalte eines Profils für wen zugänglich sein sollen, basierend auf einem abgestuften Vertrauenskonzept der untereinander vernetzten Nutzenden. Neben der grundsätzlichen Empfehlung, in sozialen Netzwerken unter Pseudonym aufzutreten, raten wir den Nutzenden, die Möglichkeiten zur Einschränkung der Sichtbarkeit einzusetzen, bevor sensitive Profildaten angegeben werden. Der Anbieter der Plattformen hat zugesagt, dies aktiv zu unterstützen, indem er insbesondere neue Mitglieder über die Schutzmöglichkeiten im Rahmen einer „Privacy-Tour“ informiert. Zudem konnte erreicht werden, dass die Nutzung der Plattformen unter Pseudonym zumindest nicht unterbunden wird und entgegen dem ursprünglichen Vorhaben des Anbieters keine Vorratsdatenspeicherung der Aktivitäten der Nutzenden erfolgt. Eine kurzfristige Speicherung für die Dauer von maximal fünf Tagen muss jedoch zugestanden werden, um die technische Sicherheit der Plattformen bei Angriffen aus dem Internet gewährleisten zu können. Die tatsächliche Praxis bezüglich Pseudonymen und Nutzungsdatenspeicherung sollte zwar auch unmissverständlich in den Allgemeinen Geschäftsbedingungen (AGB) und der Datenschutzerklärung dargelegt werden. Die derzeitige Lösung, die die aktuelle, rechtskonforme Praxis auf verlinkten Informationsseiten erklärt, kann jedoch hingenommen werden. Wünschenswert wäre zudem, die für neue Nutzende vorgewählten Datenschutzeinstellungen restriktiver zu gestalten, als dies der Betreiber momentan als realisierbar ansieht.

Wer soziale Netzwerke betreibt, muss die Nutzenden darauf hinweisen, welche Risiken auf solchen Plattformen bestehen und wie sie zu begrenzen sind. Wer eine solche Plattform nutzt, sollte nicht jedem „Freund“ alles über sich „auf die Nase binden“. Das würde man auch im wirklichen Leben nicht tun.

2.3 Wartung und Fernwartung von informationstechnischen Systemen

Seit der Einführung von Rechentechnik ist deren Wartung für einen störungsfreien Betrieb unverzichtbar. Mit der Verfügbarkeit schneller Datenübertragungswege wurde es möglich, Wartungsvorgänge auch aus der Ferne auszuführen. Somit gewann die Fernwartung immer mehr an Bedeutung. Bei der Wartung und Fernwartung sollte zwar der Zugang zu personenbezogenen Daten vermieden werden. Er lässt sich jedoch nicht immer ausschließen. Da Wartung und Fernwartung meistens von spezialisierten Fremdunternehmen durchgeführt werden, stellt sich die Frage nach ihrer datenschutzrechtlichen Einordnung. Das Berliner Datenschutzgesetz (BlnDSG) berücksichtigt ebenso wie das Brandenburgische Datenschutzgesetz (BbgDSG), aber im Gegensatz zu allen anderen Landesdatenschutzgesetzen, dass Wartung oder Fernwartung kein „Auftrag" zur Verarbeitung personenbezogener Daten ist, sondern diese wenn möglich vermieden werden sollte[38]. Auch das Bundesdatenschutzgesetz erwähnt die Wartung explizit, behandelt sie jedoch analog zur Auftragsdatenverarbeitung[39].

Nach dem BlnDSG ist „die Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung und Reparatur oder der Austausch von Hardware". Die Fernwartung ist danach „Wartung der Hard- und Software von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtung zur Datenübertragung vorgenommen wird". Sie betrifft Telefonanlagen ebenso wie PCs, Server und ganze Rechenzentren.

Man kann generell drei Formen der Wartung unterscheiden: Die Wartung durch eigenes Personal der Daten verarbeitenden Stelle, die Wartung vor Ort durch externe Fachkräfte und die Fernwartung durch externe Fachkräfte, der wir hier besondere Aufmerksamkeit widmen.

38 § 3 a BlnDSG, § 11 a BbgDSG
39 § 11 Abs. 5 BDSG

Welche Form der Wartung ist angemessen?

Wenn möglich sollte die Wartung durch eigenes Personal erfolgen, weil damit die Kontrolle durch die einsetzende Stelle am besten gewährleistet ist. Häufig ist jedoch spezielles Fachwissen erforderlich, das bei der Daten verarbeitenden Stelle nicht vorgehalten werden kann, was die Beauftragung eines externen Dienstleistungsunternehmens erforderlich macht. Der Einsatz von Fernwartung birgt allerdings ein höheres Risikopotenzial, weil eine wirksame Kontrolle nur begrenzt möglich ist und es damit sehr auf das Vertrauen ankommt, das man dem Dienstleistungsunternehmen entgegenbringt. Fernwartung sollte deshalb auf ein unablässiges Mindestmaß reduziert und in ein Sicherheitskonzept explizit aufgenommen werden. Es ist immer genau abzuwägen, ob der erwartete wirtschaftliche Vorteil die Probleme hinsichtlich der Sicherheit und der damit zusätzlich zu treffenden Maßnahmen aufwiegt.

In bestimmten Fällen ist der Einsatz von Fernwartung gesetzlich ausgeschlossen. Im medizinischen Sektor verbietet die ärztliche Schweigepflicht grundsätzlich einen entsprechenden Einsatz, sofern die Kenntnisnahme der Daten durch das Wartungspersonal nicht wirksam verhindert werden kann, z.B. durch die Verwendung einer Speicherverschlüsselung.[40]

Fernwartung birgt ein höheres Risikopotenzial als Wartung vor Ort, weil eine wirksame Kontrolle nur begrenzt möglich ist. Daher sollte sie nur in unerlässlichen Ausnahmen erfolgen, wenn der Dienstleister vertrauenswürdig ist und wenn die Risiken in einem Sicherheitskonzept auf ein tragbares Maß begrenzt werden.

Rechtlicher Rahmen der Wartung und Fernwartung

Öffentliche Stellen des Landes Berlin haben bei der Beauftragung und Durchführung der Wartung oder Fernwartung von IT-Systemen, mit denen personenbezogene Daten verarbeitet werden, § 3 a BlnDSG zu beachten.

Danach ist schon bei der Gestaltung von Datenverarbeitungssystemen darauf zu achten, dass die Wartung datenschutzfreundlich durchgeführt werden kann. Sie

40 Vgl. dazu auch 8.2.5

sollte möglichst ohne personenbezogene Daten auskommen. Sofern dies nicht möglich ist, müssen technische und organisatorische Maßnahmen durchgeführt werden, um sicherzustellen, dass der Zugriff auf die Daten auf das unbedingt erforderliche Maß beschränkt bleibt. Die im Gesetz formulierten Anforderungen betreffen die Autorisierung des Wartungspersonals, die Kontrollierbarkeit und Revisionsfähigkeit der Wartungsvorgänge durch die Daten verarbeitende Stelle, die Verhinderung unbefugter Entfernung und Übertragung von Daten sowie des unbefugten Aufrufs und der unbefugten Änderung von Datenverarbeitungsprogrammen bei der Wartung.

Wie die Auftragsdatenverarbeitung nach § 3 BlnDSG darf die Wartung oder Fernwartung nach § 3 a BlnDSG nur aufgrund schriftlicher Vereinbarungen erfolgen, die Art und Umfang regeln sowie die Rechte und Pflichten von Auftraggeber und Auftragnehmer, die Protokollierung der Wartungsvorgänge beim Auftraggeber, die Zweckbindung der verwendeten personenbezogenen Daten, das Verbot der Weitergabe der Daten an Dritte, die Löschung der Daten nach Beendigung der Wartung, die Verschlüsselung der Daten bei eventuellen Datenübertragungen (z.B. im Rahmen der Fernwartung). Es muss außerdem verabredet werden, dass nur der Auftraggeber eine Fernwartung auslösen kann und dass dessen Systemverwaltung bei der Fernwartung anwesend ist. Da weiterhin § 5 BlnDSG zu beachten ist, sind die konkreten Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu konkretisieren. Die Umsetzung des Katalogs der schriftlich zu regelnden Maßnahmen entfällt, wenn nur ein Zugriff auf verschlüsselte, anonymisierte oder pseudonymisierte Daten möglich ist und damit sichergestellt wird, dass Betroffene bei der Wartung nicht identifiziert werden können.

Bei privaten Organisationen bildet das BDSG die Rechtsgrundlage, sofern keine spezialrechtlichen Regelungen gelten. Nach § 11 Abs. 5 BDSG gelten für die Überprüfung und Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen die Regelungen zur Auftragsdatenverarbeitung nach § 11 Abs. 1 - 4 BDSG. Für die technischen und organisatorischen Maßnahmen gilt § 9 BDSG einschließlich seiner Anlage.

Werkzeuge zur Fernadministration

Auf dem Markt existieren diverse Anwendungen, die für eine Fernwartung verwendet werden können. Einige sind als Open-Source-Produkte frei verfügbar,

andere als kommerzielle Software. Aber auch Betriebssysteme und betriebssystemnahe Software halten Komponenten zur Fernwartung bereit.

Ein Open-Source-Produkt zur Fernadministration ist Virtual Network Computing (VNC). VNC ist in mehren Varianten von verschiedenen Anbietern erhältlich. Es unterstützt die Betriebssysteme Windows und Linux. Mit VNC kann der Bildschirminhalt eines entfernten Rechners auf einem lokalen Rechner angezeigt werden und der entfernte Rechner mit Tastatur und Maus des lokalen Rechners gesteuert werden. Somit kann der entfernte Rechner aus der Ferne bedient werden. Auf diese Weise kann aus der Ferne Software installiert und es können Fehler behoben werden. Andererseits kann solche Software auch als Spionage-Software wirken. Um das zu verhindern, sind Maßnahmen zu ergreifen, mit denen der entfernte Rechner gegen den unbemerkten und gegen seinen Willen erfolgenden VNC-Einsatz geschützt werden kann. Als zweites Beispiel ist der Fernadministrationsteil der Windows-Betriebssysteme ab Version XP zu nennen.

Die Nutzung von Software zur Fernadministration ist in den Standardeinstellungen in den meisten Fällen nicht ohne Datenschutzrisiken. Eine Justierung der Werkzeuge für die Belange des Datenschutzes ist daher oft unumgänglich. Folgende Voraussetzungen für eine Fernadministration müssen erfüllt werden:
Sie ist im infrastrukturellen Sicherheitskonzept, ggf. auch in betroffenen verfahrensspezifischen Sicherheitskonzepten zu betrachten und zu bewerten. Sie muss jeweils durch die Nutzenden vor Sitzungsbeginn gestattet und jederzeit durch sie unterbrochen und überwacht werden können. Es sind Maßnahmen zu treffen, die eine Nutzung der Fernadministration durch Unbefugte ausschließen. Ein Beispiel für eine solche Maßnahme ist die Verwendung von Verschlüsselungsprotokollen bei der Nutzung von Netzwerken, die nicht unter voller Kontrolle der administrierenden Stelle stehen (z. B. Mietleitungen).

2.4 Videoüberwachung – Big Brother überall?

Technische Entwicklung der Videoüberwachung

Der Einsatz von Videoüberwachungssystemen hat sowohl im öffentlich zugänglichen als auch im privaten Bereich weiter stark zugenommen. Dies hat mehrere Gründe: Zum einen sind die Anschaffungskosten für den Erwerb von Überwachungstechnik rapide gesunken, da es mittlerweile am Markt eine Vielzahl konkurrierender Hersteller gibt, die Videoüberwachungsanlagen für unterschiedlichste Einsatzmöglichkeiten anbieten. Zum anderen wird die Videotechnik immer leistungsfähiger und damit auch vielfältiger einsetzbar. So gibt es Videokameras mit Weitwinkel- und Zoom-Funktionen, die gestochen scharfe Bilddaten in Panorama-Format liefern, dabei aber so klein sind wie ein Stecknadelkopf. Sogenannte intelligente Kameras können anhand biometrischer Merkmale bestimmte Personen identifizieren. Andere wiederum erkennen vom normalen Bewegungsablauf eines beobachteten Menschen abweichende Bewegungen (z. B. schnelles Laufen, Sturz, schwankender Gang usw.) und speichern nur diese Sequenzen zur späteren Auswertung.

Darüber hinaus schreitet die Vernetzung von Kameras und Kamerasystemen weiter voran. Immer mehr Kameras besitzen inzwischen eine WLAN-Funktion und können Bilder über den DSL-Anschluss direkt ins Internet schicken. Da einige Kameras auch über einen GPS-Empfänger verfügen und die Bilder mit Positionsdaten versehen werden können, sind die Fotos später auch auf Online-Landkarten im Internet sichtbar.

Nicht immer steht bei diesen technischen Neuerungen die gezielte Personenüberwachung im Vordergrund. Dennoch wird aufgrund des inzwischen geringen Kostenaufwands, der einfachen Installation und der leichten Bedienbarkeit das Beobachten von Personen mit Kameras immer attraktiver. Bedingt durch die enorme Vielfalt der technischen Möglichkeiten werden oftmals die Persönlichkeitsrechte der beobachteten Personen nicht berücksichtigt und treten in den Hintergrund. In vielen Fällen verschwimmen beispielsweise die Grenzen zwischen der Darstellung allgemeiner Landschaftsaufnahmen, auf denen Menschen nur als „Beiwerk“ zu sehen sind, und dem gezielten Voyeurismus und Ausspionieren von Verhaltensmustern betroffener Personen.

Schon seit langer Zeit wird auf politischer Ebene und in den Medien kontrovers darüber diskutiert, ob und ggf. in welchem Umfang der zunehmende Einsatz von Videoüberwachungstechnik tatsächlich ein geeignetes Mittel ist, um Straftaten aufzuklären – präventiv wirkt sie allenfalls bei bestimmten Straftaten wie z.B. Sachbeschädigung durch Graffiti. Die trotz Videotechnik anhaltenden Angriffe auf Bedienstete im öffentlichen Nahverkehr belegen, dass die abschreckende Wirkung von Videokameras oft überschätzt wird.

Dennoch ist die „videotechnische Aufrüstung" durch Geschäfte und Privatpersonen in jüngster Vergangenheit sprunghaft angestiegen. Bürgerinnen und Bürger reagieren deswegen zunehmend sensibler auf Kameras, die sie im öffentlich zugänglichen oder im privaten Bereich entdecken. In den vielen Beschwerden, die wir zu diesem Thema erhalten haben, werden wir nach der Rechtmäßigkeit und der Notwendigkeit solcher Maßnahmen gefragt und entweder um allgemeine Auskunft zur Rechtslage oder konkrete Unterstützung im Einzelfall gebeten.

Videoüberwachung im Einzelhandel

Einen Schwerpunkt bildet dabei die Videoüberwachung in Geschäften: Nicht nur Außenfassaden und Geschäftsräume, in denen Kundinnen und Kunden verkehren, werden überwacht. Kameras werden oft gezielt in Kassenbereichen installiert. Hier besteht die Gefahr, dass die Eingabe von PIN-Nummern in das EC-Lesegerät registriert wird. Um eine Kamerabeobachtung auszuschließen, verfügen die meisten Lesegeräte deshalb über einen kleinen Sichtschutz am Display und sind schwenkbar. Da dies aber keinen absoluten Schutz vor fremden Blicken bietet, empfiehlt es sich grundsätzlich, bei der Eingabe der PIN-Nummer das Display mit der Hand vor den Blicken Dritter abzudecken.

Immer häufiger werden Kameras auch zur gezielten Personalüberwachung eingesetzt, wobei auch Pausen- oder Umkleidebereiche ins Visier kommen. Teilweise werden Minikameras in Rauchmeldern oder in der Deckenverkleidung von Geschäften installiert. Für die Beschäftigten gibt es oft keine Möglichkeit, sich der Erfassung durch Kameras zu entziehen. Arbeitgeber führen in erster Linie den Schutz ihres Personals vor Übergriffen und den Diebstahlschutz als Gründe für die Überwachung an. Der eigentliche Grund ist aber häufig die Leistungs- und Verhaltenskontrolle der Beschäftigten durch die Geschäftsführung. Dabei kontrolliert sie auch das Verhalten ihrer Angestellten gegenüber

den Kundinnen und Kunden, die korrekte Abrechung bei Bezahlvorgängen oder die Einhaltung von Pausenzeiten. Viele solcher Kameras werden daher heimlich installiert.

Eine heimliche Kamerainstallation ist jedoch ohne ein konkretes Verdachtsmoment stets rechtswidrig. Nach § 6 b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Diese Vorgabe kann am einfachsten in Form eines Schildes umgesetzt werden (**„Achtung! Dieses Geschäft wird videoüberwacht"**). Dabei müssen Kundinnen und Kunden, die das Geschäft betreten, vor Eintritt in den Erfassungsbereich der Kamera auf sie hingewiesen werden. Des Weiteren ist auf dem Schild die verantwortliche Stelle (z.B. Geschäftsführung, Sicherheitsdienst) zu nennen, bei der ausführliche Informationen erfragt werden können (z.B.: Welchem Zweck dient die Überwachung? Wie lange bleiben die Bilddaten gespeichert? Wer hat Zugriff darauf?).

Beschäftigte sollten diese ausführlichen Informationen vor Installation einer Videoüberwachungsanlage schriftlich von ihrer Geschäftsführung erhalten. Der Arbeitgeber sollte seine Angestellten über den Überwachungszweck, die Speicherdauer der Bilddaten und die Zugriffsmöglichkeiten auf die Daten in Kenntnis setzen. Dieser Zugriff und damit das Sichten und Auswerten des Bildmaterials darf nur bei begründetem Tatverdacht und nur im Zusammenwirken von Geschäftsführung und Betriebsrat erfolgen.

Bei einer Videoüberwachung und -aufzeichnung in nicht-öffentlichen Räumen ist § 6 b BDSG nicht anwendbar. Wenn ein Firmengelände nur durch Zutrittskontrollanlagen zu betreten und somit für Unbefugte nicht zugänglich ist, findet § 28 BDSG Anwendung. Darüber hinaus sind arbeitsrechtliche Vorgaben zu beachten.

Insbesondere ist die Zulässigkeit der Überwachung am Arbeitsplatz mittels Videobeobachtung am Persönlichkeitsrecht der Beschäftigten zu messen. Bereits die Möglichkeit der jederzeitigen Überwachung erzeugt einen Überwachungsdruck, der mit dem Anspruch der Beschäftigten auf Wahrung ihrer Persönlichkeitsrechte nicht zu vereinbaren ist. Insoweit ist eine Videoüberwachung am Arbeitsplatz nur durch besondere Sicherheitsinteressen des Arbeitgebers ausnahmsweise gerechtfertigt. Folgende Grundsätze sind daher zu beachten:

- Das berechtigte Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl, Unterschlagung oder Verrat von Betriebsgeheimnissen, muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen die gesamte Belegschaft reicht nicht aus.
- Eine unter diesen Voraussetzungen statthafte Videoüberwachung ist grundsätzlich offen nach vorheriger Information der Belegschaft durchzuführen.
- Eine Überwachung durch verdeckte Kameras ist als letzte Möglichkeit nur ausnahmsweise zulässig, wenn dieses Mittel die einzige Möglichkeit darstellt, berechtigte schutzwürdige Interessen des Arbeitgebers zu wahren. Eine Totalüberwachung ist ebenso unzulässig wie die Aufzeichnung von Räumen, in denen Beschäftigte in ihrer körperlichen Intimsphäre betroffen wären (WC, Dusche, Umkleidekabine).
- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrates oder der Personalvertretung. Aber auch die Zustimmung des Betriebs- oder Personalrates kann eine unzulässige Videoüberwachung nicht rechtfertigen.
- Die durch eine datenschutzwidrige Überwachung gewonnenen Erkenntnisse unterliegen einem Verwertungsverbot und können im arbeitsgerichtlichen Verfahren regelmäßig nicht verwertet werden.

Videoüberwachung in Mehrfamilienhäusern

Auch Vermieter oder beauftragte Hausverwaltungen setzen verstärkt Videoüberwachung ein. Die Kamerainstallation wird in solchen Fällen zumeist mit der Wahrnehmung des Hausrechts oder der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke nach § 6 b Abs. 1 BDSG begründet. Besonders in den Eingangs-, Flur- und Hofbereichen von Mehrfamilienhäusern kommt es immer wieder zu Sachbeschädigungen an Fahrzeugen oder Briefkästen. Die Wände von Treppenhäusern werden beschmiert oder die Kellerbereiche mit Sperrmüll zugestellt. Müllcontainerbereiche werden von Unbefugten oder von Mietern selbst dermaßen verunreinigt und zweckentfremdet, dass in extremen Fällen eine fachgerechte Entsorgung des normalen Hausmülls durch die BSR kaum noch möglich ist. Vermieter und Hausverwaltungen erhoffen sich, mit der Installation von Videoüberwachungskameras die Verursacher identifizieren und damit überführen zu können.

Nach unserer Erfahrung sind der Abschreckungseffekt und die Effizienz von Videokameras gerade in diesen Bereichen jedoch nur von kurzer Dauer. Oftmals sind gespeicherte Bildaufnahmen, die ein Fehlverhalten belegen sollen, trotz hochwertiger Kameratechnik wenig aussagekräftig. Verursacher sind häufig nicht eindeutig zu identifizieren, so dass nur eine Anzeige gegen Unbekannt aufgegeben werden kann. Darüber hinaus gerät eine Vielzahl unbeteiligter Personen in den Überwachungsbereich, deren schutzwürdige Interessen überwiegen.

Wir empfehlen den verantwortlichen Stellen, über eine Alternative nachzudenken, mit der einerseits die Zwecke von Vermieter bzw. Hausverwaltung erfüllt werden und gleichzeitig die Persönlichkeitsrechte aller betroffenen Mieter gewahrt bleiben:

Bei den überwachten Bereichen handelt es sich meistens um Hauseingangs- und Hofbereiche, zu denen nur die dort wohnenden Mieter Zugang haben sollten. Mit einer entsprechenden Schließanlage an der Hauseingangstür wäre zu gewährleisten, dass nur diese Mieter Zugang zum Haus und zum Hof haben. Damit wäre fremden Personen, die in der Vergangenheit die Bereiche für Sachbeschädigung bzw. illegale Müllentsorgung genutzt haben, der Zugang verwehrt. Zusätzlich kann eine Gegensprechanlage installiert werden, mit der die Mieter ihre Gäste einlassen. Erst wenn diese alternativen, datenschutzfreundlichen Maßnahmen die Situation im Überwachungsbereich nicht verbessern, kann über eine Videoüberwachung nachgedacht werden.

Mieter dürfen grundsätzlich keine private Videoüberwachung in Mehrfamilienhäusern betreiben, da sie im Gegensatz zum Vermieter kein Hausrecht in den Treppenhäusern und Fluren innehaben. Zum Schutz ihres Eigentums oder ihrer persönlichen Sicherheit ist ihnen allenfalls gestattet, in ihrer Mietwohnung eine Überwachungsanlage anzubringen, die ausschließlich Bereiche innerhalb der Wohnung erfasst. Es ist allerdings fraglich, ob eine solche Überwachungsmaßnahme ein geeignetes Mittel ist, die Privatsphäre zu schützen. Die Installation einer Alarmanlage wäre sicher ein effektiveres Mittel.

Videoüberwachung von Privatgrundstücken

Viele Bürgerinnen und Bürger sind an uns herangetreten, die sich durch die Videoüberwachungsmaßnahmen ihres Nachbarn überwacht fühlten und sich in

ihren Persönlichkeitsrechten verletzt sahen. Zur Klärung des Sachverhalts muss eine Stellungnahme des verantwortlichen Kamerabetreibers eingeholt werden. Stellt sich heraus, dass von der Videoüberwachung nicht nur der Privatbereich des Verantwortlichen, sondern auch angrenzendes öffentliches Straßenland betroffen ist, ist § 6 b BDSG einschlägig.

Demnach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Öffentlich zugängliche Räume sind z.B. Straßen, Bürgersteige, Einkaufspassagen und Parks, die der Allgemeinheit gewidmet sind, sowie alle anderen Bereiche, die von jeder Person ohne eine spezielle Zugangsberechtigung betreten werden können. Nicht-öffentlich zugänglich sind hingegen Firmengelände, die z.B. nur mit Werks- oder Besucherausweis betreten werden können, umfriedete Parks außerhalb der Öffnungszeiten und Privatgrundstücke. Anliegerzufahrten bzw. Anliegerwege über Privatgrundstücke, für die Dritte ein Geh-, Fahr- und Leitungsrecht besitzen, sind als öffentlich zugängliche Räume zu betrachten.

Wer neben seinem Grundstück auch öffentliches Straßenland mit Videotechnik beobachtet, kann sich **nicht** auf die Wahrnehmung des Hausrechts stützen, da der öffentliche Raum nicht in seinen Hausrechtsbereich fällt. Er kann die Videoüberwachung auch nur eingeschränkt mit der Wahrnehmung seiner berechtigten Interessen für konkret festgelegte Zwecke begründen (z.B. Schutz des Eigentums vor Diebstahl), da die Videoüberwachung nicht beliebig auf weite Teile des öffentlichen Raumes ausgeweitet werden darf. Auf keinen Fall darf er fremde Grundstücke mit einer Videoanlage beobachten, da damit der höchstpersönliche Lebensbereich anderer Personen durch Bildaufnahmen nach § 201 a Strafgesetzbuch (StGB) verletzt werden kann. Möchte er seine an die Grundstücksgrenze reichende Hausfassade vor Graffiti-Schmierereien schützen bzw. Graffiti-Sprüher abschrecken, muss gewährleistet sein, dass der erfasste Bereich bis auf maximal einen Meter von der Hausfassade reduziert ist[41].

41 Vgl. AG Berlin-Mitte, Urteil vom 18. Februar 2003 – 16 C 427/02 („Dussmann“)

Liegen im Erfassungsbereich der Videoüberwachung öffentlich zugängliche Bereiche, müssen nach § 6 b Abs. 2 BDSG betroffene Passantinnen und Passanten auf den Umstand der Beobachtung und die verantwortliche Stelle aufmerksam gemacht werden (**„Die Hausfassade wird videoüberwacht. Bei Fragen wenden Sie sich bitte an den Haus- bzw. Grundstückseigentümer“**). Der Hinweis sollte vor Betreten des überwachten Bereichs deutlich erkennbar sein. Die von der Videoüberwachung regelmäßig betroffenen Personen bzw. die Mitnutzenden des Grundstücks sind vom verantwortlichen Kamerabetreiber mündlich oder schriftlich über die Umstände und den Zweck der Beobachtung in Kenntnis zu setzen (z.B.: Welche Bereiche werden aus welchen Gründen überwacht? Werden die Bilddaten gespeichert und wenn ja, wie lange?). Die rechtlichen Anforderungen an eine Videoüberwachung sind umso strenger, je weniger Möglichkeiten die Personen haben, der Überwachung auszuweichen.

Im Zweifel bleibt den Betroffenen die Möglichkeit, zivilgerichtlich gegen diese Überwachungsmaßnahme vorzugehen und auf Unterlassung zu klagen. In der Vergangenheit sind Klagen nach § 823 i.V. m. § 1004 Bürgerliches Gesetzbuch (BGB) gegen derartige Maßnahmen zumeist erfolgreich verlaufen, weil eine Verletzung des allgemeinen Persönlichkeitsrechtes häufig anerkannt wurde.

Die Vielzahl der genannten Beispiele für den Einsatz von Videoüberwachungssystemen macht deutlich, dass eine pauschale datenschutzrechtliche Bewertung nicht möglich ist. Im Einzelfall kann häufig erst durch eine Kontrolle vor Ort die Sachlage eindeutig geklärt werden. Wenn die Verantwortlichen die Vorgaben des Bundesdatenschutzgesetzes nicht beachten, droht ihnen ein Bußgeld von bis zu 250.000 Euro. Wird der Intimbereich von Dritten heimlich überwacht, kann eine Videoüberwachung auch strafbar sein.

3. Öffentliche Sicherheit

3.1 Änderung des Gesetzes über das Bundeskriminalamt

Im letzten Jahr[42] haben wir über den Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG) berichtet, mit dem die Sicherheitsarchitektur in Deutschland grundlegend geändert wird. Das am 1. Januar 2009 in Kraft getretene Gesetz[43] enthält einen umfangreichen Katalog von Befugnissen, die das BKA zur Bekämpfung des internationalen Terrorismus einsetzen soll. Vorgesehen sind z.B. Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung. Auch die Befugnis zur sog. Online-Durchsuchung erlaubt dem BKA weit reichende Grundrechtseingriffe in Berlin. Die Datenschutzbeauftragten des Bundes und der Länder haben darauf hingewiesen, dass das BKA mit dem Gesetz mehr Befugnisse erhält, als einzelnen Länderpolizeien zur Erfüllung ihrer eigenen Gefahrenabwehr zustehen. Sie haben zudem die mangelhafte Abgrenzung der Befugnisse des BKA zu denen der Länderpolizeien und der Verfassungsschutzbehörden bemängelt.[44]

Der Entwurf wurde in den Gesetzgebungsgremien heftig und kontrovers diskutiert. Da er zwar vom Deutschen Bundestag verabschiedet, vom Bundesrat aber wegen erheblicher rechtsstaatlicher Mängel abgelehnt wurde, musste der Vermittlungsausschuss entscheiden, der einige Korrekturen vorgenommen hat. Unter anderem verständigte man sich darauf, dass die Online-Durchsuchungen privater Computer künftig ausnahmslos unter Richtervorbehalt stehen. Der Richter wird auch bei der Auswertung der gewonnenen Daten stärker eingebunden. Die Durchsicht hat unter der Sachleitung des anordnenden Gerichtes zu geschehen. Die Zuständigkeiten des BKA werden abschließend aufgezählt und damit klarer gefasst. Diesem Kompromiss stimmte der Bundesrat mit knapper Mehrheit zu – ohne die Stimme Berlins.

42 JB 2007, 2.1 und 3.1.1

43 BGBl. I 2008, S. 3083

44 Entschließung der 75. Konferenz am 3./4. April 2008 in Berlin: Mehr Augenmaß bei der Novellierung des BKA-Gesetzes, vgl. Dokumentenband 2008, S. 12

Jedoch bleiben weitere rechtsstaatliche Mängel bestehen. So hat die Senatorin für Justiz die Ablehnung Berlins im Bundesrat auch damit begründet, dass das absolute Auskunftsverweigerungsrecht für alle Berufsgeheimnisträger gelten müsse, also auch für Rechtsanwälte, Ärzte oder Journalisten. Das Gesetz sieht diesen Schutz nur für Abgeordnete, Geistliche oder Strafverteidiger vor.

Die Entscheidung des Bundesverfassungsgerichts bleibt abzuwarten: Es sind bereits Verfassungsbeschwerden angekündigt.

3.2 Kontrolle der IT-Sicherheit beim polizeilichen Informationssystem POLIKS

Ende 2007 wurde eine Kontrolle der IT-Sicherheit beim Einsatz des neuen polizeilichen Informationssystems POLIKS[45] durchgeführt. Gegenstände der Kontrolle waren das IT-Sicherheitsmanagement beim Polizeipräsidenten in Berlin, die Umsetzung des IT-Sicherheitskonzepts, der multifunktionale Arbeitsplatz (MAP) und die Schnittstellen von POLIKS zu anderen Verfahren. Es erfolgte ferner eine Unterrichtung über die polizeiliche IT-Infrastruktur, über die an dieser Stelle nicht berichtet wird.

Eine rechtliche Überprüfung galt der Schnittstelle zu den IT-Verfahren ASTA und MODESTA der Generalstaatsanwaltschaft Berlin. Eine vorgesehene Prüfung der Schnittstelle zum Verbundverfahren INPOL beim Bundeskriminalamt wurde zunächst ausgesetzt, da aufgrund der Komplexität dieser Schnittstelle nicht mit zeitnahen Ergebnissen gerechnet werden konnte.

Das **IT-Sicherheitsmanagement** bei der Polizei wurde an Hand der Kriterien des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[46] kontrolliert. Die Polizei verfügt über eine Geschäftsanweisung IT-Sicherheit, die die Rolle einer IT-Sicherheitsleitlinie einnimmt und in der die Ziele der IT-Sicherheit bei der Polizei, der Aufbau der IT-Sicherheitsorganisation und die Beschreibung eines IT-Sicherheitsprozesses, der die regelmäßige Anpassung des Sicherheits-

45 **Po**lizeili**c**hes **I**nformations- und **K**ommunikationssystem
46 IT-Grundschutzkataloge des BSI, BSI-Standard 100-1

konzepts an veränderte Rahmenbedingungen, insbesondere an den Stand der Technik, gewährleisten soll, enthalten sind. Wichtig ist dabei auch die Zusage, dass die IT-Sicherheit die volle Unterstützung der Behördenleitung und der gesamten Führungsebene genießt. Die Geschäftsanweisung trägt die Unterschrift des Polizeipräsidenten, ist allen Polizeidienststellen bekannt gemacht worden und im Intranet der Polizei eingestellt. Alle Bediensteten müssen einmal im Jahr die Kenntnisnahme der Regelungen bestätigen.

Seit 1997 gibt es bei der Polizei einen IT-Sicherheitsbeauftragten, der in Ausübung seiner Fachkunde weisungsfrei gestellt ist und ein direktes Vortragsrecht bei der Behördenleitung hat. Er hat den Vorsitz in einem Fachausschuss IT-Sicherheit und im IT-Sicherheitsmanagement, welches aus dem Fachausschuss und den dezentralen IT-Sicherheitsverantwortlichen besteht, die von jeder Gliederungseinheit der Polizei mit Stellvertretung zu bestellen sind. Fallweise wird das IT-Sicherheitsmanagement ergänzt um Verantwortliche für die Sicherheitstechnik und durch verfahrensbezogene Sicherheitsverantwortliche.

Die IT-Sicherheit ist Gegenstand aller Schulungen der Bediensteten für die Verwendung der polizeilichen IT-Verfahren. Das Konzept dazu wurde von der Polizeischule entwickelt. Die Sicherheitskonzepte der Polizei werden anlassbezogen aktualisiert. Anlässe dazu ergeben sich aus dem technischen Fortschritt, wesentlichen Änderungen von IT-Verfahren oder der Einbindung neuer Schnittstellen zu anderen Verfahren. Der IT-Sicherheitsbeauftragte erstellt jährlich einen Sicherheitsbericht für den Polizeipräsidenten.

Insgesamt betrachtet ist das IT-Sicherheitsmanagement beim Polizeipräsidenten in vorbildlicher Weise organisiert und ausgestattet. Leichte Abweichungen von den Maximalvorgaben des BSI wurden zwar festgestellt, stellen aber in Hinblick auf die zu erreichende IT-Sicherheit und deren Aufrechterhaltung bei Veränderungen keine Beeinträchtigung dar.

In Hinblick auf die **Ausfüllung des Sicherheitskonzepts** von POLIKS haben wir uns aufgrund unserer Erkenntnisse aus der Vorabprüfung des Sicherheitskonzepts auf die Protokollierungen und die Verteilung der Zugriffsberechtigungen konzentriert.

Es gibt zwei Protokolldateien, das Datenschutz-Journal und das POLIKS-Journal. Beide folgen einem einheitlichen Aufbau und halten Datum und Zeit, die Nummer des zugreifenden multifunktionalen Arbeitsplatzes, die gültige Protokolldatei sowie detaillierte Angaben zur protokollierten Aktion fest. Die Art der jeweils durchgeführten Transaktion bestimmt, ob der Protokolleintrag eher dem POLIKS-Journal zuordnet wird, weil die Transaktion keinem datenschutzrechtlichen Kontrollinteresse unterliegt, oder dem Datenschutz-Journal, weil eben dies doch der Fall ist. Beide Protokolldateien zusammen bilden die Aktivitäten am System detailliert ab, so dass die Revisionsfähigkeit gegeben ist.

Die Zugriffsberechtigungen an POLIKS werden mittels sog. Lesestufen organisiert. Die Rechte der Nutzenden werden mit Hilfe des Verzeichnisdienstes Active Directory von Microsoft (AD) administriert. Die Organisationsstruktur der Polizei wurde auf AD abgebildet. Die Administration erfolgt, indem den Nutzenden Aufgabenbereiche, Funktionsberechtigungen, Gruppen, Rollen und Schutzbereiche sowie die Berechtigung zum Zugriff auf Fremdsysteme oder sogar zur Erteilung von Rechten zugeordnet werden.

Diese Zuordnungen bestimmen, welche Daten eines Vorgangs sichtbar gemacht werden können (Sicht auf den Vorgang), und welche Vorgänge überhaupt gesehen werden können (Schutzbereiche für spezielle eingeschränkte Zugriffsberechtigungen, z.B. Organisierte Kriminalität, Rauschgiftdelikte, Polizeidelikte, Staatsschutz). Soweit Zugriff auf einen Vorgang genommen werden kann, werden fünf sog. Lesestufen unterschieden, die von der Zuordnung der Nutzenden zu einem Schutzbereich abhängen. Die einfachste Stufe umfasst das Lesen von nicht auf eine Person bezogenen Grundinformationen zu einem Vorgang in der ersten Stufe bis zur vollen Lesbarkeit des Vorgangs in der fünften Stufe, die dem oder der Verantwortlichen für den Vorgang zugewiesen wird. Das Zugriffskonzept der Polizei kann damit sehr differenziert gestaltet werden, ohne dass der dafür erforderliche Administrationsaufwand exzessiv wird.

Ein multifunktionaler Arbeitsplatz (MAP) ist derzeit ein Arbeitsplatzcomputer unter Windows XP, der den Nutzenden die Anwendungen und Dienste zur Verfügung stellt, die sie für ihre Aufgaben benötigen. Neben dem Zugang zum POLIKS und zum Intranet der Polizei handelt es sich dabei im Wesentlichen um Büroanwendungen mit der Ablage dienstlich gefertigter Dokumente. Die MAP-APCs sind Mitglieder einer Domäne, die gleichzeitig eine „Sicher-

heitsschale“ gegen unautorisierte Zugriffe darstellt. Diverse weitere Sicherheitsmaßnahmen sorgen dafür, dass nur autorisierte Clients Mitglieder der Domäne sein können. Die Nutzung lokaler Benutzerkonten, kritischer Anwendungen, externer Speichermedien und die Installation von Programmen werden ausgeschlossen. Die von uns mehrfach kritisierte Verwendung der Personalnummer als Identifikationsmerkmal zur Authentisierung zusammen mit einem Passwort wird abgelöst durch ein Smartcard-Verfahren mit PIN.

POLIKS kommuniziert mit einer Vielzahl anderer IT-Verfahren in unterschiedlicher Art und Weise. Innerhalb der Berliner Polizei sind es u.a. die Verfahren CASA als Auswertungstool für die Sachbearbeiter und BIDAVIS für die erkennungsdienstlichen Maßnahmen. Außerhalb der Berliner Polizei besteht z.B. Datenaustausch mit den Verfahren ASTA der Amts- und Staatsanwaltschaften, KVA des Kraftfahrzeugwesens (gestohlene Kfz) und INPOL im Fahndungsverbund mit dem Bundeskriminalamt. Auskünfte an POLIKS kommen von diversen Verfahren wie MESO (Berliner Einwohnerregister) und ZEVIS vom Kraftfahrtbundesamt, außerdem vom Bundes- und Ausländerzentralregister. Die technischen Lösungen dieser Schnittstellen erfolgen meist mit gesichertem Webservice, in einigen Fällen per File-Transfer, selten auch nur in Papierform.

Eine nähere Kontrolle der Schnittstellen erfolgte bisher nur für die Schnittstelle zu ASTA, über die per File-Transfer Daten von der Polizei an die sachleitende Staatsanwaltschaft übermittelt werden und andererseits nach § 482 Strafprozessordnung (StPO) Verfahrensausgänge zurückgemeldet werden. Verstöße gegen datenschutzrechtliche Bestimmungen wurden dabei nicht festgestellt.

Insgesamt ist deutlich geworden, dass die Sicherheit der polizeilichen Datenverarbeitung im Rahmen des POLIKS-Verfahrens für die Polizei ein wichtiges Ziel ist, dessen Erreichung mit einer Vielzahl ineinander greifender organisatorischer und technischer Maßnahmen sichergestellt wird. Aufrechterhalten wird das hohe Sicherheitsniveau durch ein IT-Sicherheitsmanagement, das in jeder Beziehung Vorbildcharakter hat.

3.3 Verfahren bei Auskunftserteilung durch die Polizei

In der Vergangenheit haben wir wiederholt über die Praxis bei der Erteilung von Auskünften durch die Polizei über die zur Person gespeicherten Daten berichtet[47]. Betroffenen, zu denen in der BKA-Verbunddatei INPOL Daten gespeichert sind, erteilt der Polizeipräsident mittlerweile den allgemeinen Hinweis: „Weiter weise ich Sie gemäß § 12 Abs. 5 BKAG darauf hin, dass hinsichtlich möglicher Speicherungen im Informationssystem der Polizei (INPOL) das Bundeskriminalamt die Datenauskunft erteilt."

Auskünfte aus dem INPOL-Datenbestand erteilt das Landeskriminalamt Berlin grundsätzlich nicht. Dies gilt auch, wenn Berlin die Daten eingestellt hat. Der Polizeipräsident begründet das damit, dass das BKA Daten verarbeitende Stelle für den INPOL-Datenbestand ist und nach § 12 Abs. 5 Bundeskriminalamtgesetz (BKAG) den Betroffenen – im Einvernehmen mit der Stelle, die die datenschutzrechtliche Verantwortung trägt (also für aus Berlin eingestellte Daten der Polizeipräsident) – Auskunft erteilt. Zu diesem Zweck fragt das BKA bei einem entsprechenden Datenbestand den jeweiligen Datenbesitzer, ob dem Antragsteller Auskunft über die zu seiner Person gespeicherten Daten erteilt werden darf. Erst dann erfolgt eine Prüfung durch das Landeskriminalamt über den in INPOL eingestellten Datenbestand.

Künftig will der Polizeipräsident auf die Tatsache hinweisen, dass er Daten zur Person des Antragstellers in das INPOL-System eingegeben hat. Eine Auskunft über die Daten will er aber weiterhin nicht erteilen. Das bedauern wir, weil damit die Gelegenheit, mehr Bürgerfreundlichkeit zu zeigen, nicht genutzt wird. Damit würde das Verfahren für den Antragsteller abgekürzt, ohne dass für das Landeskriminalamt ein Mehraufwand entsteht. Dort müsste ohnehin geprüft werden, ob der Auskunftserteilung aus dem Landessystem Verweigerungsgründe nach § 50 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) entgegenstehen. In anderen Ländern (z.B. Schleswig-Holstein) erteilt die Polizei grundsätzlich Auskunft über alle Datenspeicherungen in Landesdateien und dem INPOL-Zentralbestand, soweit keine gesetzlichen Verweigerungsgründe entgegenstehen.

47 JB 2006, 3.1.5; JB 2007, 3.1.5

Einstellungen in das Schengener Informationssystem (SIS) richten sich nach den Artikeln 95–100 des Schengener Durchführungsabkommens und erfolgen über das INPOL-System beim Bundeskriminalamt. Auch hierzu erteilt der Polizeipräsident keine Auskünfte. Bei Eingaben des Landes Berlin in das SIS würde das Bundeskriminalamt an die Staatsanwaltschaft Berlin mit der Standardformulierung „Für die Auskunft, die Sie in Ihrem Schreiben begehren, ist die Staatsanwaltschaft nach Maßgabe des Verfahrens rechtszuständig. Bitte wenden Sie sich an Ihre zuständige Staatsanwaltschaft. Ich weise Sie aber gleichzeitig darauf hin, dass der Verweis an die Staatsanwaltschaft nicht auf etwaige Maßnahmen schließen lässt“ verweisen.

Das Auskunftsrecht der Betroffenen tritt hinter einem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurück[48]. Im Falle einer Auskunftsverweigerung hat der Polizeipräsident Betroffene darauf hinzuweisen, dass sie sich an uns wenden können. Uns gegenüber muss er dann die Gründe für die Auskunftsverweigerung darlegen. Wir dürfen den Betroffenen aber keine Mitteilung machen, die Rückschlüsse über den Erkenntnisstand zulassen, es sei denn, der Polizeipräsident stimmt einer weitergehenden Auskunft ausdrücklich zu. Manchmal ist die Vorgehensweise des Polizeipräsidenten allerdings nicht oder nur schwerlich nachvollziehbar.

So hat ein der Berliner Polizei gut bekannter Petent um Auskunft nicht nur beim Polizeipräsidenten, sondern auch beim Bundeskriminalamt gebeten. Der Polizeipräsident hat darauf lediglich eine Teilauskunft erteilt und machte gegenüber dem Petenten von seiner Befugnis Gebrauch, zu bestimmten Einzeldaten eine weitergehende Auskunft zu verweigern. Das BKA hingegen hat aufgrund des Auskunftsersuchens des gleichen Petenten bei der Berliner Polizei nachgefragt und im Einvernehmen mit dem Polizeipräsidenten genau die Daten mitgeteilt, über die der Polizeipräsident die Auskunft verweigert hat. Gegen eine Auskunftserteilung durch das Bundeskriminalamt hatte er also keine Einwände. Uns gegenüber wiederum hat er – wenig überzeugend – einer Auskunftserteilung der dem Petenten ohnehin durch die Mitteilung des BKA bekannten Daten ausdrücklich nicht zugestimmt.

48 § 50 Abs. 2 ASOG

Ein anderer der Berliner Polizei ebenfalls nicht unbekannter Petent hat sich unter gleichzeitiger Vorlage eines Auszuges aus dem alten Informationssystem Verbrechensbekämpfung (ISVB - Vorläufer von POLIKS) darüber beschwert, dass ihm keine vollständige Auskunft erteilt wurde. Auch nachdem dem Polizeipräsidenten ausführlich erläutert wurde, dass dem Petenten die Daten, über die die Auskunft verweigert wurde, längst bekannt sind, hat sich nichts am Ergebnis geändert. Er hat diese Daten weder dem Petenten selbst mitgeteilt noch einer Mitteilung durch uns zugestimmt.

Der Polizeipräsident sollte die schematische Vorgehensweise bei der Bearbeitung von Anträgen auf eine Selbstauskunft überprüfen und die Besonderheiten des Einzelfalles stärker würdigen.

3.4 Das Rechtshilfeersuchen und die erkennungsdienstliche Behandlung

Aus der Praxis

Ein Petent, der als Geschäftsführer in einem Privatunternehmen tätig war, beschwerte sich darüber, dass ihn die Polizei erkennungsdienstlich behandelt hat, obwohl gegen ihn kein konkreter Tatverdacht vorlag.

Die erkennungsdienstliche Behandlung (ed-Behandlung) wurde aufgrund eines Rechtshilfeersuchens des britischen Fraud Prosecution Service durchgeführt und betraf ein Unternehmen, bei dem der Petent beschäftigt war. Dabei wurde im Fall der Festnahme durch deutsche Behörden und der Abnahme von Fingerabdrücken darum gebeten, diese den britischen Behörden zur Verfügung zu stellen. Anderenfalls wurden die deutschen Behörden ersucht, den Petenten um eine freiwillige Abgabe von Fingerabdrücken zu bitten und – falls er dieser Bitte entsprechen würde – sie an die britischen Behörden zu übermitteln. Obwohl weder ein konkreter Tatverdacht gegen den Betroffenen noch seine Einwilligung vorlag, führte die Polizei die erbetene ed-Behandlung durch.

Die Polizei hat die Befugnis, erkennungsdienstliche Maßnahmen für Zwecke des Erkennungsdienstes anzuordnen und durchzuführen. Die Maßnahme ist aber dann rechtswidrig, wenn die Polizei ihre Befugnisse überschreitet. Dies war hier der Fall. Nach dem Rechtshilfeersuchen der britischen Behörden war

eine freiwillige Abgabe der Fingerabdrücke für den Fall, dass die deutschen Strafverfolgungsbehörden in eigener Zuständigkeit keine erkennungsdienstlichen Maßnahmen gegen den Petenten als Beschuldigten durchführen, zur Zweckerfüllung ausreichend. Die britischen Behörden waren in diesem Fall diejenigen, die den Umfang der durchzuführenden Handlungen bestimmen durften. Eine effektive Rechtshilfe setzt eine Bindung der deutschen Behörden an das Ersuchen Voraus. Allerdings dürfen dabei die innerstaatlich vorgesehenen Befugnisse nicht überschritten werden.

Für die deutschen Behörden stand der Petent nicht unter Tatverdacht. Gegen ihn wurde kein Strafverfahren eingeleitet, wie uns von der Staatsanwaltschaft bestätigt wurde. Der Polizeipräsident in Berlin hat im Schriftwechsel nicht erklärt, dass er den Versuch unternommen hat, die Fingerabdrücke auf freiwilliger Basis mit Einwilligung des Betroffenen zu erhalten.

Es waren somit keine Gründe für die Überschreitung des Ersuchens ersichtlich. Wie bei einer innerstaatlichen Maßnahme sind die Grundrechtseingriffe so gering wie möglich zu halten, wenn sie zur Erfüllung eines internationalen Amtshilfeersuchens erfolgen. Somit lag ein unzulässiger Eingriff in die Grundrechte vor.

Rechtshilfeersuchen ausländischer Strafverfolgungsbehörden berechtigen die Polizei nicht dazu, innerstaatliche Befugnisgrenzen zu missachten.

4. Melde- und Personenstandswesen

4.1 Entwurf für ein Bundesmeldegesetz

Letztes Jahr haben wir die in einem Eckpunktepapier zusammengefassten Forderungen der Datenschutzbeauftragten des Bundes und der Länder an ein Bundesmeldegesetz vorgestellt[49]. Diese Forderungen sind weitgehend aktuell. Der mittlerweile vom Bundesministerium des Innern vorgelegte Referentenentwurf setzt sie nur unzureichend um.

So sieht der Entwurf neben dem kommunalen Register ein – in fast vollständigem Datenumfang der Meldebehörden – zusätzliches zentrales Bundesmelderegister und damit eine doppelte Datenhaltung vor. Das Vorhaben widerspricht dem Grundsatz der Datenvermeidung, der Vermeidung einer Vorratsdatenhaltung und dem Erforderlichkeitsprinzip. Ferner berücksichtigt der Entwurf nicht das verfassungsrechtliche Verbot eines einheitlichen und verwaltungsübergreifenden Identifikationsmerkmals. Die Ordnungsmerkmale in den Melderegistern sollen auch an andere öffentliche Stellen übermittelt werden. Zudem wird danach im Bundesmelderegister ein weiteres Ordnungsmerkmal geschaffen, das dem bundesweiten Datenaustausch dienen soll. So entstehen mehrere verknüpfbare Personenkennzeichen, die verfassungsrechtlich unzulässig sind.

Nach der Föderalismusreform hat der Bundesgesetzgeber zwar die Gesetzgebungs-, aber ausdrücklich nicht die Verwaltungskompetenz erhalten. Mit der Doppelung des nahezu kompletten kommunalen Meldedatenbestandes im Bundesmelderegister verlieren die Meldebehörden der Sache nach ihre Verantwortlichkeit, soweit die Datenverarbeitung des gespiegelten Datenbestandes dort erfolgt. Ferner sollen Datenübermittlungen in erheblichen Teilen durch das Bundesmelderegister erfolgen.

Unsere Forderung, bei einer Reform des Melderechts müsse der Umfang der im Melderegister gespeicherten Daten und die jeweiligen Datenübermittlungen einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit

49 JB 2007, 4.1

und Zweckbindung unterzogen werden, wurde nicht berücksichtigt. Vielmehr soll der Entwurf den Datenumfang und die Übermittlungen noch ausweiten. Darüber hinaus sollen die Rechte der Betroffenen nicht gestärkt werden. So wird weiter an der Widerspruchslösung bei Datenübermittlungen festgehalten, anstatt sie durch die notwendige Einwilligung zu ersetzen.

Der Referentenentwurf sieht nicht den gebotenen datenschutzrechtlichen Ausgleich für die Schaffung neuer Datenschutzrisiken durch die doppelte Datenhaltung und die Zentralisierung in einem Bundesmelderegister vor.

Bei Redaktionsschluss gab es keine Hinweise darauf, dass das Bundesministerium des Innern das Gesetzgebungsvorhaben kurzfristig voranbringen wird. Mit einer Verabschiedung vor der nächsten Bundestagswahl ist deshalb nicht zu rechnen.

4.2 Persönliches Erscheinen bei Speicherung einer zu benachrichtigenden Person

Bei der Novellierung des Berliner Meldegesetzes[50] wurde die rechtliche Möglichkeit geschaffen, mit Einwilligung der Einwohnerin oder des Einwohners und der betroffenen Person zusätzlich zu den gesetzlich vorgesehenen Daten Familiennamen, Vornamen, gegenwärtige Anschrift und Telefonnummer einer Person zu speichern, die benachrichtigt werden soll, wenn die Einwohnerin oder der Einwohner aufgrund eines Unglücksfalles in eine hilflose Lage gerät oder stirbt[51].

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) hat die Auffassung vertreten, dass hierzu das persönliche Erscheinen der Antrag stellenden Person erforderlich ist. Die Willenserklärung der Betroffenen über die Speicherung der Daten einer anderen Person sei eine so wichtige Handlung, die aus Sicht des LABO nicht durch Dritte vertretbar sei. Ein Antrag auf dem Postweg würde ferner die Beglaubigung der Unterschriften beider Personen

50 GVBl. 2006, S. 896
51 § 2 Abs. 3 MeldeG

erfordern. Dafür müssten die Antrag stellende und die einzutragende Person ein Bürgeramt oder eine andere dazu befugte Stelle aufsuchen. Zudem ist eine Unterschriftsbeglaubigung kostenpflichtig, was kaum im Interesse der Betroffenen liegen dürfte.

Zugleich vernachlässigt das LABO den Umstand, dass eine Pflicht zum persönlichen Erscheinen nach dem Verwaltungsverfahrensgesetz[52] nur dann besteht, wenn sie durch Rechtsvorschrift vorgesehen ist. Das ist beispielsweise bei § 23 Asylverfahrensgesetz (persönliches Erscheinen bei der Antragstellung) oder § 17 Wehrpflichtgesetz (Musterung) der Fall. Demgegenüber schreibt § 2 Abs. 3 MeldeG ein persönliches Erscheinen gerade nicht vor. Ferner ist es nicht ersichtlich, aus welchem Rechtsgrund die Beglaubigung der Unterschriften erforderlich sein soll oder welche Dritte hier eine Willenserklärung für die Betroffenen abgeben. Hier wurden nicht zu rechtfertigende bürokratische Hindernisse aufgebaut. Erst nachdem wir den Vorgang beanstandet haben, hat das LABO eingelenkt und das Verfahren eingestellt.

Die Anordnung des persönlichen Erscheinens liegt nicht im freien Ermessen der Behörde. Sie muss vielmehr gesetzlich vorgesehen sein. § 2 Abs. 3 MeldeG sieht eine solche Befugnis für die Speicherung von zu benachrichtigenden Personen nicht vor.

4.3 Reform des Personenstandsrechts – Familienforscher atmen auf

Ende des Jahres ist das Personenstandsrechtsreformgesetz in Kraft getreten. Schwerpunkte der Reform sind

- die Einführung elektronischer Personenstandsregister anstelle der bisherigen Personenstandsbücher,
- die Begrenzung der Fortführung der Personenstandsregister durch das Standesamt sowie die Abgabe der Register an die Landesarchive,

52 § 26 Abs. 2 VwVfG

- die Ersetzung des Familienbuches durch Beurkundungen in den Personenstandsregistern,
- die Reduzierung der Beurkundungsdaten auf das für die Dokumentation des Personenstandes erforderliche Maß,
- die Neuordnung der Benutzung der Personenstandsbücher,
- die Schaffung einer rechtlichen Grundlage für eine Testamentsdatei.

Insbesondere die Neuordnung der Benutzung der Personenstandsbücher dürfte für die Familienforschung von unmittelbarer praktischer Bedeutung sein. Immer wieder haben Betroffene, die Ahnenforschung betreiben wollten, mit Unverständnis darauf reagiert, wenn ihnen die Standesämter keine Auskünfte zu – oft schon lange verstorbenen – Angehörigen erteilt haben. Das geschah mit der zutreffenden Begründung, dass Auskünfte aus den Personenstandsbüchern an ein rechtliches Interesse geknüpft sind und die reine Familienforschung diesen Anforderungen nicht entspricht. Diese strenge Regelung beruht nicht auf typischen Gefahren der automatisierten Datenverarbeitung, sondern auf den Erfahrungen mit dem Missbrauch, der mit den Personenstandsbüchern im Dritten Reich betrieben wurde. Jetzt ist die Benutzung der Bücher bei der Glaubhaftmachung eines berechtigten Interesses zugelassen, wenn seit dem Tod der/des zuletzt verstorbenen Beteiligten 30 Jahre vergangen sind. Beteiligte sind im Geburtenregister die Eltern und das Kind, beim Eheregister die Ehegatten und beim Lebenspartnerschaftsregister die Lebenspartner.

Daneben ist das Kernelement der Reform vor allem die Beurkundung in elektronisch geführten Personenstandsregistern und ein weitgehend standardisierter elektronischer Mitteilungsverkehr der Standesämter untereinander und mit anderen Behörden eingeführt worden. Die elektronische Registerführung wird – nach Ablauf einer Übergangszeit – voraussichtlich zum 1. Januar 2014 für alle Standesämter obligatorisch sein.

Das neue Personenstandsrecht lässt einen angemessenen Ausgleich zwischen den Interessen Von Familienforscherinnen und -forschern und ihrer verstorbenen Angehörigen zu.

5. Verkehr

5.1 Namensvetter in der Fluggäste-Datei

Aus der Praxis

Ein Berliner Flugreisender erlebte am Check-in-Automaten seiner Fluggesellschaft, bei der er die Reise gebucht hatte, eine Überraschung: Als er seine Bordkarte anklicken wollte, wurde ihm nicht nur sein eigener Flug angezeigt, sondern auch die Flugbuchungen anderer Passagiere, die den gleichen Nachnamen trugen wie er. Beim Rückflug aus dem Ausland nach Berlin widerfuhr ihm das Gleiche noch einmal. Er hätte sogar die Bordkarte einer anderen Person für einen anderen Flug ausdrucken können.

Wir haben die Fluggesellschaft aufgefordert, uns von sofortigen Maßnahmen zu unterrichten, die einen solchen unbefugten technischen Zugriff auf fremde Daten künftig ausschließen. Die Fluggesellschaft teilte uns mit, dass sie unverzüglich eine Anpassung des **„Automaten-SELF-Check-in-Systems“** einleiten würde.

Die getroffenen Maßnahmen waren hinreichend geeignet, um den Zugriff auf fremde Daten zu unterbinden. Es ist davon auszugehen, dass damit auch dem Bedürfnis der Reisenden nach einer unbürokratischen und schnellen Abwicklung des Check-in Rechnung getragen werden kann.

Die zunehmende Automation von Geschäftsvorgängen darf nicht dazu führen, dass schwerwiegende Mängel bei der Zugriffskontrolle über gespeicherte Daten entstehen und unzulässige Datenzugriffe erfolgen können. Die aus der Automation resultierenden Vorteile dürfen speichernde Stellen nicht dazu verleiten, Sicherheitsrisiken für ihre Geschäftspartner bei der automatischen Datenverarbeitung hinzunehmen.

5.2 Fotoabgleich bei Verkehrsverstößen

Im Rahmen einer Geschwindigkeitsmessung in Brandenburg wurde ein Kraftfahrzeugführer wegen einer Geschwindigkeitsüberschreitung durch ein Frontfoto erfasst. Das Fahrzeug soll in einer Ortschaft die zulässige Höchstgeschwindigkeit um 25 km/h überschritten haben. Das Frontfoto wies eine männliche Person als Fahrzeugführer aus. Die Ermittlungsbehörden des Landkreises schlossen die in Berlin ansässige weibliche Kraftfahrzeughalterin des besagten Fahrzeuges von vornherein als Täterin aus und leiteten den Vorgang samt Frontfoto an den Polizeipräsidenten in Berlin zur Ermittlung des Fahrzeugführers.
Der unmittelbar angeschriebene Kraftfahrzeugführer unterstellte den Ermittlungsbehörden, sie hätten, ohne ihn vorher anzuhören, die Ermittlungen gegen ihn durch einen unzulässigen Fotoabgleich mit der Bilddatei der Ausweisbehörde geführt.

Die datenschutzrechtlich zulässige Durchführung eines Fotoabgleichs mit der Bilddatei der Ausweisbehörde setzt auch bei außerhalb von Berlin ermittelten Verkehrsverstößen voraus, dass ein Tatverdächtiger vor dem Fotoabgleich angehört wird[53]. Der Polizeipräsident bestätigte uns, dass vom Landrat des brandenburgischen Landkreises lediglich die Halterin des Fahrzeuges angehört worden war. Sie habe ihre Täterschaft mit der Begründung „siehe Foto“ bestritten. Der Landrat habe ihn im Wege der Amtshilfe ersucht, anhand des „geblitzten“ Frontfotos den Fahrzeugführer zu ermitteln. Die Halterin sei vom Polizeipräsidenten nochmals vergeblich angeschrieben und aufgefordert worden, im nächstgelegenen Polizeiabschnitt vorzusprechen. Es seien weitere Umfeldermittlungen aufgenommen und daraufhin bei der Meldebehörde ermittelt worden, dass unter der Adresse der Kraftfahrzeughalterin eine männliche Person gemeldet war. Ohne diese melderechtlich ermittelte Person vorher anzuhören, sei ein Fotoabgleich durchgeführt worden.

Der Polizeipräsident sicherte uns jedoch zu, künftig auch bei Ermittlungen zu Verkehrsverstößen außerhalb Berlins, die im Wege der Amtshilfe durchge-

53 Vgl. JB 2007, 4.2.2

führt werden, die vorherige Anhörung des Tatverdächtigen vor der Durchführung eines Fotoabgleichs sicherzustellen. Durch eine ausdrückliche Handlungsanweisung, die uns vorgelegt wurde, ist dies inzwischen gewährleistet. Weitere Beschwerden sind seitdem nicht mehr eingegangen.

Künftig wird jeder im Wege einer Umfeldermittlung ermittelte Tatverdächtige angehört, bevor der Fotoabgleich zur Täteridentifikation durchgeführt wird.

5.3 Datensicherheit beim Führerschein-Register

Bereits im letzten Jahr[54] hatten wir festgestellt, dass aufgrund der Umstellung auf einen Rechnerverbund und einer neuen Datenbanksoftware die Überarbeitung und Fortschreibung des vorhandenen Sicherheitskonzeptes notwendig war. Die damals von uns entdeckten Mängel betrafen erhebliche Risiken für die Verfügbarkeit des Systems, weil der Einbruchs- und Brandschutz für den Serverraum unzureichend gewährleistet war.

Diese Mängel sind inzwischen nahezu alle abgestellt worden. Es wurden entsprechende Einschränkungen des Zugangs veranlasst, und für die baulichen Veränderungen wurde die zuständige Berliner Immobilien Management GmbH (BIM) als Verwalterin der öffentlichen Gebäude beauftragt, entsprechend tätig zu werden. Das beauftragte Ingenieurbüro hat ein umfangreiches Leistungsverzeichnis für die erforderliche Ausschreibung erstellt. Mit einem Abschluss der baulichen Maßnahmen ist in naher Zukunft zu rechnen.

Gerade wenn es um teure bauliche Maßnahmen geht, die für die Datensicherheit erforderlich sind, gilt: Es währt immer lange. Aber: Was lange währt ...

54 JB 2007, 4.2.5

6. Justiz

6.1 Verfassungswidrige Vorratsdatenspeicherung

Über das Inkrafttreten des scharf kritisierten Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG haben wir bereits berichtet.[55] Das Gesetz verpflichtet Anbieter von Telekommunikationsdienstleistungen zur anlassfreien sechsmonatigen Erfassung von Verkehrsdaten. Diese Speicherung dient dazu, den Sicherheitsbehörden bei Bedarf den Zugriff auf diese Verkehrsdaten zu ermöglichen. Bislang konnten sie auf die Daten zugreifen, welche die Anbieter für die Vertragsabwicklung mit ihren Kunden gespeichert hatten. Daneben sieht das Gesetz eine Neuregelung von verdeckten Ermittlungsmaßnahmen wie die Telekommunikationsüberwachung und den Einsatz des IMSI-Catchers zur Ortung von aktiv geschalteten Mobiltelefonen vor.

Mittlerweile sollen ca. 35.000 Verfassungsbeschwerden gegen das Gesetz beim Bundesverfassungsgericht eingegangen sein, das uns Gelegenheit zur Stellungnahme gegeben hat. Wir haben gemeinsam mit den übrigen Datenschutzbeauftragten der Länder auf die nachfolgenden erheblichen rechtsstaatlichen Mängel des Gesetzes hingewiesen:

Die anlassfreie Erfassung sämtlicher Telekommunikationsverkehrsdaten verstößt gegen die Wesensgehaltsgarantie des Fernmeldegeheimnisses. Zwar werden regelmäßig „nur“ die Verkehrsdaten und nicht die Inhalte der Telekommunikation erfasst. Darauf kommt es jedoch nicht an: Wenn die Begleitumstände **jeder** Telekommunikation erfasst werden, wird eine unbefangene Nutzung dieser unentbehrlichen Technik unmöglich gemacht. Überdies ist die Neuregelung in § 113b Satz 1, § 113 Telekommunikationsgesetz (TKG) krass unverhältnismäßig. Sie ermöglicht im Ergebnis sämtlichen Ordnungsbehörden den Zugriff auf Vorratsdaten im Sinne des § 113a TKG. Im Klartext: Dem Wortlaut nach könnte theoretisch ein simpler Verstoß gegen Straßenverkehrsregeln, etwa

55 JB 2007, 5.1

ein Falschparken, dazu führen, dass auf die Telekommunikationsverkehrsdaten zugegriffen wird. Die Neuregelungen genügen nicht den Anforderungen an normenklare und hinreichend bestimmte Befugnisse. Sie gewährleisten weder einen hinreichenden Schutz des Kernbereichs privater Lebensgestaltung noch einen angemessenen Schutz von Berufsgeheimnisträgern.

In zwei Eilentscheidungen[56] hat das Bundesverfassungsgericht das Gesetz vorläufig darauf beschränkt, dass Verkehrsdaten nur dann an Strafverfolgungsbehörden übermittelt werden dürfen, wenn im Einzelfall schwerwiegende Straftaten verfolgt werden, die nicht auf andere Weise aufgeklärt werden können. Zudem dürfen weder Polizeibehörden für präventive Zwecke noch Nachrichtendienste auf diese Daten zugreifen.

Eine abschließende Entscheidung des Bundesverfassungsgerichts zu den Verfassungsbeschwerden steht noch aus. Bereits getroffene Eilentscheidungen deuten jedoch auf die Verfassungswidrigkeit einiger Regelungen hin.

6.2 Evaluierung der Organisationsstruktur von Justizvollzugsanstalten

Aus der Praxis

Im Herbst 2006 wurden die Organisationsstrukturen der Justizvollzugsanstalten Tegel, Moabit, Hakenfelde, Plötzensee und der Justizvollzugsanstalt für Frauen sowie der Jugendstrafanstalt bewertet. Unsere Überprüfung ergab, dass die Senatsverwaltung ein Verfahren gewählt hatte, das die datenschutzrechtlichen Belange der Belegschaft beachtete.

Zur Durchführung der Evaluierung teilten die Justizvollzugsanstalten einer Unternehmensberatung die Anzahl der Bediensteten mit, die für eine Befragung geeignet waren. Anschließend sandte die Unternehmensberatung die gleiche Zahl von Bewertungsbögen der jeweiligen JVA zu, die die Bögen an die Bediensteten weiterleitete. Beigefügt war ein Begleitschreiben der Unternehmensberatung, welches das Bewertungsverfahren näher beschrieb.

56 Beschlüsse vom 11. März 2008 und vom 28. Oktober 2008 – 1 BvR 256/08

Wir stellten fest: Den Dienstkräften wurde verdeutlicht, dass bei einer Rücksendung des Fragebogens der Name/die Schlüsselnummer ausschließlich der Unternehmensberatung bekannt würde. Die Nennung diene „lediglich dazu, die Rücklaufquote zu steuern sowie Gesprächspartner für spätere, vertiefende Gespräche auszuwählen. Einzelauswertungen werden nicht vorgenommen." In den Justizvollzugsanstalten wurden Sammelbehälter aufgestellt, um den Bediensteten eine anonyme Abgabe ihrer Fragebögen zu ermöglichen. Die Sammelbehälter wurden nur von Angestellten der Unternehmensberatung geöffnet.

Danach haben die Justizvollzugsanstalten und die Senatsverwaltung keine personenbezogenen Mitarbeiterdaten an die Unternehmensberatung weitergegeben. Die Entscheidung, ob solche Daten an dieses Unternehmen gelangten, lag allein in der Hand der Betroffenen. Umgekehrt hat die Unternehmensberatung Personaldaten weder an die Justizvollzugsanstalten noch an die Senatsverwaltung übermittelt. Den schriftlichen Verfahrensbeschreibungen zufolge wurden die Fragebögen nach Auswertung durch die Unternehmensberatung vernichtet. Eine Einzelauswertung fand nicht statt.

Als Verbesserungsmöglichkeit für künftige Evaluierungen regten wir in Anlehnung an § 6 Abs. 4 Berliner Datenschutzgesetz (BlnDSG) lediglich an, dass im ersten Anschreiben ausdrücklich auf die Freiwilligkeit der Mitwirkung der betroffenen Mitarbeiterinnen und Mitarbeiter hingewiesen wird.

6.3 Videoüberwachung der Gedenkstätte Plötzensee

Nicht nur eine Anfrage der Senatsverwaltung für Justiz veranlasste uns, im Herbst 2007 die Videoüberwachungsanlage der Jugendstrafanstalt (JSA) Plötzensee von außen in Augenschein zu nehmen. Es waren medienwirksam Vorwürfe laut geworden, dass die Videoüberwachung, die den Überwurf von Gegenständen über die Mauer verhindern soll, auch die angrenzende Gedenkstätte Plötzensee erfasse. Eine eingehende Prüfung der Videoüberwachung im April bestätigte diese Befürchtung. Die JSA hat Abhilfe angekündigt, die allerdings noch aussteht.

Wir haben unser Augenmerk insbesondere auf die Beobachtung der unmittelbaren Außenbereiche gelegt, also ein angrenzendes Grundstück des Deutschen Paketdienstes, die Gedenkstätte Plötzensee sowie die öffentlich zugänglichen Straßen und Bürgersteige. Unsere Prüfung ergab, dass eine Rundumkamera, die eigentlich die Kontrolle einer Torzufahrt ermöglichen soll, nicht nur das Gelände der JSA, sondern auch Teile der angrenzenden Gedenkstätte Plötzensee erfasst. Insoweit ermöglicht die Kamera technisch eine Datenerhebung, die über das erforderliche Maß hinausgeht.

Die JSA hatte hierzu zwar die zuständigen Bediensteten mündlich sensibilisiert, die Funktionalität dieser Kamera nicht voll auszuschöpfen. Dies allein genügt jedoch nicht den Anforderungen des § 5 BlnDSG, der von der verantwortlichen Stelle verlangt, die für die Einhaltung der datenschutzrechtlichen Vorschriften erforderlichen technischen und organisatorischen Vorkehrungen zu treffen. Eine Kamera, die einen Erfassungsgrad von 360° besitzt, erfüllt diese Kriterien vorliegend nicht, zumal man nachträglich nicht nachvollziehen kann, wer wann weisungswidrig die Gedenkstätte mit der Kamera beobachtet.

Deshalb haben wir einen datenschutzrechtlichen Mangel nach § 26 Abs. 2 BlnDSG festgestellt. Da die mit der Kamera eigentlich zu überwachende Torzufahrt künftig geschlossen werden soll, hat die JSA angekündigt, die Kamera mit der Schließung dieser Torzufahrt zurückzubauen. Der Rückbau soll bis Ende März 2009 stattfinden. Weitere datenschutzrechtliche Mängel wurden bei der Überprüfung der Videoüberwachung nicht festgestellt. Die JSA zeichnet Bilder für die Dauer von 12 Wochen auf, anschließend werden die Bilder automatisch überschrieben. Die relativ lange Aufzeichnungsdauer ist bei einer Justizvollzugsanstalt den Besonderheiten des Überwachungsbetriebs geschuldet und damit erforderlich.

Sollten die Baumaßnahmen an der Torzufahrt noch weiter in das Jahr 2009 hineinreichen, ist eine technische Lösung des Problems der Mitüberwachung der Gedenkstätte dringlich umzusetzen.

7. Finanzen

7.1 Holpriger Start für die bundeseinheitliche Steuer-Identifikationsnummer

Der Gesetzgeber hat mit dem Jahressteuergesetz 2003 Regelungen über die Einführung einer neuen bundeseinheitlichen Steuer-Identifikationsnummer in die Abgabenordnung aufgenommen[57]. Mit diesem Ordnungsmerkmal, das aus einem elfstelligen Code besteht, wird jede Bundesbürgerin und jeder Bundesbürger (vom Baby bis zum Greis) künftig lebenslang bei den Steuerbehörden registriert.

Die Vergabe der Steuer-Identifikationsnummer durch das Bundeszentralamt für Steuern (BZSt) dauerte viel länger als ursprünglich vorgesehen und war mit erheblichen Problemen behaftet. Bereits im Sommer 2007 übersandten die Meldebehörden dem BZSt die Daten aller Einwohnerinnen und Einwohner, die mit ihrem Wohnsitz (zum Stichtag 1. Juli 2007) im Melderegister erfasst waren. Die den Meldebehörden seitdem angezeigten Umzüge wurden dem BZSt laufend nachgemeldet und ebenfalls in der dortigen Datenbank erfasst. Im Sommer 2008 wurde damit begonnen, die Steuer-ID-Nummer (in mehr als 80 Millionen Briefen) zu versenden. Dabei kam es - aufgrund von fehlerhaften Datensätzen aus den Meldebehörden - zu einer erhöhten Anzahl von nicht zustellbaren Mitteilungsschreiben. Nach Angaben des Bundesministeriums der Finanzen belief sich die Anzahl der unzustellbaren Schreiben bundesweit auf bis zu 330.000 Fälle. Die Versendung von bis zu 440.000 weiteren Mitteilungsschreiben mit fehlerhaften Adressen wurde daraufhin bis zum 24. Dezember 2008 zurückgestellt. Deshalb ist davon auszugehen, dass bundesweit insgesamt etwa 770.000 nicht aktuelle Datensätze in der Datenbank des BZSt erfasst sind. Wie viele dieser Fälle sich auf Berlin beziehen, ist uns nicht bekannt.

Mehrere Bürgerinnen und Bürger haben sich bei uns darüber beschwert, dass die Angaben zum Geburtsland in ihrem Datensatz an die heute gültigen Grenzen angepasst wurden. Es stellte sich heraus, dass es sich dabei ebenfalls um ein

57 §§ 139 a bis 139 d AO

bundesweit auftretendes Problem handelte. Das Bundesministerium der Finanzen teilte dazu in einer Antwort auf eine parlamentarische Anfrage mit[58], dass die Daten in der Datenbank des BZSt den bei den Meldebehörden gespeicherten Informationen entsprechen. Diese würden den Geburtsstaat in Form eines Gebietsschlüssels erfassen. Zur Vergabe dieses Schlüssels habe sich keine bundesweit einheitliche Praxis entwickelt. So seien Geburtsorte, die zur Zeit der Geburt zum Deutschen Reich gehörten, mit dem aktuellen Gebietsschlüssel versehen worden. Dies habe dazu geführt, dass in einigen Fällen ein ausländischer Geburtsstaat eingetragen wurde, obwohl der Geburtsort zum Zeitpunkt der Geburt innerhalb der Grenzen des damaligen Deutschen Reiches lag.

Nach Mitteilung des Bundesministeriums der Finanzen werden die Angaben zum Gebietsschlüssel in den Meldebehörden überarbeitet. Sobald die korrigierten Daten von den Meldebehörden an das Bundeszentralamt für Steuern übermittelt worden sind, erhalten alle Betroffenen ein erneutes Schreiben mit den berichtigten Daten zum Geburtsland.

7.2 Angaben zur Religionszugehörigkeit bei Kapitalerträgen

Aus der Praxis

Ab dem Jahr 2009 werden Erträge aus privaten Kapitalanlagen grundsätzlich nicht mehr im Rahmen der Einkommensteuerveranlagung, sondern im Wege des Steuerabzuges vom Kapitalertrag erfasst[59]. Dies macht eine landesrechtliche Regelung erforderlich, wonach die Kirchensteuer auf diese Einkünfte ebenfalls an der Quelle dieser Einkünfte (Geldinstitute, Banken) erhoben werden kann.

In § 3 Abs. 5 des Entwurfs für ein „Gesetz über die Erhebung von Steuern durch öffentlich-rechtliche Religionsgemeinschaften im Land Berlin (Kirchensteuergesetz – KiStG)“[60] wird zur Festsetzung und Erhebung der Kirchensteuer

58 BT-Drs. 16/10649, S. 10
59 Unternehmensteuerreformgesetz 2008 vom 14. August 2007, BGBl. I, S. 1912
60 Abghs.-Drs. 16/1933

ab 2009 – datenschutzrechtlich unzureichend – pauschal auf die Anwendung des § 51a Einkommensteuergesetz (EStG) verwiesen.

Der Bundesgesetzgeber hat den Steuerpflichtigen in der Evaluierungsphase bis 30. Juni 2010 die Freiheit eingeräumt, selbst zu entscheiden, ob sie ihrer Bank durch Mitteilung ihrer Religionszugehörigkeit die Einbehaltung der Kirchenkapitalertragssteuer im Rahmen des Abgeltungssteuerverfahrens ermöglichen oder ob die Einbehaltung der Kirchenkapitalertragssteuer (wie bisher) im Rahmen des Veranlagungsverfahrens erfolgen soll.[61] Außerdem ist vorgesehen, dass eine Bank die durch den Kirchensteuerabzug erlangten Daten für andere Zwecke nur verwenden darf, soweit die Steuerpflichtigen dem zugestimmt haben oder dies gesetzlich zugelassen ist.

Es ist zweifelhaft, ob die Regelungen im Einkommensteuergesetz die Betroffenen ausreichend über die Bedeutung der Einwilligung in die Verarbeitung von Daten über die Religionszugehörigkeit und die Rechtsfolgen beim Fehlen der Einwilligung aufklären. In keinem Fall entspricht der allgemeine Verweis auf diese Regelungen im EStG durch § 3 Abs. 5 des Entwurfs für ein Kirchensteuergesetz Berlin jedoch den Vorgaben des Berliner Datenschutzgesetzes. Nach § 6a Abs. 1 BlnDSG handelt es sich bei Angaben zur religiösen Überzeugung um eine besondere Kategorie von personenbezogenen Daten. Diese sensitiven Daten dürfen nur auf der Grundlage eines konkreten Erlaubnistatbestandes in einer besonderen Rechtsvorschrift, die den Zweck der Verarbeitung hinreichend bestimmt, verarbeitet werden.

In einer ersten Stellungnahme hat die Senatsverwaltung für Finanzen erklärt, sie sehe keinen Anlass für die Schaffung solcher Befugnisnormen.

Wegen der besonderen Sensitivität des Merkmals „Religionszugehörigkeit" im Zusammenhang mit der Einbehaltung der Kapitalertragssteuer sind umfassende und normenklare Regelungen zur Verarbeitung dieses Datums in das Berliner Kirchensteuergesetz aufzunehmen.

61 § 51 a Abs. 2 c und d EStG

7.3 Vorlage von Mietverträgen im Besteuerungsverfahren eines Vermieters

Aus der Praxis

Der Vermieter eines Zwölffamilienhauses beschwerte sich darüber, dass das Finanzamt von ihm im Rahmen der Ermittlung seiner Einkünfte aus Vermietung und Verpachtung die Vorlage der vollständigen Mietverträge aller Mietparteien und eine Begehung seiner Wohnung verlangt habe.

Das Finanzamt begründete die Datenerhebung damit, dass es im Rahmen der Einkünfte aus Vermietung und Verpachtung zu prüfen habe, inwieweit Erhaltungsaufwendungen den vermieteten Wohnungen oder der vom Vermieter selbst genutzten Wohnung zuzuordnen sind. Dabei diene die Vorlage der Mietverträge dazu, die Höhe der Mieteinnahmen zu verifizieren.

Nach der Abgabenordnung ist das Finanzamt berechtigt, die für die Aufklärung des steuerlichen Sachverhaltes relevanten Daten zu erheben. Die Erhebung von personenbezogenen Daten ist jedoch nur dann zulässig, wenn deren Kenntnis für die Erfüllung der Aufgaben des Finanzamtes auch tatsächlich erforderlich ist. Erforderlich ist die Kenntnis der Daten nur dann, wenn das Finanzamt seine Aufgabe im jeweiligen konkreten Einzelfall ohne diese Daten nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Darüber hinaus müssen die Daten auch für die Aufgabenerfüllung geeignet sein. Dabei sind unter Beachtung des Grundsatzes der Verhältnismäßigkeit die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen.

Insofern ist das Finanzamt grundsätzlich berechtigt, zur Bestimmung des betrieblichen Anteils der vom Vermieter genutzten Wohnung Daten zu erheben. Soweit die Daten durch eine Inaugenscheinnahme der Wohnung der steuerpflichtigen Person erhoben werden sollen, ist zu beachten, dass diese Maßnahme mit einem erheblichen Eingriff in die Privatsphäre verbunden ist. In Anwendung des Grundsatzes der Verhältnismäßigkeit ist eine derartige Maßnahme daher nur als „Ultima Ratio“ vorzunehmen, also wenn alle anderen Möglichkeiten der Nachweisführung durch die Steuerpflichtigen ausgeschlossen sind.

Durch die Vorlage der vollständigen Mietverträge erhält das Finanzamt eine Vielzahl von Angaben über die persönlichen Verhältnisse der Mieterinnen und

Mieter (wie Name, Vorname, Beruf, Familienverhältnisse). Diese Angaben sind für die Ermittlung der steuerpflichtigen Einkünfte des Vermieters aus Vermietung und Verpachtung grundsätzlich nicht erforderlich. Ausreichend dafür ist vielmehr die Feststellung, in welchem Umfang das Mietobjekt tatsächlich vermietet ist und in welcher Höhe der Vermieter dafür Mietzins eingenommen hat. Als Nachweise können Kontoauszüge und Mietquittungen (ohne personenbezogene Angaben zu den Mietparteien) dienen. Warum darüber hinaus im konkreten Einzelfall die vollständigen Mietverträge (mit allen personenbezogenen Mieterdaten) erforderlich waren, konnte die Finanzverwaltung nicht darlegen.

Da Angaben zu den Mieterinnen und Mietern für die Ermittlung der steuerpflichtigen Einkünfte des Vermieters grundsätzlich nicht erforderlich sind, ist die Erhebung dieser personenbezogenen Daten über Dritte durch das Finanzamt in der Regel unzulässig.

8. Sozialordnung

8.1 Sozial- und Jugendverwaltung

8.1.1 Kinderschutzgesetz: Eltern unter Generalverdacht?

Nachdem in einigen Bundesländern bereits Kinderschutzgesetze in Kraft getreten sind, liegt nun auch der Entwurf für ein Berliner Gesetz zum Schutz und Wohl des Kindes (Stand: 2. Dezember 2008) vor. Das Gesetz verfolgt den Zweck, den Kinderschutz im Land Berlin zu verbessern. Ein Ziel, das es zu unterstützen gilt.

Die federführende Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz hat uns bereits bei der Erstellung des Referentenentwurfs beteiligt, sodass wir unsere datenschutzrechtlichen Erwägungen frühzeitig einbringen konnten. Erfreulicherweise wurden einige unserer Anregungen übernommen. Allerdings sind noch immer ganz erhebliche datenschutzrechtliche Bedenken anzumelden.

Die Früherkennungsuntersuchungen für Kinder (U4 bis U9) sollen zwar nicht verpflichtend gemacht werden. Es ist jedoch ein verbindliches Einladungswesen zu den weiterhin freiwilligen Untersuchungen eingeplant. Zu diesem Zweck ist bei der Charité ein Berliner Kinder-Vorsorgezentrum vorgesehen, das die Daten aller Berliner Kinder der entsprechenden Altersgruppen (bis zum 6. Lebensjahr) und ihrer Eltern aus dem Melderegister erhält. Kinderärztinnen und -ärzte werden verpflichtet, Bescheinigungen über die Durchführung der Früherkennungsuntersuchungen an die Charité zu übersenden. Diese führt einen Datenabgleich der Meldedaten mit den eingegangenen Untersuchungsbescheinigungen durch und filtert die Daten derjenigen Kinder heraus, für die eine Untersuchungsbescheinigung nicht vorliegt. Die Eltern werden dann aufgefordert, die Untersuchung nachzuholen. Gehen Eltern mit ihren Kindern trotzdem nicht zu den Vorsorgeuntersuchungen, wird der Kinder- und Jugendgesundheitsdienst des Gesundheitsamtes informiert, der bei den betroffenen Familien einen Hausbesuch durchführt. Falls sich der Verdacht einer

Kindeswohlgefährdung erhärtet, wird das Jugendamt informiert, das sich dann um die Familie kümmert.

Wir haben gegen dieses verbindliche Einladungswesen und Rückmeldeverfahren verfassungsrechtliche Bedenken. Zum einen bestehen erhebliche Zweifel daran, ob die Überwachung der Teilnahme an den Früherkennungsuntersuchungen ein geeignetes Mittel ist, Gefährdungen des Kindeswohls frühzeitig zu erkennen und zu verhindern. Zum anderen greift die vollständige Erfassung aller Berliner Kinder und ihrer Eltern erheblich in ihr Recht auf informationelle Selbstbestimmung ein. Diese werden unter einen Generalverdacht gestellt, obwohl nicht ansatzweise Anhaltspunkte für eine Kindeswohlgefährdung vorliegen. Allein die Tatsache, dass Kinder – aus welchen Gründen auch immer – nicht an einer Vorsorgeuntersuchung teilgenommen haben, führt zu einem Hausbesuch durch das Gesundheitsamt.

Besonders zu kritisieren ist, dass der Gesetzentwurf keine Datenverarbeitungsregelungen enthält. Es ist also völlig unklar, wie die Daten der Kinder und ihrer Eltern verarbeitet und gespeichert werden und wann sie zu löschen sind. Die Datenverarbeitung soll in einer später zu erlassenden Rechtsverordnung geregelt werden. Diese Verfahrensweise ist angesichts des mit der Datenverarbeitung durch das Berliner Kinder-Vorsorgezentrum verbundenen erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung jedoch nicht akzeptabel und verstößt gegen die vom Bundesverfassungsgericht aufgestellten Grundsätze zum Vorbehalt des Gesetzes. Danach können erhebliche Grundrechtseingriffe nicht allein in einer Rechtsverordnung geregelt werden, sondern müssen zumindest in den wesentlichen Zügen gesetzlich vorgezeichnet sein.

Betrachtet man die in der Vergangenheit bekannt gewordenen tragischen Fälle gravierender Kindeswohlgefährdungen, zeigt sich, dass in keinem der bekannt gewordenen Fälle Datenschutzregelungen notwendige Mitteilungen verhindert haben. Sofern der Gesetzentwurf das Ziel verfolgt, bei der Wahrnehmung des Schutzauftrages bei Kindeswohlgefährdung die Kooperation zwischen allen für den Kinderschutz wichtigen Einrichtungen zu verbessern, begrüßen wir dies ausdrücklich. Eine bessere Kooperation der beteiligten Stellen und die Schaffung von lokalen Netzwerken ist ein sinnvolles Instrument, um betroffenen Familien die notwendigen Hilfen im Zusammenwirken mehrerer Beteiligter anbieten zu können.

Allerdings sind Kooperationsvereinbarungen nicht geeignet, bestehende Datenschutzvorschriften außer Kraft zu setzen und über die Gesetze hinausgehende Datenübermittlungsbefugnisse zu schaffen. Ein Informationsaustausch muss also immer im Einklang mit den bestehenden Datenschutzvorschriften stehen.

Überdies stellt die Wahrung von Diskretion und Vertraulichkeit zwischen der helfenden Stelle (wie Ärztin/Arzt, Gesundheitsamt, Jugendamt) und den Betroffenen die entscheidende Grundlage für den Aufbau einer Vertrauensbeziehung dar. Die Betroffenen werden sich nur dann offenbaren, wenn sie sicher sein können, dass mit den preisgegebenen Informationen vertraulich umgegangen wird, ihr Recht auf informationelle Selbstbestimmung also gewahrt wird.

Vor diesem Hintergrund ist die Aussage „Kinderschutz geht vor Datenschutz", mit der wir immer wieder konfrontiert werden, eine kontraproduktive Leerformel. Es wird der Eindruck erweckt, die bestehenden Datenschutzgesetze würden in Fällen von Kindeswohlgefährdungen die zur Abwehr der Gefahr ggf. notwendige Informationsweitergabe verhindern und müssten durch einen außerhalb der Gesetze stehenden „Grundsatz" ausgehebelt werden.

Tatsächlich wird in der Praxis häufig ein falsch verstandener Datenschutz als Hindernis für eine notwendige Kooperation angeführt. In erster Linie sind die in Kontakt zu der Familie stehenden Personen und Institutionen gehalten, im Rahmen ihrer Möglichkeiten Hilfsangebote zu unterbreiten und in Fällen möglicher Kindeswohlgefährdungen mit den notwendigen Maßnahmen dem Verdacht nachzugehen. In Fällen, in denen sich der Verdacht erhärtet, andere Handlungsmöglichkeiten zur Abwehr der Gefährdung nicht zu Verfügung stehen und eine Information des Jugendamtes erforderlich erscheint, stehen datenschutzrechtliche Vorschriften einer tatsächlich erforderlichen Datenübermittlung nicht entgegen. Regelmäßig werden hier die Voraussetzungen des rechtfertigenden Notstandes gegeben sein, sodass sich die handelnden Personen nicht selbst strafrechtlicher Verfolgung aussetzen müssen.

Allerdings kann ein staatlicher Schutz von gefährdeten Kindern nur funktionieren, wenn Vertrauensverhältnisse zu betroffenen Familien geschützt und nicht hinter deren Rücken beliebig Informationen ausgetauscht werden. Insofern setzt Kinderschutz Datenschutz voraus.

Der Gesetzgeber ist aufgerufen, den mit dem vorliegenden Gesetzentwurf verbundenen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung aller Berliner Kinder und ihrer Personensorgeberechtigten abzuwenden. Der Entwurf muss dringend nachgebessert werden. Es ist ein angemessener Ausgleich zwischen dem hohen Verfassungsgut des Kinderschutzes einerseits und dem Recht auf informationelle Selbstbestimmung aller von der Regelung betroffenen Kinder und ihrer Eltern andererseits herzustellen.

8.1.2 Jobcenter: Diskretion unter der Lupe

Seit Jahren erhalten wir viele Beschwerden, die sich auf die mangelnde Diskretion bei der Beratung in den Jobcentern beziehen[62]. Die bereits 2006 eingeleiteten Kontrollen der Jobcenter hinsichtlich ihrer räumlichen Bedingungen zur Gewährleistung vertraulicher Gespräche wurden fortgesetzt und haben inzwischen alle zwölf Berliner Jobcenter erfasst. Dabei wurden folgende Feststellungen getroffen:

Die Bearbeitung von Kundenanliegen sowie die Ausstattung der Jobcenter sind im Wesentlichen standardisiert. Diese Einheitlichkeit lässt darauf schließen, dass nach Vorgaben der Bundesagentur für Arbeit verfahren wird.

Soweit keine Terminvereinbarung mit einer Mitarbeiterin oder einem Mitarbeiter vorliegt, wenden sich die Kundinnen und Kunden grundsätzlich zunächst an den Empfangstresen, der mit mehreren Arbeitsplätzen ausgestattet ist. Hier wird erstmalig das Anliegen in Kürze erfasst und der Fall zu einer Sachbearbeiterin oder einem Sachbearbeiter vermittelt. Die Bearbeitung erfolgt entweder in einem Großraumbüro oder in einem Büro, das mit bis zu zwei Dienstkräften besetzt ist.

Sobald in einem Büroraum mehr als eine Person gleichzeitig ihr Anliegen vorträgt, können die anwesenden Jobsuchenden dies beiläufig mithören. Die räumliche Ausstattung sieht für die Großraumbüros lediglich eine optische Trennung vor, in kleineren Büros fehlt auch diese. Die akustische Trennung

62 JB 2005, 3.1; JB 2006, 9.3; JB 2007, 11.3

ist unzureichend. Um dem Problem zu begegnen, wurden Absprachen mit allen Jobcentern getroffen, dass für Kundinnen und Kunden, die ihr Anliegen vertraulich vortragen möchten, Einzelbüroräume vorhanden sind, in denen sie mit der Sachbearbeiterin oder dem Sachbearbeiter allein sprechen können. Auf diese Möglichkeit der diskreten Gesprächsführung soll in den Warteräumen und Großraumbüros hingewiesen werden. Die Diskretionsregelung gilt auch für kleinere Büros, in denen mehr als eine Person gleichzeitig empfangen wird.

Drei Jobcenter verfügen über Bearbeitungsbereiche, die direkt an öffentliche Straßen grenzen. Dort besteht die Möglichkeit, dass Passantinnen und Passanten durch die Fenster Einsicht auf Akten und Computerbildschirme nehmen. Ein Sichtschutz ist meistens vorhanden, wird aber oft nicht verwendet, da er die Lichtverhältnisse im Raum verschlechtert. Nach Aussagen der Jobcenter wird regelmäßig auf die Verwendung hingewiesen. Die Praxis zeigt jedoch, dass die gewünschte Wirkung nicht erzielt wird. In einem Jobcenter konnte das Problem durch Absperrungen im Außenbereich wirkungsvoll gelöst werden. Bei den anderen beiden Jobcentern ist dies aufgrund der räumlichen Gegebenheiten nicht möglich, sodass hier noch nach einer Lösung gesucht werden muss.

Die Jobcenter sind verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Vertraulichkeit der Beratungsgespräche zu gewährleisten. Es ist ferner zu verhindern, dass Sozialdaten Unbefugten zur Kenntnis gelangen können. Die Jobcenter sind zudem verpflichtet, auf Wunsch Einzelberatungen in einem separaten Raum anzubieten. Die Betroffenen sind durch gut sichtbare Aushänge auf diese Möglichkeit hinzuweisen. Zusätzlich sollten auch in den Großraumbüros Maßnahmen getroffen werden, die die beiläufige Kenntnisnahme verhindern.

Die Problematik der beiläufigen Kenntnisnahme durch Dritte erstreckt sich auf einen weiteren Bereich, der nicht ohne weiteres optisch oder akustisch wahrgenommen wird: Es geht um die Versendung personenbezogener Daten per E-Mail. Einen Einzelfall nahmen wir zum Anlass, um die generelle Verfahrensweise in den Jobcentern zu prüfen.

Insgesamt wurden drei Varianten verwendet: Der normale Brief über Postzustellungsdienste, Mitteilungen über Fax und E-Mail-Versand. Die ersten beiden Varianten können bei Einhaltung der entsprechenden Sorgfalt als datenschutzgerecht angesehen werden, da bei beiden Kommunikationsformen die Sendungen relativ gut gegen unbefugte Kenntnisnahme geschützt werden können. Der E-Mail-Versand verstößt gegen das datenschutzrechtliche Gebot der Sicherstellung der Vertraulichkeit auf dem Übertragungsweg, wenn der Versand unverschlüsselt erfolgt. Solange die Jobcenter ebenso wenig wie die Kundinnen und Kunden über die technischen Voraussetzungen für einen verschlüsselten Versand verfügen, liegt beim unverschlüsselten Versand „sensitiver" personenbezogener Daten per E-Mail durch die Jobcenter ein schwerer Mangel der Weitergabekontrolle nach Nr. 4 der Anlage zu § 78 a Satz 1 Sozialgesetzbuch X (SGB X) vor. Die Daten übermittelnden Stellen haben zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Bei der Übertragung von Daten per E-Mail kann dies nur mit der Verschlüsselung der Daten sichergestellt werden.

Zur Versendung von E-Mails gab es keine einheitlichen Regelungen, sodass die Art und Weise des Versands im Ermessen der zuständigen Sachbearbeitung lag. Es bestand Einigkeit, dass zukünftig bei der Verwendung von E-Mail eine Verschlüsselung zwingend einzusetzen ist. Uns wurde zugesagt, dass die Jobcenter für sich entsprechende Anweisungen erarbeiten und umsetzen werden.

Der unverschlüsselte Versand von Sozialdaten per E-Mail ist stets unzulässig, weil im Internet die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten nicht sichergestellt werden kann.

8.1.3 Nachlese: Schwärzungen im Mietvertrag

Die generelle Anforderung von Unterlagen durch Jobcenter ohne Möglichkeit für Sozialleistungsbedürftige, nicht leistungsrelevante Daten zu schwärzen, ist unzulässig. Das gilt insbesondere für die Vorlage von Mietverträgen.[63]

Mietverträge enthalten eine Vielzahl von Daten, die für die Feststellung der Höhe des Leistungsbedarfs nicht erforderlich sind. Oftmals enthält ein Mietvertrag individuelle Regelungen etwa über die Haltung eines bestimmten Haustieres oder über Ruhezeiten. Dies alles ist für die Bearbeitung des Leistungsantrages nicht erforderlich. Auch die Angaben zur vermietenden Person sind, außer in Ausnahmefällen, in denen die Miete direkt an sie überwiesen wird, leistungsrechtlich nicht relevant und können somit geschwärzt werden. Die Sozialleistungsträger haben die Pflicht, die Bedürftigen auf die Möglichkeit des Schwärzens hinzuweisen. Nur die leistungsrechtlich relevanten Angaben müssen auf dem Mietvertrag erkennbar sein. Die Anforderung eines ungeschwärzten Mietvertrages ist ausnahmsweise zulässig, wenn im Einzelfall konkrete Anhaltspunkte für den Verdacht einer Manipulation des Mietvertrages bestehen. Dann kann der Leistungsträger die Vorlage eines ungeschwärzten Mietvertrages verlangen und muss es begründen. Daher war das Vorgehen eines Jobcenters zu beanstanden.

Zwar hat das Bundessozialgericht entschieden[64], dass entgegen unserer bisherigen Auffassung[65] die Jobcenter vollständige Kontoauszüge verlangen dürfen. Sensitive Informationen (z.B. Zahlung von Gewerkschaftsbeiträgen) dürfen allerdings auch dort geschwärzt werden. Diese Grundsätze lassen sich jedoch nicht auf Mietverträge übertragen, die häufig noch andere für den Leistungsbezug irrelevante Daten enthalten.

Auf unseren Vorschlag hat der parlamentarische Unterausschuss „Datenschutz und Informationsfreiheit“ eine Beschlussempfehlung gefasst, nach der darauf hinzuwirken ist, dass die Jobcenter nur die erforderlichen Daten erheben und Antrag stellende Personen geschwärzte Mietverträge vorlegen dürfen, worauf sie hinzuweisen sind.

63 JB 2007, 7.2.3

64 Urteil vom 19. September 2008 – B 14 AS 45/07 R

65 Vgl. http://www.datenschutz-berlin.de/content/veroeffentlichungen/hinweise

8.2 Gesundheit

8.2.1 Online-Gesundheitsakten

Aus der Praxis

Zwei Firmen baten uns um Beratung, weil sie personenbezogene Gesundheitsdaten auf Servern im Internet ablegen wollen. Der Zweck solcher Angebote ist, Patientinnen und Patienten eine eigenständige, vollständige und jederzeit verfügbare Dokumentation ihrer Gesundheitsunterlagen zu ermöglichen. Auf diese Weise soll, ähnlich wie für die elektronische Gesundheitskarte geplant, ein geordneter Datensatz über alle Arztbesuche, verordnete Medikamente, Krankenhausaufenthalte und Basisdaten wie Blutgruppe und Impfungen entstehen. Je nach Konzept ist vorgesehen, dass behandelnde Ärztinnen und Ärzte die Dokumentation direkt einsehen und ergänzen können, soweit die behandelte Person damit einverstanden ist. Darüber hinaus soll es ärztlichem Personal ermöglicht werden, im Einzelfall auch ohne Beteiligung der Patientin oder des Patienten – etwa bei einem Unfall – zeit- und ortsunabhängig auf die erforderlichen medizinischen Basisinformationen (Notfalldaten) zuzugreifen.

Ähnliche Konzepte werden bereits von weiteren Firmen in anderen Bundesländern und ausländischen Unternehmen umgesetzt, die möglicherweise künftig auch auf dem deutschen Gesundheitsmarkt auftreten werden. Ein deutsches Unternehmen bietet seine Dienstleistung bereits in Kooperation mit einer Krankenkasse an.

Bei Gesundheitsdaten handelt es sich um sensitive und daher besonders schutzwürdige Informationen, deren Verarbeitung nur unter engen Voraussetzungen erlaubt ist. Jeder Person, die solche Daten auf einem Internetserver ablegt, sollte aber bewusst sein, dass dieser rechtliche Schutz nicht immer gewährleistet werden kann und nicht ausreicht, um die Daten wirksam vor Missbrauch zu schützen. Die Gesundheitsdaten werden hier nicht in der Arztpraxis geführt und aufbereitet, sondern von dem Dienstanbieter im Patientenauftrag gespeichert. Daher unterliegen sie auch nicht der ärztlichen Schweigepflicht und beim Dienstleister keinem Beschlagnahmeschutz. Das Problem verschärft sich dadurch, dass die Daten von sehr vielen Patientinnen und Patienten zentral an einer Stelle verfügbar sind.

Im Gegensatz zu medizinischen Fallakten, in denen die an einer Therapie beteiligten Ärztinnen und Ärzte nur die für diese Therapie notwendigen Daten ablegen, ist bei obigen Konzepten auch der beabsichtigte große Umfang der Daten und deren lange Speicherdauer als kritisch einzuschätzen, da sie das Risiko einer missbräuchlichen Nutzung erhöhen. Schließlich besteht die Gefahr, dass Dritte (z.B. Arbeitgeber, Versicherungen) auf die Nutzerinnen und Nutzer dieser Angebote dahingehend einwirken, ihre zentral gesammelten Gesundheitsdaten zu offenbaren. Aus technischer Sicht sind solche Angebote aus folgenden Gründen problematisch:

- Die Konzepte sehen den Abruf der Daten über normale Internet-PCs vor. Es ist jedoch einer Privatperson kaum möglich, gewöhnliche Internet-PCs soweit abzusichern, dass ihnen besonders sensitive Daten anvertraut werden können. Man muss immer davon ausgehen, dass solche Daten in die Hände von Dritten geraten, insbesondere wenn nicht nur der eigene Rechner verwendet wird.
- Die Speicherung von personenbezogenen Daten auf Servern mit Zugang zum Internet birgt grundsätzlich ein Risiko, da eine hundertprozentige Absicherung der Server vor Angriffen nicht garantiert werden kann und immer wieder erfolgreiche Angriffe zu beobachten sind. Im Datenspeicher sollen die Gesundheitsdaten zwar (zumindest bei den Berliner Firmen) verschlüsselt abgelegt werden, aber zum Zeitpunkt des Zugriffs durch die Nutzenden hat der Webdienst Zugriff auf die zur Entschlüsselung benötigten Schlüssel. Ein kompromittierter Webdienst könnte daher abgerufene Daten auch an Dritte weiterleiten. Dies hat zur Folge, dass ein erfolgreicher Angriff auf den Webserver unberechtigten Dritten einen Zugriff auf die Gesundheitsdaten eröffnet.
- Da die Konzepte eine leichte Zugänglichkeit der Gesundheitsdaten vorsehen, wird meist auf sichere Authentifizierungstechniken, wie z.B. durch Chipkarten, verzichtet. Die meisten Dienste verlangen stattdessen nur die Eingabe von Nutzernamen und Passwort. Bei unachtsamer Nutzung oder wenn ein durch Schadsoftware unsicher gewordener PC genutzt wird, können Angreifer die Anmeldedaten ausspähen und mit allen Möglichkeiten der Einsichtnahme und Änderung auf die Daten zugreifen.

- Grundsätzlich sollten sich alle, die solche Dienste nutzen wollen, bewusst machen, dass deren Anbieter jederzeit die Möglichkeit haben, auf die abgelegten Gesundheitsdaten zuzugreifen. Da zudem nicht alle Angebote ein tragfähiges kommerzielles Konzept vorweisen, ist langfristig eine anderweitige Verwendung der Daten, z.B. zu Zwecken der Werbung oder der Forschung, nicht auszuschließen. Auch ist offen, was mit den Daten bei einer Insolvenz des Anbieters geschieht.

Obwohl eine abschließende Bewertung noch aussteht, haben wir den Firmen die datenschutzrechtlichen und sicherheitstechnischen Probleme aufgezeigt und sie ermutigt, sichere Konzepte zu entwickeln. Zur Speicherung und Übermittlung derart sensitiver Daten sollten keine Dienstleistungen angeboten und genutzt werden, die einen geringeren Schutz bieten, als es technisch möglich wäre.

Die Sicherheitskonzepte für die elektronische Gesundheitskarte und insbesondere die elektronische Patientenakte als deren Anwendung sollten als Maßstab für alle patientengeführten Gesundheitsakten im Internet herangezogen werden.

8.2.2 Was bewirkt eine Beschwerde bei der Ärztekammer?

Aus der Praxis

Mehrere Patientinnen und Patienten haben sich darüber beschwert, dass sie keine Informationen über den Ausgang ihres bei der Berliner Ärztekammer eingeleiteten Beschwerdeverfahrens erhalten. Sie hatten sich dorthin gewendet, um eine aus ihrer Sicht nicht ordnungsgemäße ärztliche Untersuchung oder Behandlung prüfen zu lassen.

Die Ärztekammer überwacht nach dem Berliner Kammergesetz die Einhaltung der Berufspflichten ihrer Mitglieder. Sie ermittelt wegen berufsrechtlicher Verstöße und leitet erforderlichenfalls berufsrechtliche Maßnahmen ein. Die Sanktionsmöglichkeiten der Kammer bei Verstößen gegen das Berufsrecht reichen je nach Schwere des Verstoßes von einer Untersagungsverfügung über die berufsordnungsrechtliche Rüge bis hin zur Einleitung eines Untersuchungs- oder berufsgerichtlichen Verfahrens. Auch schriftlichen Beschwerden von Patientinnen und Patienten oder Dritten wird in jedem Einzelfall nachgegangen.

Bislang sieht sich die Ärztekammer durch das Datenschutzrecht daran gehindert, den Beschwerdeführenden den Stand und das Ergebnis der dortigen Ermittlungen über Verstöße gegen Berufspflichten durch Kammermitglieder mitzuteilen oder über ergriffene berufsrechtliche Maßnahmen zu informieren.

Nach derzeitiger Rechtslage sehen auch wir allenfalls beschränkte Möglichkeiten für die Betroffenen, Informationen über den Stand ihrer Beschwerde bei der Ärztekammer zu erhalten. Ein Anspruch der Beschwerde führenden Person gegen die Ärztekammer auf Auskunft oder Akteneinsicht besteht im berufsgerichtlichen Verfahren nicht. Spätestens nach der Entscheidung des Kammervorstandes, ein förmliches Untersuchungsverfahren gegen den Beschwerdegegner (Kammermitglied) einzuleiten, handelt es sich um ein Verwaltungsverfahren zwischen der Kammer und der beschuldigten Person als Verfahrensbeteiligte. Die Beschwerde führende Person ist ggf. als Zeugin zu hören, aber nicht selbst akteneinsichtsberechtigte Beteiligte. Der Ausgang des Verfahrens hat auch keine rechtliche Wirkung für die Beschwerde führende Person und dient allenfalls mittelbar ihren Interessen, indem die künftige Einhaltung der Berufspflichten erreicht werden soll.

Bis zur Entscheidung über die Einleitung eines Untersuchungsverfahrens führt die Kammer in der Regel berufsrechtliche Vorermittlungen durch. In dieser Phase scheitert ein Akteneinsichtsrecht der Beschwerdeführenden bereits daran, dass es sich hierbei um ein informelles Verfahren handelt, auf das die Vorschriften über die Akteneinsicht durch Beteiligte nach dem Verwaltungsverfahrensrecht keine direkte Anwendung finden.

Danach bleibt der Beschwerde führenden Person nur die Möglichkeit, einen Auskunftsanspruch nach § 16 Abs. 1 Berliner Datenschutzgesetz (BlnDSG) geltend zu machen. Dabei ist allerdings zu berücksichtigen, dass sich der Auskunftsanspruch nur auf die Daten bezieht, die **zu der betroffenen Person** gespeichert sind. Soweit ein Verwaltungsverfahren im Sinne des § 9 Verwaltungsverfahrensgesetz (VwVfG) geführt wird, ergibt sich aus dessen Regelungen zur Beteiligteneigenschaft zugleich, zu welcher Person die im Verfahren verarbeiteten Daten gespeichert werden. Das bedeutet, dass Stellungnahmen der beschuldigten Person in einem dem Berufsgerichtsverfahren vorgeschalteten Untersuchungsverfahren grundsätzlich zur beschuldigten und nicht zur Beschwerde führenden Person gespeichert werden. Der datenschutzrechtli-

che Auskunftsanspruch liefe damit insoweit ins Leere. Davon abgesehen sind Geheimhaltungsinteressen der beschuldigten Person zu berücksichtigen.

Ein Recht auf Auskunft über Stand, Inhalt und Ausgang des Verfahrens und ggf. ergriffene berufsrechtliche Maßnahmen besteht derzeit nicht. Im Hinblick auf eine gesteigerte Bürgerfreundlichkeit und Transparenz im Gesundheitswesen halten wir die Schaffung einer Rechtsgrundlage im Berliner Kammergesetz für wünschenswert und haben dies gegenüber dem Abgeordnetenhaus angeregt. Nur mit einer solchen Regelung können die betroffenen Patientinnen und Patienten erfahren, was aus „ihrer" Beschwerde geworden ist und ob sie tatsächlich etwas bewirkt hat.

8.2.3 Praxisaufgabe oder Praxisübergabe – Wohin mit den Patientenakten?

Aufgrund mehrerer Eingaben von betroffenen Patientinnen und Patienten haben wir uns verstärkt mit der Frage beschäftigt, wie mit Patientenakten im Falle einer Praxisaufgabe oder Praxisübergabe zu verfahren ist. Wir nehmen dies zum Anlass, auf die wichtigsten Grundsätze hinzuweisen.

Auch nach Aufgabe einer Arztpraxis sind die ärztlichen Aufzeichnungen und Untersuchungsbefunde weiterhin aufzubewahren. Das Berufsrecht sieht dafür eine Frist von zehn Jahren nach Abschluss der jeweiligen Behandlung vor. Die Akten können in den praxiseigenen oder in angemieteten Räumen aufbewahrt werden. Letzteres setzt allerdings voraus, dass der Praxisbelegschaft im Mietvertrag ein alleiniges Zugriffsrecht eingeräumt wird und dieses durch organisatorische Maßnahmen gesichert ist. Kommen die Praxisinhaber dieser Aufbewahrungsverpflichtung nicht nach, ist die Ärztekammer befugt, die Unterlagen zu verwahren und zu verwalten oder durch Dritte verwahren und verwalten zu lassen. Alternativ können die Aufzeichnungen auch den Patientinnen und Patienten übergeben werden, damit diese sie einer weiterbehandelnden Ärztin oder einem Arzt ihrer Wahl aushändigen. Die Aushändigung sollte dann – aus Gründen der späteren Beweisbarkeit – schriftlich quittiert werden.

Bei der Übergabe einer Praxis an eine Nachfolgerin oder einen Nachfolger ist das Patientengeheimnis im Hinblick auf die bereits vorhandenen Patienten-

akten zu beachten. Eine Praxisveräußerung einschließlich der Übertragung der Patientenkartei und dazugehöriger Unterlagen ist ohne die eindeutige und unmissverständliche Einwilligung der Patientinnen und Patienten wegen Verstoßes gegen die ärztliche Schweigepflicht grundsätzlich unwirksam. Entsprechend regelt die Berufsordnung der Ärztekammer, dass die Ärztin oder der Arzt, denen bei einer Praxisübergabe ärztliche Aufzeichnungen über Patientinnen und Patienten ausgehändigt werden, diese Aufzeichnungen unter Verschluss halten muss und sie nur mit Einwilligung der behandelten Person einsehen oder weitergeben darf.

Wenn die Zustimmung derjenigen Patientinnen und Patienten, die die Praxis vor Übertragung nicht mehr aufsuchen, nicht eingeholt werden kann, bietet sich eine vertragliche Vereinbarung an, nach der die erwerbende Person die Patientenunterlagen für die Verkäuferin oder den Verkäufer verwahrt und sich dazu verpflichtet, Einsicht nur dann zu nehmen, wenn eine Patientin oder ein Patient in seiner Praxis zur Weiterbehandlung erscheint. Die alte Akte darf dann bei deren oder dessen Einverständnis entnommen und durch den die erwerbende Person fortgeführt oder mit einer laufenden Patientenkartei des Erwerbers zusammengeführt werden. Das Einverständnis ist in der Akte zu dokumentieren. Bei elektronisch geführten Akten ist der Altbestand zu sperren und der Zugriff hierauf z.B. mit einem Passwort zu sichern.

Bei einer Praxisübergabe sind die ärztliche Schweigepflicht und das informationelle Selbstbestimmungsrecht der Patientinnen und Patienten zu wahren. Ein Zugriff auf die vorhandenen Patientenakten durch den Praxisnachfolger ist nur bei Vorliegen einer Einwilligung der behandlungsbedürftigen Person zulässig.

8.2.4 Ungestörtes Stöbern in Patientenakten

Im März konfrontierte uns eine Zeitung mit der Information, auf dem Gelände des Helios Klinikums in Berlin-Buch würden in einem nur unzureichend gesicherten Gebäude zahlreiche Patientenakten und Befundmaterial gelagert. Eine noch am selben Tag durch uns vor Ort durchgeführte Prüfung bestätigte den Vorwurf.

Bei dem fraglichen Gebäude handelt es sich um die alte Pathologie des Krankenhauses, die 1991 stillgelegt wurde. Eine ordnungsgemäße Räumung des Gebäudes wurde nie durchgeführt. Bei unserer Begehung waren sowohl Mobiliar und technisches Gerät als auch Patientenakten (z.B. Sektionsberichte) und unzählige histologische Schnitte (Glas- und Paraffineinschluss) noch vorhanden. Bis in das Jahr 2003 wurden zudem weitere Patientenunterlagen in einem Archivraum im Erdgeschoss des Gebäudes zwischengelagert. Es handelte sich dabei vornehmlich um Befundberichte zu Krebsfrüherkennungsuntersuchungen.

An dem neueren Teil des Gebäudes befinden sich rundherum Fenster in Brusthöhe. Bei den Eingangstüren handelt es sich um Glastüren. Zahlreiche dieser Fenster und eine Eingangstür waren eingeschlagen, wodurch ein Zugang zum Gebäude durch Unbefugte leicht möglich war. Die Tür zu dem Archivraum war aufgebrochen. Offensichtlich waren in den vergangenen Jahren häufiger Personen in das Gebäude eingedrungen. Darauf deuteten Graffitis und Verwüstungen in einzelnen Räumen hin. Das Klinikum teilte uns mit, dass man am Tag vor unserer Ortsbegehung einen Hinweis auf einen Einbruch erhalten habe.

Zum Zeitpunkt unserer Prüfung hatte man damit begonnen, die Schäden an Fenstern und Türen provisorisch zu beseitigen sowie das Gebäude zu räumen und zu sichern. Wir konnten erreichen, dass das Gebäude bis zur vollständigen Sicherstellung der Patientenakten rund um die Uhr durch Sicherheitspersonal überwacht wird.

Es stellt einen erheblichen organisatorischen Mangel der Datenverarbeitung dar, wenn Patientenunterlagen, die der ärztlichen Schweigepflicht unterliegen, in derart ungeeigneten Räumen gelagert werden. Allerdings ist der Vorfall durch die Klinikleitung bisher nicht abschließend untersucht und aufgearbeitet worden. Wir haben dringend dazu geraten, eine Krankenhaus-Archivordnung zu erlassen, in der klare Regelungen u.a. zur Verantwortlichkeit, zur Vertraulichkeit, zur Aktenanforderung, zur Aktenauslieferung, zur Einsichtnahme und zur Datensicherheit getroffen werden.

Nachdem schon im letzten Jahr auf dem Gelände des ehemaligen Leichenschauhauses Patientenakten im Bauschutt aufgetaucht sind, ist jetzt erneut ein Fall bekannt geworden, in dem vertrauliche Gesundheitsdaten für Unbefugte frei zugänglich waren. Es wurden grundlegende Anforderungen der technisch-organisatorischen Sicherung von sensitiven Daten missachtet. Derartig gravierende Versäumnisse weisen häufig leider auch auf strukturelle Mängel in der gesamten Datenschutzorganisation eines Unternehmens hin, die es zu beseitigen gilt.

8.2.5 Outsourcing in der Charité

Im letzten Jahr[66] berichteten wir darüber, dass die Charité Aufgaben, die nicht oder nur mittelbar mit medizinischen Behandlungen verbunden sind, auf die Charité CFM Facility Management GmbH ausgelagert hat. Nun haben wir geprüft, wie dies mit dem Datenschutz und der ärztlichen Schweigepflicht zu vereinbaren ist.

Einige der dabei aufgeworfenen Fragen können nicht mit einfachen Empfehlungen zu technischen und organisatorischen Maßnahmen beantwortet werden, da man gleichzeitig der Effizienz und der Sicherheit der Patientinnen und Patienten bei den Abläufen in einem großen Klinikum hohen Stellenwert einräumen muss. Aus diesem Grunde waren wir uns mit dem Vorstand der Charité bald einig, dass die Kontrolle dazu dient, gemeinsam Lösungen zu finden, die einerseits die Auslagerung von Dienstleistungen im Krankenhaus ermöglichen und andererseits nicht im Widerspruch zu den Vertraulichkeitsregeln stehen, die zur Grundlage des besonderen Vertrauensverhältnisses zwischen medizinischem Personal und Patientinnen und Patienten gehören. Die Kontrolle soll also zu Prinzipien führen, die auch für andere Krankenhausunternehmen an Bedeutung gewinnen sollen.

Dazu haben wir die verschiedenen dem Outsourcing unterliegenden Dienstleistungen unterteilt, um eine Abschichtung der Fallgruppen und eine Fokussierung auf die schwierigen Fälle zu ermöglichen. Wir gehen von sechs Kategorien aus:

66 JB 2007, 7.3.3

A) Dienstleistungen, bei denen der Umgang mit personenbezogenen Daten grundsätzlich entfällt,

B) Dienstleistungen, bei denen nicht die ärztliche Schweigepflicht, sondern andere datenschutzrechtliche Aspekte zu beachten sind,

C) Dienstleistungen, bei denen durch eine andere Arbeitsorganisation oder verbesserte Hilfsmittel (z.B. Software) die Kenntnisnahme von patientenbezogenen Daten unterbunden werden kann,

D) Dienstleistungen, bei denen die Kenntnisnahme von patientenbezogenen Daten nicht erforderlich ist, aber nicht ausgeschlossen werden kann,

E) Dienstleistungen, bei denen die Kenntnisnahme der patientenbezogenen Daten erforderlich bzw. unvermeidlich ist,

F) Dienstleistungen, bei denen die Kenntnisnahme der patientenbezogenen Daten unvermeidlich ist, die aber nicht von eigenem Personal des Krankenhauses erbracht werden können, jedoch zwingend erforderlich sind.

Die Dienstleistungen der Kategorie A) haben keine datenschutzrechtliche Relevanz. Zu den Dienstleistungen der Kategorie B) gehören alle Arbeiten, die den Umgang mit Personaldaten erforderlich machen. Die Charité hat angekündigt, für diese Leistungsbereiche einen Rahmenvertrag zur Auftragsverarbeitung zu schließen.

Bei Dienstleistungen der Kategorie C) können durch entsprechend organisierte Geschäftsabläufe Verletzungen der ärztlichen Schweigepflicht unterbunden werden. Im Bereich der internen Postdienste nehmen Beschäftigte der CFM Patientendaten im Rahmen der Vorsortierung in Patienten-, Mitarbeiter- oder nicht eindeutig zuzuordnende Post zur Kenntnis. Dies berührt jedoch nicht die ärztliche Schweigepflicht, weil die Offenbarung durch die Patientinnen und Patienten selbst (bei ausgehender Post) oder durch Dritte, nicht jedoch durch das Krankenhaus erfolgt. Hier würde das Postgeheimnis zur Geltung kommen, weil die CFM in diesem Fall als geschäftsmäßiges Postdienstleistungsunternehmen angesehen werden kann. Eingehende Post, die nicht eindeutig zugeordnet werden kann, soll verschlossen an eine bestimmte Stelle der Charité weitergeleitet werden, die die Post öffnet und damit die Adressaten ermittelt. Eine Offenbarung von Briefinhalten an die CFM erfolgt so nicht. Wir sehen in dieser Lösung einen gangbaren Weg. Offen ist noch, ob die Patientenverpflegung

in diese Kategorie C) fällt und auf Basis pseudonymisierter Daten ermöglicht werden kann. Dies wird seitens der Charité noch als problematisch angesehen. Die Telefongebührenabrechnung für die Patientinnen und Patienten kommt ohne Offenbarung personenbezogener Daten aus, wenn vorausbezahlte Telefonkarten eingesetzt werden. Dies ist in der Charité bereits der Regelfall. Ausnahmen wären auszuschließen. Generell gilt, das bei der Vergabe von Dienstleistungen geprüft werden sollte, ob sie nicht der Kategorie C) unterfallen können, d.h., es ist zu prüfen, ob die Arbeitsorganisation so gestaltet werden kann, dass es nicht zur Offenbarung von Patientendaten durch das Krankenhaus kommt.

Zu den Dienstleistungen der Kategorie D) gehören z.B. dezentrale Reinigungs-, Desinfektions- und Stationsdienste, die in den Krankenzimmern oder Behandlungsräumen erfolgen. In diesem Fall will die Charité neben Kontrolle, Weisung und Durchsetzung eines sorgsamen Umgangs mit Patientenunterlagen geeignete organisatorische Maßnahmen treffen. Dazu gehören z.B. die Verpflichtung der in der Charité Beschäftigten, sorgsam mit personenbezogenen Unterlagen umzugehen, der Verzicht auf die Angabe von Patientennamen an den Türen und in den Krankenräumen sowie die Gesprächsdisziplin bei Anwesenheit von Servicepersonal im Kranken- oder Behandlungszimmer, etwa Reinigungskräften. Bei Dienstleistungen der Kategorie D) besteht weiter Gesprächsbedarf über eine datenschutz- und schweigepflichtkonforme Lösung.

Alle Dienstleistungen, für deren Erfüllung der Umgang mit Patientendaten erforderlich ist (Kategorie E), sollen unter der uneingeschränkten Kontrolle und Weisung der in der Charité Beschäftigten durchgeführt werden, die damit „berufsmäßig tätige Gehilfen“ im Sinne von § 203 Abs. 3 Strafgesetzbuch (StGB) sind. Der eng auszulegende Gehilfenbegriff verlangt jedoch eine gewisse organisatorische Einbindung und damit die Zugehörigkeit zum Krankenhausbetrieb und muss demzufolge von Beschäftigten der Charité ausgefüllt werden. Erfasst werden dabei die Dienstleistungen in den Archiven und der Internen Postdienste, soweit die Patientendaten berührt sind (und nicht nur Mitarbeiterdaten), sowie viele Aufgaben des Betriebs der Informations-, Kommunikations- und Sicherheitstechnik (Wartungs- und Störungsdienste, die auch in den Krankenzimmern vorkommen können). Inwieweit auch Dienste des internen Krankentransports in diese Kategorie oder eher in die Kategorie D) fallen, bedarf noch der abschließenden Klärung. Dienstleistungen dieser

Kategorie können also nicht auf einen Dienstleister wie die CFM übertragen werden, sondern müssen von Beschäftigten der Charité ausgeführt werden. Zu klären wäre jedoch, ob das bei den Archivdiensten angewandte Modell der Arbeitnehmerüberlassung bei uneingeschränkten Weisungsrechten der ärztlichen Leitung auch für andere Dienstleistungen in Frage kommt.

In die Kategorie F) fallen Wartungs- und Administrationstätigkeiten bei medizintechnischen Geräten, mit denen auch personenbezogene Daten verarbeitet werden. Tatsächlich dürfte es keinem Krankenhaus, auch nicht der großen Charité, möglich sein, eigenes Wartungspersonal für die komplexen medizinischen Geräte wie z.B. Computertomografie und MRt vorzuhalten und zu qualifizieren. Andererseits dürfte es vor allem im Störungsfall nicht immer möglich sein, personenbezogene Daten der aktuell behandelten Patientinnen und Patienten so zu entfernen, dass das fremde Wartungspersonal sie nicht zur Kenntnis nehmen kann.

Es besteht Konsens, dass sich das Dilemma nur lösen lässt, entweder wenn konsequent datenschutzfreundliche Wartungsverfahren eingesetzt werden (technische Lösung), z.B. die permanente Verschlüsselung der Daten auf diesen Geräten, oder durch die Öffnung der Offenbarungsbefugnisse des Landeskrankenhausgesetzes für diese eng umrissenen Dienstleistungen (gesetzliche Lösung).

Um die Prinzipien der ärztlichen Schweigepflicht auch in den arbeitsteilig organisierten, vom komplexen Technologieeinsatz geprägten Großkrankenhäusern aufrechtzuerhalten, sind nicht nur technische und organisatorische Fantasie, sondern wahrscheinlich auch die Anpassung gesetzlicher Regeln erforderlich.

8.2.6 Migration von Verfahren der Gesundheitsämter

Die Geschäftsstelle zur Koordinierung und Beratung bezirklicher Verfahren – KoBIT – mit dem Projekt „Migration der Verfahren SpDI, BfBI und KiPsl“ ist an uns herangetreten, um unsere Meinung dazu einzuholen, welche Lösung wir bei der Umstellung auf eine neue Betriebsform befürworten würden. Bei SpDI handelt es sich um die Automationsunterstützung der Sozialpsychiatrischen Dienste, bei BfBI um das Informationssystem der Beratungsstelle für Chronisch Kranke, bei KiPsI um das Informationssystem des Kinder- und Jugendpsychiatrischen Dienstes.

Einige Bezirke hatten sich Hilfe suchend an die KoBIT gewandt, da die Antwortzeiten der Verfahren inzwischen erheblich zugenommen hatten. Als mögliche Ursache wurde die Datenbank „Access“ analysiert, die beim Handling der Datensätze einen erheblichen Rechenaufwand verursacht. Es wurde vorgeschlagen, die Verfahren auf eine leistungsfähigere Datenbank umzustellen und als Client-Server-Lösung aufzusetzen, ansonsten aber keine Änderungen vorzunehmen. Der zweite Vorschlag war, den Betrieb des Verfahrens ins ITDZ zu verlagern, eine Datenbank einzusetzen, die höheren Anforderungen genügt, und das Verfahren über eine Terminal-Server-Lösung aufzurufen. Beim dritten Vorschlag könnte das Verfahren in eine Webanwendung migriert werden, die entweder im ITDZ oder der örtlichen IT-Stelle administriert wird.

Grundsätzlich berührt die Migration der Verfahren die IT-Sicherheit, die bei den drei genannten Verfahren höchste Priorität genießen muss, weil die verarbeiteten Daten der ärztlichen Schweigepflicht unterliegen und darüber hinaus von besonderer Sensitivität sind. Daten über psychische Erkrankungen, Suchterkrankungen oder über z.B. AIDS-Kranke sind Daten mit sehr hohem Schutzbedarf im Sinne der BSI-Grundschutzkataloge, da ihre missbräuchliche Verwendung die gesellschaftliche und wirtschaftliche Stellung der Betroffenen in nicht reparabler Weise beeinträchtigen würde. Ihr Schutzbedarf ist daher wesentlich höher als die üblicherweise in den Netzen der Bezirksämter verarbeiteten Daten, und es sind spezielle Schutzmaßnahmen notwendig.

So ist z.B. durch geeignete Verschlüsselungsverfahren sicherzustellen, dass Dritten – und dazu gehören im Geltungsbereich der ärztlichen Schweigepflicht auch Systemverwalter und -betreuer außerhalb der Gesundheitsämter – die

Kenntnisnahme der Dateninhalte verwehrt wird. Diese Anforderungen, die schon in den alten Anwendungen für die bezirkliche Infrastruktur galten, sind natürlich auch im ITDZ zu erfüllen, wenn die Verarbeitung dorthin verlagert wird.

Grundsätzlich begrüßen wir es, wenn sensitive IT-Verfahren im Terminal-Server-Betrieb durchgeführt werden, da damit viele Risiken vermieden werden können, die durch missbräuchliches (oder fahrlässiges) Handeln an den Clients entstehen. Insofern würden wir den Terminal-Server-Betrieb im ITDZ befürworten, sofern dabei die beschriebenen Vertraulichkeitsanforderungen erfüllt werden.

Für eine fundierte datenschutzrechtliche Bewertung ist die Einschätzung der Risiken der Vertraulichkeit und Integrität der Daten bei den drei genannten Migrationsvarianten und der dagegen verfügbaren Sicherheitsmaßnahmen von elementarer Bedeutung. Diese Risikoanalysen für den Vergleich der drei Verfahren wurden bisher nicht vorgelegt, sodass eine Konkretisierung unserer Empfehlung nicht möglich ist.

8.3 Personaldaten

8.3.1 Whistleblower-Plattformen – Keine „Compliance“ um jeden Preis

Mehrfach waren wir mit Plänen konfrontiert, welche die Einrichtung sog. Whistleblower-Plattformen betrafen. Als Whistleblower (engl. Pfeifenbläser) bezeichnet man einen internen Informanten, der Missstände, illegales Handeln (wie Korruption, Insiderhandel) oder allgemeine Gefahren, von denen er an seinem Arbeitsplatz erfährt, an seine Vorgesetzte weiterleitet oder an die Öffentlichkeit bringt.

Häufig handeln Whistleblower verantwortungsvoll und auch loyal, weil sie mit der Meldung ihre Unternehmen bzw. ihre Dienstherren vor negativen Entwicklungen schützen wollen. Nicht immer wird dieses Verhalten von ihren unmittelbaren Vorgesetzten für gut befunden, sei es, dass diese selbst eines Fehl-

verhaltens beschuldigt werden, sei es, dass sie das „Verpfeifen“ von Fehlentwicklungen aus ihrem Verantwortungsbereich zu vermeiden suchen.

Deshalb wird auch in Deutschland zu Recht diskutiert, ob zur Eindämmung von Korruption und zur Sicherung des sozialen Friedens Regelungen geschaffen werden sollen, die einen effektiven Schutz von Whistleblowern vor Maßregelung sicherstellen.[67] Dies dient in bestimmtem Umfang auch dem Schutz öffentlicher Interessen wie der Informationsfreiheit.

Datenschutzrechtlich problematisch sind jedoch stets Internet-Plattformen, die Whistleblowern und externen Hinweisgebern technisch eine absolute Anonymität ihrer Meldung gewährleisten sollen. Sie sind u.a. deshalb riskant, weil sie die Gefahr einer hemmungslosen Denunziation begründen können. Wir möchten nicht ausschließen, dass eine anonyme Meldeplattform datenschutzkonform ausgestaltet werden kann. Zu einer sachgerechten Begrenzung des genannten Risikos sind allerdings anspruchsvolle Anforderungen zu erfüllen. Die Artikel 29-Datenschutzgruppe hat hierzu wertvolle Hinweise gegeben.[68]

Eine unabdingbare Voraussetzung ist die Begrenzung des Personenkreises, der zur Meldung von angeblichen oder tatsächlichen Missständen befähigt wird. Eine **jedermann** zugängliche Internetplattform, die in erster Linie zu einer anonymen Meldung auffordert, ist damit unzulässig. Denn hierbei kann fast nie sichergestellt werden, dass die schutzwürdigen Belange der betroffenen Personen gewahrt bleiben. Befürworter solcher Plattformen versichern zwar immer wieder, man könne mit einer sorgfältigen Plausibilitätskontrolle und mit (technisch möglichen!) Nachfragen beim Whistleblower zuverlässig herausfinden, ob eine Meldung lediglich der Anschwärzung einer Person diene oder tatsächlich „werthaltig“ sei. Konkrete und nachvollziehbare Kriterien für eine solche Abgrenzung kennen wir bislang nicht. Vor allem sollte den Hinweisgebern nahegelegt werden, ihre Identität offenzulegen, deren vertrauliche Behandlung zugesichert werden sollte. Das kann glaubwürdig in der Weise

67 Derzeit wird auf Bundesebene die Einführung eines § 612 a BGB geprüft, der diesen Schutz sicherstellen soll.

68 Stellungnahme 1/2006 vom 1. Februar 2006 über die Anwendung von EU-Datenschutzvorschriften auf innerbetriebliche Maßnahmen zur Unterstützung von Hinweisgebern (whistleblowing) in den Bereichen Buchhaltung, Rechnungsprüfung, Buchprüfung und Kampf gegen Bestechung sowie Bank- und Finanzkriminalität, WP 117

geschehen, dass ein externer Ombudsmann die Hinweise entgegennimmt. Der Vorrang der Vertraulichkeit vor der Anonymität entspricht dem gesetzlichen Schutz von Whistleblowern in Großbritannien[69]. Anonyme Hinweise bleiben daneben ausnahmsweise möglich und werden auch aufgegriffen, wenn sie stichhaltig erscheinen.

Auch konkrete Verfahrensregeln zum Schutz der betroffenen Personen sind in Deutschland häufig Mangelware. Um es pointiert auszudrücken: Stets fordern zwar die Compliance-Abteilungen von der Belegschaft die Einhaltung von gesetzlichen und unternehmensinternen Regeln ein. Bereits die Datenschutzskandale des vergangenen Jahres verdeutlichen, dass zahlreiche Unternehmen für die Ermittlungen ihrer Compliance-Abteilungen keine festen Regeln vorgeben. Das wirkt sich massiv zulasten der betroffenen Beschäftigten aus, wie wir nicht nur anlässlich der Überprüfung eines großen Wirtschaftsunternehmens feststellen mussten. Diese Feststellung galt auch bei der Einführung der dortigen Whistleblower-Plattform: Es wurden keine konkreten Kriterien zur Beurteilung der anonymen Meldungen genannt, eine Benachrichtigung der Betroffenen war auch dann nicht vorgesehen, wenn sich eine Meldung als haltlos erwies. In Verdachtsfällen wurde einfach „drauflos ermittelt", ohne dass dies erkennbar von Regeln geleitet oder gar vom Betriebsrat kontrolliert gewesen wäre. Das Verfahren gegen dieses Unternehmen ist noch nicht abgeschlossen.

Im Bereich der öffentlichen Verwaltung ist bei der Einrichtung von Whistleblower-Plattformen zudem der Gesetzesvorbehalt zu beachten. Für eine verwaltungsübergreifende Whistleblower-Plattform gibt es im Berliner Recht keine gesetzliche Grundlage: Das Disziplinargesetz verlangt für Datenerhebungen tatsächliche Anhaltspunkte für ein Fehlverhalten. Das wird bei den Whistleblower-Plattformen gerade nicht zur Voraussetzung von Meldungen gemacht. Das Berliner Recht gestattet zwar die gesetzlich vorgesehene Verarbeitung von personenbezogenen Daten zur Aufgabenerfüllung. Dabei gilt die Wahrnehmung der „internen Revision" nicht als zweckändernde Datenverarbeitung. Die Zweckbindungsregel erlaubt allerdings keine Verwendung zur verwaltungsübergreifenden Revision. Allein deshalb waren Pläne datenschutzrechtlich bedenklich, bei der Senatsverwaltung für Stadtentwicklung eine verwaltungsübergreifende Whistleblower-Plattform anzusiedeln. Erfreulicherweise

69 Public Interest Disclosure Act

hat sich die Senatsverwaltung unseren Bedenken angeschlossen und die Einführung einer solchen Plattform zurückgestellt. Das Bezirksamt Spandau hat seit längerem einen Ombudsmann mit der Entgegennahme von Hinweisen beauftragt, ein System, das wir ebenfalls unterstützen.

Die Erfahrungen mit Whistleblower-Plattformen werfen die Frage nach der datenschutzrechtlichen Kontrolle von Compliance- und Revisionsabteilungen auf. Wir werden dieser Frage weiter nachgehen. Auch wenn sie zweifelsohne ein wichtiges Anliegen verfolgen, ist es keineswegs akzeptabel, wenn Compliance und Revision gleichsam in einem „rechtsfreien Raum" agieren.

Bei der Einrichtung von technischen Whistleblower-Plattformen muss darauf geachtet werden, dass nicht nur die meldende, sondern auch die gemeldete Person schutzwürdig ist. Zur Wahrung dieser schutzwürdigen Belange beider Personengruppen sind konkrete Verfahrensregeln geboten. Auch die Compliance bzw. Revision hat datenschutzrechtliche Mindestanforderungen zum Schutz betroffener Personen zu beachten.

8.3.2 Umgang mit Personaldaten von Gewerkschaftsmitgliedern

Eine Beschäftigte in einem bundesweit tätigen Unternehmen hatte sich in einer E-Mail an ihren Betreuer einer großen Gewerkschaft über das Verhalten ihres Arbeitgebers und über die Arbeit des dortigen Betriebsrats beschwert. Kurze Zeit später erhielt die Beschäftigte eine Abmahnung von ihrem Arbeitgeber. Darin wurde ausdrücklich auf die an die Gewerkschaft gerichtete E-Mail der Beschäftigten Bezug genommen, die dem Arbeitgeber angeblich von der besagten Gewerkschaft zugeleitet worden war. Daraufhin informierte die Beschäftigte den betreffenden Gewerkschaftsbetreuer und Empfänger der E-Mail und bat um Nennung aller Namen derjenigen Personen, an die er die E-Mail weitergeleitet hatte. Eine Antwort der Gewerkschaft blieb aus.

Der von uns um Stellungnahme gebetene betriebliche Datenschutzbeauftragte der Gewerkschaft konnte den Sachverhalt ebenso wenig aufklären wie die dortige Rechtsabteilung, die verlauten ließ, es gebe keine Indizien für eine

unerlaubte Weiterleitung der E-Mail an den Arbeitgeber. Nach entsprechender Bitte übersandte der Arbeitgeber uns die fragliche E-Mail und teilte mit, er habe die Mail in Papierform einen Monat nach Absendung an die Gewerkschaft in seinem Postfach vorgefunden. Er wisse jedoch nicht, welche Person ihm diesen Auszug überlassen habe. Die E-Mail wies als Absender eine Beschäftigte der Gewerkschaft aus.

Erst daraufhin teilte uns die Gewerkschaft auf entsprechenden Vorhalt mit, eine dort Beschäftigte habe die Mail der in dem Unternehmen tätigen Gewerkschaftsfunktionärin zur Klärung der betrieblichen und betriebsrätlichen Aspekte im Interesse der Geschädigten übergeben. Sie habe jedoch nicht gewusst, dass diese Funktionärin gleichzeitig Betriebsratsvorsitzende des Unternehmens sei, in dem die Petentin beschäftigt war.

Indem die Mitarbeiterin der Gewerkschaft die E-Mail an die Betriebsratsvorsitzende weiterleitete, verstieß sie gegen § 28 Abs. 1 Satz 1 Nr. 1 und 2 Bundesdatenschutzgesetz (BDSG). Schreiben oder E-Mails mit vertraulichem Inhalt an Gewerkschaftsbetreuer dürfen keinesfalls ohne Einverständnis der Betroffenen an Dritte weitergegeben bzw. weitergeleitet werden. Dies trifft auch auf Funktionäre der Gewerkschaft zu, erst recht wenn sie wie hier gleichzeitig Mitglied des Betriebsrats eines Arbeitgebers sind, gegen den sich die Beschwerde richtet.

Da jedoch die betreffende Gewerkschaftsmitarbeiterin in dem guten Glauben handelte, zur Lösung eines Problems zwischen der Beschäftigten und dem Arbeitgeber und dessen Betriebsrat beitragen zu können, haben wir von der Einleitung eines Ordnungswidrigkeitenverfahrens abgesehen. Wir haben die Gewerkschaft jedoch aufgefordert, alle Mitarbeitenden in einem Informationsschreiben auf die Pflicht zu einem vertraulichen Umgang mit zugeleiteten Schreiben hinzuweisen. Im Übrigen haben wir bemängelt, dass der Betroffenen nicht unverzüglich und vollständig Auskunft über die weiteren Empfängerinnen und Empfänger der E-Mail bei der Gewerkschaft erteilt wurde. Trotz des massiven Vorwurfs des Arbeitgebers, er habe die E-Mail von der Gewerkschaft erhalten, hielt diese es nicht für nötig, sofort umfangreiche und intensive Ermittlungen zur Aufklärung des Sachverhalts zu stellen oder selbst die Aufsichtsbehörde einzuschalten.

Das Ergebnis unserer Überprüfung konnte die Betroffene als Grundlage verwenden, Schadensersatzansprüche gegen die Gewerkschaft geltend zu machen. Zugleich haben wir der Gewerkschaft verdeutlicht, dass sie bei vergleichbaren Missständen künftig mit einer härteren aufsichtsbehördlichen Vorgehensweise rechnen muss.

Gewerkschaften sind verpflichtet, mit ihren Mitgliedsdaten besonders vertraulich umzugehen. Hierzu gehört insbesondere, dass personenbezogene Daten nicht ohne Einverständnis der Betroffenen an Dritte weitergegeben werden.

8.3.3 Datenerhebung bei Nebentätigkeiten

Ein Beschäftigter der Humboldt-Universität beschwerte sich darüber, dass die Personalabteilung offenkundig Auskünfte bei einem Unternehmen eingeholt habe, bei dem der Petent eine Nebentätigkeit verrichtete. Dabei seien Personaldaten des Petenten ohne seine Einwilligung an den Geschäftsführer des Unternehmens übermittelt worden, insbesondere die Information, die Nebentätigkeit sei nicht genehmigt.

Diese Vorgehensweise verstieß gegen das Gebot der Direkterhebung nach § 4 Abs. 2 BDSG. Danach sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Von diesem Grundsatz darf nur in engen Grenzen abgewichen werden. Voraussetzung ist, dass eine Aufgabe ohne die Kenntnis der Betroffenendaten nicht ordnungsgemäß erfüllt werden kann. Diese Ausnahme vom Grundsatz der Direkterhebung setzt allerdings voraus, dass es sich um eine spezifische Verwaltungsaufgabe handelt, die ihrer Art nach eine Erhebung ohne Mitwirkung erforderlich macht.

Im vorliegenden Fall hatte die Mitarbeiterin der Universität wiederholt bei dem Unternehmen telefonisch nachgefragt, ob und wann der Petent als Dozent im Rahmen einer Nebenbeschäftigung, die nach dem geltenden Tarifvertrag einer Genehmigung bedurfte, bei Veranstaltungen des Unternehmens tätig wurde.

Dass es sich hierbei um eine Verwaltungsaufgabe handelte, die nicht allein durch die Mitwirkung des Betroffenen erfüllbar ist, war nicht ersichtlich. Vielmehr

war hier der Grundsatz der Direkterhebung anzuwenden, der auch keinen unverhältnismäßigen Aufwand im Sinne des § 4 Abs. 2 Satz 2 Nr. 2 b) BDSG erfordert hätte. Gründe, die dafür sprechen, den Betroffenen von der Mitwirkung der Erhebung auszuschließen, waren nicht erkennbar.

Soweit die Personalabteilung der Universität anführte, es müsse dem Arbeitgeber möglich sein, bei vermuteten Vertragsverstößen seines Mitarbeiters eigene Nachforschungen anzustellen, war dem entgegenzuhalten, dass jedenfalls zuvor eine unmittelbare Klärung mit dem Betroffenen anzustreben ist. An einem solchen direkten Aufklärungsversuch fehlte es hier jedoch. Vielmehr hatte sich die Personalabteilung aufgrund eines nicht erhärteten Verdachts sofort an das Unternehmen gewandt, um eigene Ermittlungen durchzuführen.

Darüber hinaus verstieß die Vorgehensweise der Personalstelle gegen das Prinzip der Verhältnismäßigkeit (§ 4 Abs. 2 BDSG). Durch ihre Anfrage erfuhr das Unternehmen nämlich, dass der Petent offensichtlich in arbeitsrechtliche Streitigkeiten mit seinem Arbeitgeber verwickelt war.

Personalabteilungen dürfen bei vermuteten Vertragsverstößen von Beschäftigten eigene Nachforschungen bei Dritten erst dann anstellen, wenn der Aufklärungsversuch beim betroffenen Personal gescheitert ist.

8.3.4 Feedbackkarten für Trainer im Fitnessstudio

Aus der Praxis

Die Geschäftsleitung eines Sportstudios plante, dass jede Trainerin und jeder Trainer nach einer Trainingsbegleitung den Kundinnen und Kunden eine Feedbackkarte aushändigt. Die Feedbackkarten sollten mit der Personalnummer der jeweiligen Trainerin oder des Trainers versehen werden sowie eine Bewertung bezüglich der Qualität von Trainingsbegleitung und Betreuung enthalten. Die Einstufung sollte über die Wertungspunkte von „gut“ bis „schlecht“ und bezüglich der Häufigkeit dieser Einschätzung von „einmalig“ und „wiederholt“ aufgeteilt werden. Ferner sollte die positive wie auch die negative Wertung der Kundin oder des Kunden für einzelne Beschäftigte aufgeschlüsselt werden und als Grundlage für spätere Mitarbeitergespräche dienen.

Das geplante Verfahren war unzulässig. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG darf der Arbeitgeber Daten über seine Beschäftigten erheben, speichern, verarbeiten und nutzen, soweit es dem Zweck des Arbeitsvertrages dient. Der Arbeitgeber darf eine sachliche und objektive Beurteilung der fachlichen Leistung und Befähigung in der Personalakte festhalten. Andere Angaben dürfen nicht in die Beurteilung mit einfließen. Insbesondere dürfen Angaben von Dritten grundsätzlich nicht erhoben werden. Die Verwendung von Werturteilen setzt ein erhöhtes Interesse der verantwortlichen Stelle voraus, weil die bewerteten Personen durch Missdeutungen besonders gefährdet sind.

Demgegenüber haben Beschäftigte ein Recht auf die Erhebung korrekter Personaldaten. Der Arbeitgeber muss die Beurteilung in einem ordnungsgemäßen Verfahren erstellen. Im vorliegenden Fall sollten die Feedbackkarten grundsätzlich nur die Kundenbeurteilung festhalten. Durch die Zuordnung zu den Beschäftigten per Personalnummer sollte zugleich ihre Beurteilung ermöglicht werden. Die Kundenbefragung zur Zufriedenheit war dafür aus mindestens drei Gründen ungeeignet:

1. Kundinnen und Kunden sind nicht verpflichtet, eine objektive Beurteilung abzugeben.
2. Es besteht die Möglichkeit, dass die Kundin oder der Kunde sachfremde Erwägungen in die Beurteilung einfließen lässt, z.B. bei Verärgerung über hohe Preise. Insofern ist die Feedbackkarte eine wenig geeignete Beurteilungsgrundlage.
3. Der Arbeitgeber hat die Bewertung nicht selbst abgegeben. Wenn er sie in ein Arbeitszeugnis übernimmt, verletzt er das Gebot zur erhöhten Vorsicht bei Werturteilen von Dritten.

Die Feedbackkarte mit Personalnummer diente daher nicht dem Zweck des Arbeitsvertrages.

Zwar hat der Arbeitgeber außerdem ein Recht zur Datenerhebung und -verarbeitung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, soweit er eigene berechtigte Interessen verfolgt und die Interessen der Betroffenen nicht überwiegen. Das Interesse des Arbeitgebers an Feedbackkarten liegt in der Erfassung der Kundenzufriedenheit. Die genaue Zuordnung durch Angabe der Personalnummer

könnte auch die Organisation des Geschäftsbetriebes unterstützen, um das bestmögliche Trainer-Kunden-Verhältnis herzustellen. Jedoch haben die Beschäftigten ein schutzwürdiges Interesse an einer möglichst objektiven Beurteilung ihrer persönlichen Leistung und Eignung.

Das Interesse des Arbeitgebers an der Verbindung der Feedbackkarte mit der beabsichtigten Beurteilung seiner Beschäftigten tritt insoweit hinter deren Interesse an einer objektiven Beurteilung zurück. Deshalb war die Verbindung der Feedbackkarte mit der Personalnummer auch nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG unzulässig.

Feedbackkarten ohne Personalnummer dienen dem Interesse des Fitnessstudiobetreibers, ohne jedoch das Interesse der Beschäftigten erheblich zu beeinträchtigen. Die Verwendung ist ebenso zielführend und darüber hinaus angemessen.

8.4 Wohnen und Umwelt

8.4.1 Google Street View

Seit Mai 2007 ist die Funktion Google Street View der Internet-Suchmaschine Google verfügbar, die für viele amerikanische Städte und Nationalparks als Navigationshilfe genutzt werden kann. Diese Funktion erlaubt es den Nutzenden, bei einem virtuellen Spaziergang einen Straßenzug aus der Perspektive eines Fußgängers zu betrachten. Da etwa alle zehn Meter ein Foto gemacht wird, kann man eine gewünschte Strecke (fast) lückenlos in Etappen virtuell zurücklegen und sie auch in einer 360°-Panoramaansicht „durchfliegen". Die Panoramabilder werden von einem mit einer speziellen Kamera ausgestatteten PKW aufgenommen, der durch die Straßen fährt. Entsprechende Aufnahmen sind auch in Berlin und anderen deutschen Großstädten gemacht worden, die nach Angaben von Google im Frühjahr 2009 abrufbar sein sollen.

Google Street View erlaubt eine Vielzahl praktischer Anwendungen. So kann man einen Restaurantbesuch mit Freunden planen, den besten Zuschauerplatz bei einem Marathon oder einer Parade finden und sich vor einer Reisebuchung ein ausgewähltes Hotel und dessen Nachbarschaft ansehen.

Allerdings birgt Google Street View auch datenschutzrechtliche Risiken: Da auf den ersten im Internet veröffentlichten Bildern sowohl Gesichter von Passantinnen und Passanten als auch Nummernschilder klar zu erkennen waren, gibt es Proteste von betroffenen Bürgerinnen und Bürgern und kritische Stimmen nationaler und internationaler Aufsichtsbehörden. Seit Mai 2008 durchsucht Google daher das neu aufgenommene und bereits veröffentlichte Bildmaterial mit einer speziellen Software nach Gesichtern von Passantinnen und Passanten und Autonummernschildern, um sie dann durch Weichzeichnung unkenntlich zu machen. Google will langfristig alle Bilder dieser Prozedur unterziehen. Da es sich jedoch um einen automatisierten Vorgang handelt, kann es vorkommen, dass Gesichter oder Nummernschilder nicht vollständig unkenntlich gemacht werden. Zur Behebung dieser Problematik bietet Google folgende Lösungsmöglichkeit an:

Sofern im Einzelfall trotz Einsatzes dieser Technologie ein Gesicht oder ein Nummernschild erkennbar sein sollte, können alle Nutzenden ein solches Bild melden. Google sichert zu, das Bild entsprechend zu bearbeiten. Dafür muss auf der Internetseite von Google Maps unten links im Street View Fenster der Link **„Bedenken melden“** angeklickt und als Kategorie entweder **„Bedenken in Bezug auf Privatsphäre“**, **„Anstößige Inhalte“**, **„Sonstiges“** oder **„Allgemeines Feedback zu Google Street View“** gewählt werden. Trotz dieser Möglichkeit, die Privatsphäre zu schützen, wächst in Deutschland der Widerstand gegen die Veröffentlichung von Bildern bundesdeutscher Städte.

Da das für Street View verantwortliche Unternehmen Google seine deutsche Niederlassung in Hamburg hat, ist der Hamburgische Datenschutzbeauftragte die dafür zuständige Aufsichtsbehörde. Problematisch ist, dass sich die Zentrale von Google in den USA befindet und die gemachten Aufnahmen auf amerikanischen Servern liegen. Google hat bisher nicht die Frage beantwortet, ob und wie lange die Rohdaten solcher personenbezogenen Bilder gespeichert bleiben, deren Veröffentlichung unterbunden wird.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) haben in einem Beschluss die Veröffentlichung von digitalen Straßenansichten im Internet bewertet. [70] Darin wird betont, dass

70 Vgl. Dokumentenband 2008, S. 37

die betroffenen Personen (Passantinnen und Passanten, Anwohnerinnen und Anwohner) das Recht haben, zumindest der Veröffentlichung von Bildern zu widersprechen, auf denen sie erkennbar sind. Auch Gebäude und Grundstücke müssen soweit verschleiert werden, dass keine individuellen Eigenschaften von Bewohnerinnen und Bewohnern mehr erkennbar sind. Dieser Beschluss bezieht sich nicht nur auf Google Street View, sondern gilt für alle Anbieter in Deutschland, die digitale Bilder oder Panoramabilder von öffentlich zugänglichen Räumen im Internet zur Verfügung stellen. Für den Fall, dass ein Berliner Unternehmen eine ähnliche Dienstleistung wie Google Street View anbietet, muss es zumindest die von den Aufsichtsbehörden genannten Vorgaben umsetzen.

Wer virtuelle Straßenansichten im Internet anbietet, muss schon bei der Datenerhebung die Rechte von Personen berücksichtigen, die dabei abgebildet werden. Verkehrsteilnehmende und Anwohnende haben jedenfalls das Recht, einer Speicherung und Veröffentlichung von Bildern, auf denen sie erkennbar sind, zu widersprechen.

8.4.2 Videoeinsatz bei der Evaluierung der Umweltzone

Aus der Praxis

Um die Wirkungen der Einrichtung der Umweltzone auf das Verkehrsgeschehen, die Fahrzeugflotte und Luftschadstoffbelastungen darstellen zu können, hat die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz im September eine Untersuchung durchgeführt, wie sich der Fahrzeugbestand, der sich innerhalb der Umweltzone befindet, von dem außerhalb der Zone unterscheidet. Dazu wurden an sieben Standorten, davon drei in der Umweltzone und vier außerhalb, spezielle Videokameras aufgestellt, die so eingestellt werden konnten, dass mit Ausnahme des Kennzeichens alles andere bei der Erfassung ausgeblendet wurde.

Wir haben uns davon überzeugt, dass das Verfahren datenschutzkonform betrieben wird.

Die bei der Kennzeichenerfassung erhobenen Daten beschränkten sich auf das Kennzeichen, den Erhebungstag und den Erhebungsort. Auf weitere Daten wie Fahrzeugfoto und genauere Zeitangaben, die durch das eingesetzte Video-

verfahren erhoben werden könnten, ist verzichtet worden, weil sie zur Verfolgung des Projektziels nicht erforderlich waren.

Die Auswertung erfolgte für Berliner Fahrzeuge durch die Kfz-Zulassungsstelle des Landesamtes für Bürger- und Ordnungsangelegenheiten, die Auswertung für andere in Deutschland zugelassene Fahrzeuge erfolgte durch das Kraftfahrtbundesamt. Ausländische Fahrzeuge wurden nicht in die Auswertung einbezogen.

Für die Auswertung genügt die Bereitstellung der Kennzeichen und ein den auswertenden Behörden nicht bekannter Code (pseudonyme Kennzeichnung der sieben Messstellen) für den Erhebungsort. Zeitangaben sind dabei nicht erforderlich. Die auswertenden Behörden stellen aggregierte Listen her, die für jeden Straßenquerschnitt die Anteile der Abgasstandards je Fahrzeugkategorie enthalten und an die Senatsverwaltung zurückgeliefert werden. Ein Kennzeichenbezug wird nicht hergestellt, und sonstige auf die Halterin oder den Halter bezogene Angaben werden nicht zurückgemeldet.

Da die Datenerhebung und -auswertung nach dem Bundesimmissionsschutzgesetz erforderlich war und die Art der Durchführung datenschutzfreundlich und datensparsam erfolgte, bestanden keine datenschutzrechtlichen Bedenken gegen das Projekt.

Wir hatten empfohlen, das Projekt mit einer sorgfältigen Aufklärung der Öffentlichkeit zu verbinden, um Beunruhigungen durch den Einsatz von Videotechnik auf den Straßen zu vermeiden. Die Erhebungen sollten offen erfolgen und nicht den Eindruck heimlicher Ausforschung erwecken. Dieser Empfehlung ist die Senatsverwaltung allerdings nicht gefolgt, sodass pünktlich zum ersten Auftreten von Videokameras im Straßenraum in der Presse und in der Politik Mutmaßungen über eine Videoüberwachung zur Entdeckung von Fahrzeugen ohne Plakette angestellt wurden.

Das Projekt erhob die personenbezogenen Daten der Fahrzeughalterinnen und -halter nicht und war daher in vorbildlicher Weise datenschutzfreundlich gestaltet. Leider hat sich die Senatsverwaltung zu spät um das Vertrauen der Öffentlichkeit bemüht, die erfahrungsgemäß in Berlin überdurchschnittlich kritisch ist.

8.4.3 Intelligente Stromzähler

Mit dem „Gesetz zur Öffnung des Messwesens bei Strom und Gas für Wettbewerb“[71] wurde das Energiewirtschaftsgesetz (EnWG) geändert. Dabei geht es um die europaweite Liberalisierung des sog. Messmarktes. Danach können unterschiedliche Unternehmen mit der Energielieferung, dem Betrieb des Verteilnetzes und dem Betrieb der Messstellen beauftragt werden - Leistungen, die heute noch meist in einer Hand liegen. Bedeutsamer sind die Anforderungen an das Zählerwesen in dieser Gesetzesänderung:

- Danach sind ab 2010 – sofern technisch machbar und wirtschaftlich zumutbar – bei Neubauten und bei größeren Renovierungen Messeinrichtungen einzubauen, die den jeweiligen Anschlussnutzenden den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln (§ 21 b Abs. 3 a EnWG).
- Ebenfalls ab 2010 ist der Bestandskundschaft anzubieten, dass solche Messeinrichtungen eingebaut werden, die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln. Bestandskundinnen und -kunden können das Angebot ablehnen (§ 21 b Abs. 3 b EnWG).
- Ab sofort sind die Energielieferanten verpflichtet, der Kundschaft die monatliche Rechnungsstellung anzubieten (§ 40 Abs. 2 EnWG).
- Ferner haben Energieversorgungsunternehmen – sofern technisch machbar und wirtschaftlich zumutbar – bis Ende 2010 für Letztverbraucher von Elektrizität einen Tarif anzubieten, der einen Anreiz zu Energieeinsparung oder Steuerung des Energieverbrauchs setzt. Solche Tarife sind insbesondere lastvariable oder tageszeitabhängige Tarife (§ 40 Abs. 3 EnWG).

Das Automatic Meter Management ermöglicht die monatliche Turnusablesung, die stichtagsbezogene Ablesung, die Ablesung für Vertragswechsel und Schlussabrechnung, die Null-Verbrauchskontrolle und die Leeranlagenüberwachung, die Fernschaltung und -steuerung, z.B. von Heizungen, die variable Gestaltung von Tarifzeitmodellen usw.

71 BGBl. I 2008, S. 1790

Der sog. Profizähler, der von Vattenfall erprobt werden soll, misst in kurzen Abständen den Energieverbrauch und sendet die Angaben verschlüsselt über die Stromleitung[72] zu einem dezentralen Konzentrator in der nächstgelegenen Netzstation. Von dort werden die Daten verschlüsselt über Funktechnik und Internet zu einem zentralen Server geleitet, dort aufbereitet (z.B. grafische Darstellung) und den Kundinnen und Kunden im Internet zur Verfügung gestellt. Sie können damit ihre Verbrauchswerte permanent im Auge behalten, um gezielter Energie einzusparen. Vattenfall selbst benötigt nur jene Daten, die für die Abrechnungszwecke erforderlich sind.

Bei den bis Ende 2010 anzubietenden Tarifen, die einen Anreiz zur Steuerung des Energieverbrauchs geben, soll jederzeit der aktuelle berlinweite Strombedarf im Verhältnis zur Stromerzeugung gemessen werden. Bei der Stromerzeugung spielen insbesondere die wetterbedingt schwankenden Stromeinspeisungen durch Windkraftwerke und Solaranlagen eine Rolle. Der Strom soll umso billiger sein, je geringer der Gesamtverbrauch und je höher die Gesamtstromerzeugung ist, und teurer, wenn es umgekehrt ist. Diese Werte stehen nur dem Stromerzeuger bzw. -lieferanten zur Verfügung. Es muss aber aktuell den abnehmenden Haushalten bekannt gemacht werden, ob gerade ein teurer oder ein preisgünstiger Tarif besteht.

Vattenfall stellte uns das Erprobungskonzept vor und bat um eine datenschutzrechtliche Abstimmung, weil das Unternehmen mit unserer positiven Bewertung um Akzeptanz werben wollte. Zunächst erprobte Vattenfall die Profizähler mit 85 sog. Treppenhauszählern, mit denen keine personenbezogenen Verbrauchsdaten erhoben werden können, sowie mit weiteren 115 Kundinnen und Kunden, die freiwillig unter festgelegten Bedingungen und nach eingehender Information an dem Test teilnehmen wollten. Dagegen bestehen keine Einwände.

Geplant ist außerdem ein gemeinsames Projekt von Vattenfall und GASAG mit dem Berliner Beamten-Wohnungs-Verein mit 500 Gas- und 500 Stromzählern sowie als „Leuchtturmprojekt“ ab Mitte 2009 der Einbau von 12.000 Profizählern in Neubauten im Märkischen Viertel. Dabei gilt eine mehrstufige Verfahrensweise:

72 sog. Power Line Communication (PLC)

- Der Einbau der Zähler basiert auf der unternehmerischen Entscheidung, ältere Zähler durch neue Technik zu ersetzen. Die Kundinnen und Kunden werden darüber informiert, dass zu festgelegten Zeiten (einmal im Jahr) eine Fernablesung erfolgt, über die abgerechnet wird. Sie haben die Möglichkeit zur Kontrolle der Ablesung, da sie die Ablesetermine genau kennen. Es wird garantiert, dass weitere Ablesungen nicht erfolgen, abgesehen von nötigen Zwischenablesungen bei Mieterwechseln. Unter diesen Umständen kann § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Rechtsgrundlage herangezogen werden.
- Wer die monatliche, die taggenaue Ablesung oder gar die durch viertelstündliche Ablesung entstehenden Lastprofile (Tagesverbrauchskurve) für die Verfolgung des Verbrauchs wünscht, muss nach § 4 a BDSG schriftlich einwilligen. Die für die wirksame Einwilligung erforderlichen Informationen sind einer Informationsschrift zu entnehmen.
- Sofern die Kundinnen und Kunden die Energieverbrauchsdaten für wissenschaftliche Zwecke (Test der neuen Zähler, Generierung neuer Tarife nach § 40 Energiewirtschaftsgesetz) pseudonymisiert zur Verfügung stellen wollen, müssen sie dafür ebenfalls eine schriftliche Einwilligung nach § 4 a BDSG geben. Die Pseudonymisierung erfolgt vor weiterer Nutzung und Übermittlung beim Messstellenbetreiber mit einem sicheren Verschlüsselungsverfahren. Nach ihrer Verwendung werden die Daten gelöscht.
- Sofern sie später allerdings auch ihre sog. Lastgänge (monatliche Verbrauchskurve) mit dem Ziel der Steuerung des Stromverbrauchs nach dem günstigsten Tarif im Internet verfolgen wollen, soll dies ohne Pseudonymisierung erfolgen. Dafür ist dann eine weitere schriftliche Einwilligung nach § 4 a BDSG erforderlich.

Die Einwilligungen können von der Kundin oder dem Kunden jederzeit widerrufen werden. Sofern für eine der Stufen 2 – 4 keine Einwilligung gegeben wird, wird die Kundin oder der Kunde weiter unter den Bedingungen der Stufe 1 oder unter den Bedingungen der Stufe, zu der er noch eingewilligt hat, beliefert.

Unter diesen Bedingungen, die den Datenschutz sicherstellen können, haben wir es Vattenfall gestattet, öffentlich auf unsere positive Bewertung hinzuweisen.

9. Kultur

9.1 Nutzung von Patientendaten im Landesarchiv Berlin

Der Krankenhauskonzern Vivantes übergab dem Landesarchiv Berlin etwa 90.000 Patientenakten aus den Jahren 1880 bis 1960. Dazu zählten auch „Euthanasie-Akten" der früheren Karl-Bonhoeffer-Nervenklinik aus der Zeit des Nationalsozialismus. Das Landesarchiv Berlin informierte die Öffentlichkeit in einer Pressekonferenz von der Übergabe und legte dabei die psychiatrische Krankengeschichte des 1991 verstorbenen Schauspielers Klaus Kinski aus. Daraufhin erschienen Berichte in der Tagespresse, die Erkenntnisse aus der Krankengeschichte von Kinski zitierten und Abbildungen aus dem Akteninhalt zeigten. Die Aktenauszüge hatten das persönliche Umfeld Kinskis, seine psychische Erkrankung, deren Behandlung und Verlauf zum Gegenstand. Wenig später wurde diese Publikation des Inhalts der Patientenakte in der Tagespresse kritisch in Zweifel gezogen. Die Witwe des Schauspielers kündigte rechtliche Schritte gegen die Öffnung der Patientenakte an.

Wir haben von der Übergabe der Patientenakten an das Landesarchiv und von der Auslegung der Krankengeschichte Kinskis aus der Presse erfahren und daraufhin das Landesarchiv gebeten, die Akte Kinski zunächst wieder unter Verschluss zu nehmen, bis wir deren Offenlegung datenschutzrechtlich bewerten konnten. Dem hat das Landesarchiv entsprochen.

Unsere Bewertung führte zu einem Ergebnis, das wir in einer gemeinsamen Presseerklärung mit dem Landesarchiv Berlin bekannt gegeben haben, um angesichts der öffentlichen Erörterung die rechtlichen Beurteilungsgrundlagen einvernehmlich zu beschreiben: Das Patientengeheimnis unterliegt nach der ständigen Rechtsprechung der obersten Gerichte einem besonderen Schutz. Zwar enthält auch das Berliner Archivgesetz Regeln zum Schutz von Patientendaten. Sie standen hier aber einer Offenlegung der Krankengeschichte des Schauspielers nicht entgegen. Zum einen handelt es sich bei Klaus Kinski unzweifelhaft um eine Person der Zeitgeschichte. Zum anderen war in seinem Fall die – in Berlin besonders kurze – Schutzfrist von zehn Jahren nach seinem

Tod abgelaufen. Diese Regelung geht auf die Rechtsprechung des Bundesverfassungsgerichts zurück, nach der die Schutzwirkung des Grundrechts auf informationelle Selbstbestimmung bei Verstorbenen mit zunehmendem Zeitablauf abnimmt. Dies wird auch für den postmortalen Persönlichkeitsschutz von Patientinnen und Patienten zu gelten haben. Hinzu kommt, dass Klaus Kinski selbst seine Erfahrungen in der Karl-Bonhoeffer-Nervenklinik in seiner Biografie veröffentlicht hat.[73]

Allerdings haben wir festgestellt, dass die Angaben über die Begleitumstände, insbesondere zur Beziehungsperson von Klaus Kinski, vor der Offenlegung der Akte hätten anonymisiert werden müssen. Patientenakten, an denen kein vergleichbares öffentliches Interesse besteht, dürfen auch künftig, selbst nach Ablauf der Schutzfristen, grundsätzlich nicht in personenbezogener Form genutzt werden. Darauf können die Patientinnen und Patienten vertrauen.

Wir werden uns für klarstellende gesetzliche Regelungen im Archivgesetz des Landes Berlin und im Landeskrankenhausgesetz einsetzen, die für vergleichbare Fälle in der Zukunft Rechtssicherheit schaffen können. Der Staatssekretär für Kulturelle Angelegenheiten unterstützt dieses Anliegen.

Zu den übermittelten Akten gehörten sog. „Euthanasie-Akten", also Patientenakten zu Menschen, die aufgrund ihrer psychischen Erkrankung im Dritten Reich ermordet wurden. Der Tatbestand des Mordes wegen einer psychischen Erkrankung ist, auch wenn der Tötung eine ärztliche Entscheidung zugrunde lag, keinesfalls geheimhaltungsbedürftig. Deshalb dürfen diese Akten der Öffentlichkeit nicht vorenthalten werden. Sie unterliegen ohne Einschränkung der zeitgeschichtlichen Forschung.

Das Patientengeheimnis gilt auch über den Tod hinaus. Niemand, der in ärztlicher Behandlung war, muss befürchten, dass seine Krankengeschichte ohne seine Einwilligung der Forschung zugänglich gemacht oder veröffentlicht wird. Begrenzte Ausnahmen gelten für verstorbene Personen der Zeitgeschichte und Opfer von NS-Verbrechen. Der Landesgesetzgeber ist zu Klarstellungen im Archiv- und Krankenhausrecht aufgerufen.

73 Ich bin so wild nach deinem Erdbeermund. München 1975 (Kapitel „Erwachsenenhölle")

9.2 Ein Täter und seine Opfer im „Dritten Reich“

Der Berliner Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (LStU) hat eine Biografie über Dr. Walter Linse herausgegeben. Er war 1952 vom Staatssicherheitsdienst der DDR illegal aus West-Berlin entführt und nach Verhören im Ostteil der Stadt von einem sowjetischen Militärtribunal zum Tode verurteilt und in Moskau erschossen worden. In der Biografie sollten Namen von Personen genannt werden, die Opfer der antisemitischen Arisierungspolitik im „Dritten Reich“ geworden waren. Walter Linse war im Dritten Reich in Chemnitz für die Arisierung verantwortlich. Der LStU legte uns eine Namensliste mit den als Opfer ermittelten jüdischen Geschäftsleuten aus Chemnitz vor. Die Liste entstammte den archivierten Unterlagen des Gewerbeamtes Chemnitz, die nun vom Staatsarchiv Chemnitz verwaltet werden. Dieses hatte gegen die archivarische Nutzung keine Bedenken gehabt. In der Annahme, dass auch keine Auflagen zur Veröffentlichung erteilt worden waren, haben wir die Zulässigkeit der Publikation mit den Namenslisten rechtlich bewertet.

Nach dem Berliner Datenschutzgesetz dürfen „die wissenschaftliche Forschung betreibenden öffentlichen Stellen personenbezogene Daten nur veröffentlichen, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist“[74]. Die Frage der „Arisierung“ ist Gegenstand der zeitgeschichtlichen Forschung im Sinne dieser Regelung. Denn die Arisierung erfolgte während des Nationalsozialismus mit öffentlicher Wirkung aufgrund der Rassegesetze und hatte zur Folge, dass die Verfolgten aus dem Blickfeld der Öffentlichkeit verschwanden, weil sie emigrierten, untertauchten oder später ermordet wurden. Die mit staatlichem Druck betriebene Arisierung beruhte auf einer menschenrechtswidrigen Verarbeitung und Nutzung besonders schutzwürdiger persönlicher Daten wie z.B. der Religionszugehörigkeit. Dieser staatliche Missbrauch und seine bekannten öffentlichen Auswirkungen können heute nur anhand wissenschaftlich überprüfbarer Namen (auch Namenslisten und Dateien) nachvollzogen werden. Die Wissenschaftlichkeit einer solchen Abhandlung ergibt sich daraus, dass hinsichtlich jeder einzelnen betroffenen Person nachvollziehbar wird, wer sie war. Eine

74 § 30 Abs. 5 b) BlnDSG

anonymisierte Namensliste entspräche diesem unverzichtbaren Erfordernis nicht. Folglich ist die Veröffentlichung der Namensliste unerlässlich – um so eher, als auch künftig immer wieder mit Versuchen gerechnet werden muss, die Verbrechen des Nationalsozialismus pseudowissenschaftlich im Einzelfall oder in allgemeiner Form zu leugnen. Es ist zwar davon auszugehen, dass der Berliner Gesetzgeber die Schutzwürdigkeit von noch lebenden Einzelpersonen erkannt hat. Gleichwohl hat er im Vorhinein eine abstrakte Abwägung vorgenommen. Dies schließt den Schutz der im Einzelfall schutzwürdigen Einzelinteressen nicht aus. Solche Einzelfälle lagen hier jedoch nicht vor.

Die gesetzliche Regelung zur wissenschaftlichen Forschung und zum Datenschutz in § 30 Abs. 5 b) Berliner Datenschutzgesetz (BlnDSG) löst den Grundrechtskonflikt zwischen Forschungsfreiheit und schutzwürdigen Belangen der „Beforschten“ in angemessener Weise, sodass sowohl dem Forschungs- und Publikationsinteresse als auch dem Schutzbedürfnis der Verfolgten des Nazi-Regimes Rechnung getragen werden kann.

10. Wissen und Bildung

10.1 Wissenschaft und Forschung

10.1.1 „Mein“ Genom im Internet

George Church, Genetikprofessor an der Harvard Medical School in Boston, ist derzeit weltweit einer der gefragtesten Genetiker. Er arbeitet an Decodier-Robotern, die rund sieben Millionen DNA-Bausteine pro Minute lesen können. Damit wird es möglich, die Kosten für die Sequenzierung eines persönlichen menschlichen Genoms bald von gegenwärtig einer Million Dollar auf lediglich tausend Dollar zu reduzieren.

Das internationale Humangenomprojekt (HGP) hatte die DNA von sechs verschiedenen Menschen gemischt und entschlüsselt. Mittlerweile weiß man, dass das Genom eines konkreten Menschen genauso individuell mit vielen Unterschieden ist wie das Äußere einer Person. Prof. Church schlug zunächst vor, von zehn Personen, darunter auch von sich selbst, die DNA zu entschlüsseln. Die rund drei Milliarden Bausteine der DNA von jeder dieser Personen nebst Informationen zu ihrem Gesundheitszustand und ihrem Lebensstil werden dann ins Internet gestellt. Die betroffenen Personen haben eingewilligt und wurden über die Risiken aufgeklärt. Namen werden zwar nicht genannt. Dennoch ist eine Zuordnung dieser Daten zur konkreten Person schon gegenwärtig nicht auszuschließen, und in Zukunft wird das erforderliche Potenzial hierfür erheblich wachsen.

Forscherinnen und Forscher in aller Welt sind aufgerufen, das Zusammenspiel der genetischen Faktoren sowie der Einflüsse von Umwelt und Lebensstil anhand der Daten des konkreten Individuums zu untersuchen (PGP – Personal Genome Project). Das Risiko eines Datenmissbrauchs trägt jedoch die DNA spendende Person. Er wird darauf hingewiesen, dass die so im Internet veröffentlichten Daten Einfluss auf den Abschluss von Versicherungen bzw. Arbeitsverträgen haben können. Ziel des Projekts ist, derartige Daten von rund 100.000 Personen im Internet zu veröffentlichen. Die Bedeutung und Notwendigkeit solcher Ansätze sind angesichts der Entwicklung der internationalen

Genomforschung und ihrer potenziellen Konsequenzen für das Individuum nachvollziehbar und müssen sorgfältig mit den möglichen Nachteilen und Risiken abgewogen werden.

Wissenschaftler am Max-Planck-Institut für molekulare Genetik in Berlin planen in enger Kooperation mit Prof. Church die Entwicklung einer deutschen, PGP-ähnlichen Komponente. Er besuchte im Sommer das Max-Planck-Institut und diskutierte sein Projekt mit Wissenschaftlern und den Datenschutzbeauftragten der Max-Planck-Gesellschaft, aber auch mit dem Hessischen Datenschutzbeauftragten, dem Nationalen Ethikrat und uns. Dabei wurde Übereinstimmung darüber erzielt, dass ein erstes Modellprojekt mit einer begrenzten Anzahl sorgfältig ausgewählter Teilnehmerinnen und Teilnehmer nützlich sein könnte. Allerdings sollen persönliche Daten nicht wie an der Harvard Medical School öffentlich verfügbar gemacht werden. Wir werden dieses Projekt weiter sorgfältig beobachten.

10.1.2 Der lückenhafte Gesetzentwurf zur Gendiagnostik

Ende August beschloss die Bundesregierung den Entwurf eines Gendiagnostikgesetzes.[75] Einvernehmlich begrüßten zunächst die Datenschutzbeauftragten, dass damit ihrer langjährigen Forderung nach einem Gentest- oder Gendiagnostikgesetz Rechnung getragen wurde. Der Entwurf sieht vor, die Verwendung genetischer Daten im medizinischen Behandlungszusammenhang oder für medizinische Tests sowie ein Verbot der Verwendung von Gentests im Arbeitsleben und eingeschränkt in der Versicherungswirtschaft zu regeln. Genetische Untersuchungen dürfen künftig nur durchgeführt werden, wenn die Betroffenen nach umfassender Aufklärung über den Zweck und mögliche Konsequenzen in diese Untersuchung schriftlich eingewilligt haben. Heimliche genetische Tests, auch zur Klärung der Abstammung, sollen zukünftig verboten sein. Momentan ist eine Verfolgung lediglich als Ordnungswidrigkeit vorgesehen, jedoch nicht als Straftat, was angemessener wäre.

Allerdings fehlen Regelungen zum Umgang mit genetischen Daten für Forschungszwecke. Schon 2001 haben die Datenschutzbeauftragten des Bundes

75 BT-Drs. 16/10532

und der Länder einen Vorschlag für ein Gentestgesetz veröffentlicht. Darin waren auch detaillierte und praktikable Regelungen für die Forschung vorgesehen. Unternehmen und Wissenschaftler haben uns bestätigt, dass damit Rechtssicherheit für die Forschung geschaffen würde. Bislang sieht die Bundesregierung keinen solchen Regelungsbedarf. Die Regelungslücke ist jedoch angesichts der immer noch wachsenden Bedeutung von genetisch-medizinischer Forschung und der Zunahme der Zahl von Biobanken, die Proben sowie umfangreiche medizinisch-diagnostische Daten aus genetischen Untersuchungen vorhalten, nicht angemessen. Ob der Gesetzentwurf noch in der laufenden Legislaturperiode verabschiedet wird, ist ungewiss.

Die genetische Forschung benötigt klare datenschutzrechtliche Rahmenbedingungen. Dies wäre ein Standortvorteil für die Bundesrepublik Deutschland.

10.1.3 Kompetenznetz angeborene Herzfehler (KNAHF) – Ein Mehrwert für Erkrankte

Bislang waren für eine Patientin bzw. einen Patienten, die sich im Nationalen Register für angeborene Herzfehler registrieren lassen und an Studien teilgenommen hatten, diese Daten nicht unmittelbar für die Behandlung verfügbar. Mit dem Versorgungsmodul des Kompetenznetzes soll die Patientin bzw. der Patient Zugriff auf ihre/seine Daten aus der Studiendatenbank, der Bilddatenbank und dem Register erhalten. Des Weiteren kann sie oder er die Möglichkeit nutzen, selbst Daten zum Gesundheitszustand einzupflegen. Damit kann sich die betroffene Person über ihre Krankheit informieren und direkt Zugang zu neuen Forschungsergebnissen erhalten. Falls sie dies wünscht, stehen diese Daten damit auch der behandelnden Ärztin oder dem Arzt zur Verfügung. Bislang wäre nur ein sehr zeitaufwendiger Weg über ein Auskunftsersuchen möglich gewesen. Das Versorgungsmodul ist als Patientenportal ausgerichtet. Das ärztliche Personal kann aufgrund der vielfältigen technischen und organisatorischen Probleme, insbesondere auch wegen der nicht kompatiblen Software, diese Möglichkeit noch nicht direkt erhalten. Des Weiteren wird mit diesem Portal den Patientinnen und Patienten die Möglichkeit gegeben, untereinander in Foren Kontakt aufzunehmen und Erfahrungen auszutauschen. Datenschutz-

rechtlich entscheidend ist bei diesem Verfahren, dass die Identifikationsdaten und die medizinischen Daten in getrennten Datenbanken gehalten werden.

Mit dem Versorgungsmodul des KNAHF können künftig die Patientinnen und Patienten darüber entscheiden, welche medizinischen Daten auch für die behandelnden Ärztinnen und Ärzte oder anderweitige Kommunikation zur Verfügung gestellt werden. Möglich wird dies über ein mehrstufiges Pseudonymisierungsverfahren.

10.1.4 Gesundheitsmonitoring des Robert-Koch-Instituts

Das Robert-Koch-Institut (RKI) ist eine Einrichtung des Bundesgesundheitsministeriums und fällt damit in die Kontrollzuständigkeit des Bundesbeauftragten für Datenschutz und Informationsfreiheit. Gleichwohl führt das RKI in Berlin für eine Reihe von Erhebungen Pretests durch und kooperiert dabei eng mit der Charité. Deshalb beraten wir das RKI im Rahmen der Vorbereitung der Pretests. Kern des Gesundheitsmonitorings ist das sog. Bundesgesundheitssurvey. Für die Studie zur Gesundheit Erwachsener in Deutschland sollen bis 2011 über 7.000 Personen medizinisch untersucht und befragt werden. Ein neuer Aspekt ist die Studie zur Multimorbidität und Gebrechlichkeit sowie zu den Umständen der Selbstbestimmtheit der Lebensführung im Alter ab 65 Jahren. Hier sollen später 1.400 Personen befragt und untersucht werden.

Gemeinsam suchten wir nach Wegen, wie die Stichprobenziehung, die Kontaktaufnahme, verschiedene Möglichkeiten von Kurzfragebögen und Wiederholungsbefragungen datenschutzgerecht durchgeführt werden können. Auch für Menschen im hohen Alter, die bislang nicht in solche Studien einbezogen wurden, mussten Verfahren gefunden werden, die bei eingeschränkter Einwilligungsfähigkeit oder körperlichen Gebrechen nicht zum Ausschluss aus der Studie führten und damit das Ergebnis erheblich verzerrt hätten. Die Pretests in Berlin sind zwischenzeitlich abgeschlossen worden. Es haben sich punktuelle Probleme ergeben, die nunmehr durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit für die bundesweiten Hauptuntersuchungen zu lösen sind.

Pretests sind auch aus datenschutzrechtlicher Sicht insbesondere bei der Bedarfsprüfung von großer Bedeutung. Für die Hauptuntersuchungen können somit maßgeschneiderte Lösungen gefunden werden.

10.1.5 Die Freie Universität Berlin und ihre Probleme mit den Datenschutzbeauftragten

Im November 2007 erfuhr die behördliche Datenschutzbeauftragte der Freien Universität (FU), dass ein Sicherheitsreport des Campus Management Systems (CM) generiert worden war, der nach Auffassung des Personalrats beträchtliche Sicherheitsmängel aufwies. Daraufhin bat sie zunächst den Kanzler der FU um die Übergabe einer Kopie des Sicherheitsreports, um diesem Hinweis auf Mängel der ordnungsgemäßen Verarbeitung nachgehen zu können. In der Antwort erklärte ihr der Kanzler, dass aus seiner Sicht die Übermittlung des Sicherheitsreports weder notwendig noch sinnvoll erscheine. Er begründete dies damit, dass sie nicht genügend Fachwissen habe, um den Report richtig zu interpretieren, und verwies darauf, dass nach Abschluss der internen Analysen neun Monate später eine IT-Fachkraft der FU bereit sei, die Ergebnisse und Konsequenzen zu erläutern.

Darin liegt ein grober Verstoß gegen die Unterstützungspflicht, die das Präsidium der FU nach dem Berliner Datenschutzgesetz gegenüber der behördlichen Datenschutzbeauftragten hat. Nach § 19 a Abs. 2 Satz 4 Berliner Datenschutzgesetz (BlnDSG) kann sich die behördliche Datenschutzbeauftragte jederzeit an das Präsidium wenden und unterliegt in Datenschutzangelegenheiten keinen Weisungen. Sie entscheidet daher unabhängig über das Vorgehen bei Prüfhandlungen. Die Erklärung, die erbetene Übermittlung sei „weder sinnvoll noch notwendig", missachtet diese Unabhängigkeit.

Technische Detailkenntnisse zu komplexen Systemen gehören nicht zur vorgeschriebenen Fachkunde der behördlichen Datenschutzbeauftragten. Dies bedeutet aber nicht, dass es unsinnig wäre, ihr die erbetenen technischen Unterlagen zur Verfügung zu stellen. Denn auch sie hat die Möglichkeit, erforderlichen Sachverstand beizuziehen. Die Unterstützungspflicht des FU-Präsidiums geht auch so weit, der behördlichen Datenschutzbeauftragten bei Bedarf FU-eigene oder fremde Sachverständige zur Verfügung zu stellen.

Die behördliche Datenschutzbeauftragte hat zu Recht auf der Übergabe des Originalreports bestanden, denn sie musste sich ein Bild davon machen, welche möglichen Sicherheitsmängel im November 2007 vorlagen, und durfte sich nicht mit der mündlichen Erläuterung einer späteren Auswertung des Reports zufrieden geben.

Das Vorgehen der FU ist gegenüber ihrem Präsidenten als Verstoß gegen die Pflicht zur Unterstützung der behördlichen Datenschutzbeauftragten beanstandet worden.

Der Sicherheitsreport weckte natürlich auch unsere Aufmerksamkeit. So baten wir den Kanzler um eine Kopie des Sicherheitsreports vom November 2007. Stattdessen erhielten wir eine Kommentierung des Reports vom Juli 2008. Dies wäre nicht weiter problematisch, sogar eine Unterstützung unserer Arbeit gewesen, wenn es sich um die Kommentierung aller Meldungen des Reports vom November 2007 gehandelt hätte. Das nahmen wir auch an und hätten den kommentierten Report vom Juli 2008 zur Vorbereitung eines verabredeten Kontrollgesprächs im November 2008 herangezogen - wenn wir nicht einen Tag vor dem Gespräch den Originalreport von der behördlichen Datenschutzbeauftragten erhalten hätten, der ihr inzwischen vom Personalrat zur Verfügung gestellt worden und wesentlich umfangreicher war als der kommentierte Report.

Das Datenschutzgesetz verpflichtet die Behörden und sonstigen öffentlichen Stellen, uns bei der Erfüllung unserer Aufgaben zu unterstützen. Dazu gehört insbesondere, uns Auskunft zu unseren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme. Diese Unterlagen und Akten sind uns herauszugeben und Kopien von Unterlagen, von automatisierten Dateien, von deren Verfahren und von organisatorischen Regelungen zur Mitnahme zur Verfügung zu stellen. Erst mit dem eher zufälligen Erhalt des Originalreports erfuhren wir, dass uns mit Schreiben im Juli eine Unterlage zugesandt worden war, die mit dem tatsächlich erbetenden Report weder identisch war (was wir wussten) noch inhaltlich mit diesem übereinstimmte (was wir erst beim Vergleich erfuhren). Somit mussten wir davon ausgehen, dass auch wir über den Inhalt des Originalreports im Unklaren gelassen werden sollten.

Dieses Verhalten der FU ist ebenfalls wegen unzureichender Unterstützung des Berliner Beauftragten für Datenschutz und Informationsfreiheit beanstandet worden.

Die behördliche Datenschutzbeauftragte hat dem Präsidium der FU mehrfach ihre Überlastung angezeigt. Es war deswegen auch zu prüfen, ob die FU ihrer Pflicht nach § 19 a Abs. 1 Satz 1 BlnDSG nachgekommen war, eine Vertreterin oder einen Vertreter der behördlichen Datenschutzbeauftragten zu bestellen, sodass von dieser Seite Unterstützung erhofft werden konnte.

Diese Pflicht zur Bestellung einer Vertreterin oder eines Vertreters der behördlichen Datenschutzbeauftragten besteht seit der Anpassung des Berliner Datenschutzgesetzes an die Europäische Datenschutzrichtlinie im Jahre 2001. Wir stellten fest, dass die FU bisher keine solche Bestellung vorgenommen hat. Bei einem Gespräch mit zwei Mitgliedern des Präsidiums wurde der Mangel eingeräumt. Als Lösung schlugen diese vor, eine gegenseitige Vertretung zwischen der Datenschutzbeauftragten der FU Dahlem und dem Datenschutzbeauftragten des Botanischen Gartens vorzusehen, der ebenfalls Teil der Freien Universität ist. Diese Lösung ist möglich, sofern der Datenschutzbeauftragte des Botanischen Gartens sowohl von der Qualifikation als auch hinsichtlich seines Zeitbudgets in die Lage versetzt wird, bei Abwesenheit der behördlichen Datenschutzbeauftragten der FU Dahlem diese zu vertreten.

Da wir allerdings danach von der Umsetzung dieser Maßnahme nichts mehr hörten, war auch dieser Verstoß gegen das Berliner Datenschutzgesetz zu beanstanden.

Die behördliche Datenschutzbeauftragte der FU beantragte beim Kanzler die Genehmigung einer Dienstreise zur Datenschutz-Sommerakademie des Unabhängigen Landeszentrums für Datenschutz in Kiel, einer Veranstaltung, bei der sich alljährlich Beschäftigte der Datenschutzbehörden sowie behördliche und betriebliche Datenschutzbeauftragte aus Deutschland und dem deutschsprachigen Ausland zur Fortbildung und zum Erfahrungsaustausch treffen. Diese Sommerakademie ist anerkanntermaßen die wichtigste Veranstaltung dieser Art in Deutschland.

Aus der Praxis

Die Datenschutzbeauftragte verfügt für Dienstreisen über ein eigenes Budget. Dennoch versagte ihr der Kanzler die Genehmigung, da er die dienstliche Notwendigkeit nicht anerkannte und mehr ein Interesse an der Aufgabenerfüllung in Berlin und am Abbau der von der Datenschutzbeauftragten angezeigten Überlastung sah.

Die Datenschutzbeauftragte unterliegt jedoch in Datenschutzangelegenheiten nach § 19 a Abs. 2 Satz 4 BlnDSG keinen Weisungen. Die Verweigerung der Genehmigung der Dienstreise, die zweifelsfrei in Datenschutzangelegenheiten erfolgen sollte, ist jedoch eine solche Weisung, der die Datenschutzbeauftragte nicht folgen musste.

Diese Missachtung der Weisungsfreiheit der behördlichen Datenschutzbeauftragten wurde nicht beanstandet, weil sie einen Antrag auf Genehmigung der Dienstreise gestellt hatte, sich selbst also darüber nicht im Klaren war, dass es einer Genehmigung nicht bedurfte.

Die behördliche Datenschutzbeauftragte nimmt derzeit ihre Aufgaben ohne jede unmittelbare personelle Unterstützung wahr. Nach dem altersbedingten Ausscheiden einer bis zum Sommer für sie tätigen Hilfskraft ist die Datenschutzbeauftragte ohne Sekretariatsunterstützung, muss also alle Sekretariatsaufgaben, die bei ihr im nicht unerheblichen Maße anstehen, selbst erledigen.

Uns wurde zugesagt, dass der behördlichen Datenschutzbeauftragten fachliche Unterstützung bei Bedarf gewährt wird. Dies gilt insbesondere für die wichtige Unterstützung aus dem IT-Bereich bzw. dem Institut für Informatik der Freien Universität. Der Datenschutzbeauftragten sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, nach § 19 a Abs. 3 Satz 2 BlnDSG Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Dazu gehört auch eine direkte personelle Unterstützung. Das Fehlen einer solchen personellen Unterstützung ist bei der Datenschutzbeauftragten einer der größten und bedeutendsten deutschen Hochschulen als unangemessen und unzumutbar anzusehen.

In Reaktion auf die Beanstandungen hat das Präsidium der FU die vorgesehene Bestellung des Stellvertreters der behördlichen Datenschutzbeauftragten inzwischen vorgenommen. Das Präsidium hat in seiner Stellungnahme zuge-

sichert, dass in Zukunft Anfragen der Datenschutzkontrollinstanzen vollständig und rechtzeitig beantwortet und die erforderlichen Unterlagen zur Verfügung gestellt werden. Die Erfüllung dieser Zusage gegenüber der behördlichen Datenschutzbeauftragten und die Beachtung ihrer Weisungsfreiheit und ihre Ausstattung werden wir weiter beobachten.

Abschließend muss aber auch anerkannt werden, dass die Freie Universität Berlin erhebliche Vorleistungen erbracht hat, um einen sicheren und ordnungsgemäßen Betrieb der universitären Datenverarbeitung zu gewährleisten. Die IT-Sicherheitsrichtlinie der FU sowie das Sicherheitskonzept für das IT-Verfahren Campus Management sind dafür gute Grundlagen. Unsere Abarbeitung des Sicherheitsreports ergab im Übrigen, dass die Gründe für die große Anzahl der Einträge im Sicherheitsreport zufrieden stellend erläutert und unsere noch offenen Fragen klar beantwortet werden konnten. Mängel waren von unserer Seite nicht mehr festzustellen. Die weitere Zusammenarbeit wurde auf fachlicher Ebene vereinbart.

Offenbar sagt die wissenschaftliche Exzellenz der Freien Universität nichts darüber aus, ob die Rechte der im Datenschutzgesetz vorgesehenen Kontrollinstanzen beachtet werden.

10.2 Schule

10.2.1 Bundesweite Schülerdatenbank – Was Neues?

Die Kultusministerkonferenz (KMK) verfolgte ihr Konzept zur Schaffung einer Datenbank zu schulstatistischen Einzeldaten über Schüler und Lehrer auch 2008 weiter. Die KMK übersandte Mitte des Jahres eine „Neufassung“ ihrer Konzeption.

Das überarbeitete Konzept lässt eine verfassungsrechtlich hinreichende Begründung bisher nicht erkennen. Die Begründungsversuche, dass die Ziele durch eine Stichprobe nicht erreichbar wären, sind nicht überzeugend. Auch andere Fragen wurden bisher nicht geklärt, die in Landesgesetzen festzuschreiben wären. Dies sind die Festlegung der Erhebungs- und Hilfsmerkmale,

Regelungen zur Auskunftspflicht und Maßnahmen zur Durchsetzung des Trennungsgebots von Statistik und Verwaltungsvollzug sowie der inneren Abschottung im Statistikbereich.

Im Konzept der KMK wird auf eine „hochwertige Pseudonymisierung der Datensätze" verwiesen. Wie hierdurch eine Rückverfolgbarkeit auf Dauer ausgeschlossen werden kann, bleibt unklar. Unklar ist bislang auch, wann und in welchem Umfang die Arbeitsgruppen der Kultusministerkonferenz unsere Bedenken aufgreifen werden.

An eine schulstatistische Datenbank, die die gesamte Schulkarriere abbilden soll, sind höhere datenschutzrechtliche Anforderungen zu stellen als an einen Datenbestand im Verwaltungsvollzug, der lediglich der Durchsetzung der Schulpflicht dient.

10.2.2 Errichtung einer automatisierten Schülerdatei in Berlin

Unabhängig von der Schülerdatenbank der KMK zur bundesweiten Erfassung von schulstatistischen Daten beabsichtigt die Senatsverwaltung für Bildung, Wissenschaft und Forschung (SenBWF) im Rahmen des Projekts eGovernment@school eine automatisierte Schülerdatei einzurichten, in der alle Schülerinnen und Schüler des Landes mit einem begrenzten Katalog von personenbezogenen Daten erfasst werden.

Eine derartige zentrale Datenerfassung über eine bestimmte Gruppe von Betroffenen ist grundsätzlich mit erheblichen datenschutzrechtlichen Risiken verbunden. Sie bedarf daher einer normenklaren gesetzlichen Regelung und gesteigerter technisch-organisatorischer Maßnahmen zur Datensicherheit. In der Rechtsgrundlage sind die Datenverarbeitungszwecke, die Voraussetzungen für die Zulässigkeit der Datenverarbeitung und die Zugriffsrechte auf den Datenbestand eindeutig, differenziert und abschließend zu bestimmen. Die Koalitionsfraktionen SPD und Die Linke haben den Entwurf für ein „Gesetz zur automatisierten Schülerdatei"[76] in das Parlament eingebracht.

76 Abghs.-Drs. 16/1931

Danach soll die automatisierte Schülerdatei ausschließlich für die Zwecke der „Schulorganisation“, der „Schulentwicklungsplanung“ sowie der „Kontrolle und Durchsetzung der Schul- und Berufsschulpflicht“ eingerichtet werden. Weitere Datenverarbeitungszwecke (wie der Kinder- und Jugendschutz) wurden entsprechend unserer Empfehlung nicht aufgenommen, da es sich nicht um originär schulbezogene Aufgaben handelt. Die personenbezogenen Daten, die über jede Schülerin und jeden Schüler in der Datei gespeichert werden sollen, sind abschließend in einem Katalog festgelegt worden. Die insgesamt 16 personenbezogenen Merkmale enthalten u.a. Angaben zum Namen, Geburtsdatum, Geschlecht, über Anschrift, Erziehungsberechtigte, Schule, Klasse, zur Überwachung der Schulpflicht, Schulanmeldung, über die nichtdeutsche Herkunftssprache und die Befreiung von der Zahlung eines Eigenanteils für Lernmittel.

Diese Daten, die bereits jetzt in den Schulen nach dem Schulgesetz und der Schuldaten-Verordnung (z.B. im Schülerbogen, wo allerdings statt der Herkunftssprache das Merkmal „Kommunikationssprache in der Familie“ erfasst wird) erhoben und gespeichert werden, sollen nach dem Gesetzentwurf von den Schulen in die vereinheitlichte Datei eingetragen und bei Bedarf berichtigt und ergänzt werden. Sie erhalten dafür Zugriffsrechte, die auf den Datenbestand der Schülerinnen und Schüler begrenzt sind, die ihre Schule besuchen, an ihr angemeldet sind oder an ihr angemeldet werden sollen. Bei einem Schulwechsel gehen die Datenverarbeitungsrechte von der abgebenden auf die aufnehmende Schule über. Auf Informationen über die nichtdeutsche Herkunftssprache oder die Befreiung von Lernmittelkosten einzelner Schülerinnen und Schüler dürfen nur die Schulen zugreifen.

Den bezirklichen Schulämtern werden nur Zugriffsrechte auf die Daten derjenigen Personen gestattet, die eine in ihrem Bezirk liegende Schule besuchen, an dieser angemeldet sind oder in deren Einschulungsbereich fallen. Der für das Schulwesen zuständigen Senatsverwaltung werden die Datenverarbeitungsbefugnisse ausschließlich für die zentral verwalteten Schulen eingeräumt. Auf die Daten der anderen Schulen kann die Senatsverwaltung ausschließlich für Zwecke der Schulorganisation und der Schulentwicklungsplanung und nur in aggregierter Form zugreifen. Ein Rückgriff auf die Daten einer konkreten Person muss ausgeschlossen sein.

Den Strafverfolgungsbehörden, der Polizei, den Jugendämtern einschließlich der Jugendgerichtshilfe, der Bewährungshilfe für Jugendliche und Heranwachsende und den Gesundheitsämtern ist auf Anfrage mitzuteilen, welche Schule eine Schülerin oder ein Schüler besucht, wenn dies für die Aufgabenerfüllung der anfragenden Stelle erforderlich ist. Die Daten in der Schülerdatei sind ein Jahr nach Ablauf des Schuljahres zu löschen, in dem die Betroffenen zuletzt eine Schule besucht haben, jedoch nicht vor Beendigung der Schulpflicht. Angaben über die Befreiung von der Zahlung eines Eigenanteils für Lernmittel sind spätestens ein Jahr nach Wegfall der Befreiung zu löschen.

Die automatisierte Schülerdatei für Berlin soll – nach Auskunft der SenBWF – in einem Rechenzentrum der Senatsverwaltung eingerichtet und mandantenfähig (13 Mandanten = für die 12 Bezirke und für die SenBWF wegen der zentral verwalteten Schulen) gestaltet werden. Die Datenauswertung und Berichterstattung soll mit einer präzisen Rollen- und Rechteverteilung erfolgen. Entsprechend der unterschiedlichen gesetzlichen und tatsächlichen Aufgabenstellung sollen die Schulen, die Schulträger in den Bezirken und die Schulaufsichtsbehörde (SenBWF) differenzierte Zugriffsrechte auf den Datenbestand erhalten. Ein direkter Zugriff von außen (z.B. durch die Justiz- oder Polizeibehörden) auf die Daten in der Schuldatenbank soll ausgeschlossen werden. Zu statistischen Zwecken sollen die Daten aus dem vorhandenen Datenbestand aggregiert werden. Der Datenzugriff soll für die Schulen über das Internet und für die Schulträger und die SenBWF über das Berliner Landesnetz jeweils verschlüsselt realisiert werden. Dies ist noch in einem detaillierten Sicherheitskonzept festzulegen, bevor die Schülerdatei betrieben werden darf.

Unsere Vorschläge zur Stärkung des Datenschutzes sind während der parlamentarischen Beratung aufgegriffen worden. Wir haben bei einer Anhörung im zuständigen Fachausschuss betont, dass vorgesehene Zweck- und Zugriffsbegrenzungen verfassungsrechtlich geboten seien und auch künftig nicht gelockert werden dürfen. Zudem müsse die Infrastruktur des Datenschutzes in den Schulen als Korrektiv zur Einführung der automatisierten Schülerdatei gestärkt werden. So müsse die Senatsverwaltung sicherstellen, dass entsprechend den gesetzlichen Vorgaben jede Berliner Schule eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennt. Der Senator für Bildung, Wissenschaft und Forschung hat dies zugesagt.

Durch die Änderung des Schulgesetzes wird eine ausreichende Rechtsgrundlage für die Einführung der automatisierten Schülerdatei geschaffen. Weitere rechtsverbindliche Vorgaben zum Umgang mit dieser Datei (z. B. Vergabe von Datenbefugnissen in den Schulen, Nutzung der Daten für Statistikzwecke und Vorgaben für technisch-organisatorische Maßnahmen) müssen durch eine Verordnung geregelt werden. Zudem muss die Infrastruktur des Datenschutzes in den Schulen verbessert werden.

10.2.3 Befragung über Unterrichtsstörer

Betroffene Eltern haben uns darüber informiert, dass Schülerinnen und Schüler einer 9. Klasse von ihrer Klassenlehrerin in einer anonymen Befragung (Fragebogenaktion) darum gebeten wurden, die Mitschülerinnen und Mitschüler namentlich zu benennen, die vermehrt den Unterricht bzw. die Klassensituation beeinträchtigen würden. Die ausgefüllten Fragebögen wurden von einer Elternvertreterin der Klasse ausgewertet. Auf Einladung dieser Elternvertreterin sollte das Thema auf einer Elternversammlung diskutiert und dabei den Eltern die Namen der angeblichen „Störer" mitgeteilt werden.

Durch die Aktion wurden personenbezogene Daten der angeblichen Störer hinter deren Rücken (da ohne deren Kenntnis) erhoben und gespeichert. Diese Form der Erhebung von personenbezogenen Daten ist datenschutzrechtlich grundsätzlich problematisch und nur in Ausnahmefällen, gestützt auf eine Rechtsgrundlage, zulässig. Nach § 64 Abs. 1 Schulgesetz (SchulG) darf die Schule personenbezogene Daten von Schülerinnen und Schülern erheben und speichern, soweit dies zur Erfüllung der ihr durch Rechtsvorschrift zugewiesenen „schulbezogenen" Aufgaben erforderlich ist. Eine „schulbezogene" Aufgabe ist die Organisation und Durchführung des Unterrichts. Den Lehrkräften wird durch § 67 Abs. 2 SchulG die Aufgabe zugewiesen, die ihnen anvertrauten Schülerinnen und Schüler im Rahmen der Bildungs- und Erziehungsziele und der geltenden Vorschriften zu unterrichten, zu erziehen, zu beurteilen, zu bewerten, zu beraten und zu betreuen. Ihnen ist dabei in gewissem Umfang ein pädagogischer Freiraum einzuräumen.

Der Auftrag der Schule und der pädagogische Freiraum der Lehrkräfte enden jedoch in jedem Fall dort, wo gezielt Maßnahmen eingesetzt werden, um Dritte (z.B. Mitschülerinnen/Mitschüler) „anonym zu denunzieren". Die Erhebung und Speicherung von personenbezogenen Daten über angebliche Unterrichtsstörer war daher ebenso unzulässig wie deren Weitergabe an die Elternvertretung der Klasse. Deren datenschutzrechtlicher Status ist im Schulgesetz nicht eindeutig geregelt. Es ist jedoch davon auszugehen, dass Elternvertretungen keine eigenen Daten verarbeitenden Stellen (wie z.B. Personalvertretungen) sind. Sie gehören vielmehr zur Schulorganisation und sind im Hinblick auf die Verarbeitung von personenbezogenen Daten Bestandteil der Schule. In den Bereichen, in denen das Datenschutzrecht berührt ist, besteht ein Über- und Unterordnungsverhältnis zwischen der Schulleitung und den Elternvertretungen mit rechtlicher Direktionsbefugnis.

Wie von uns empfohlen, hat die Schulleitung die Elternvertretung im Rahmen der Direktionsbefugnis angewiesen, die unzulässigen Daten über angebliche Unterrichtsstörer in den Fragebögen unkenntlich zu machen und dafür Sorge zu tragen, dass diese Daten in keinem Fall auf der Elternversammlung bekannt gegeben werden.

10.2.4 Einsatz von Videotechnik im Unterricht

Aus der Praxis

An einer Schule wurde in Kooperation mit externen Lerntherapeuten im Deutschunterricht mit Erstklässlern nach dem „IntraActPlus-Konzept" gearbeitet. Bei der Durchführung dieses Konzeptes wurde der Unterricht mit Videotechnik aufgezeichnet, um die „unbewussten Verhaltensanteile der Lehrer/Erzieher" und die „innere Anstrengungsbereitschaft des Kindes" im Unterricht bewusster wahrnehmen zu können. Die Speicherung der Videoaufzeichnungen sollte bis Ende des Schuljahres 2009/2010 erfolgen.

Eine „lückenlose" Videoaufzeichnung des Schulunterrichts über einen längeren Zeitraum führt zu einer umfassenden Leistungs- und Verhaltenskontrolle nicht nur der Schülerinnen und Schüler, sondern auch der Lehrkräfte. Mit dieser Maßnahme werden neben dem allgemeinen Unterrichtsgeschehen auch Verhaltensmuster und -auffälligkeiten der am Unterricht teilnehmenden Personen erfasst. Dabei handelt es sich auch um sensitive (Gesundheits-)Daten

der Betroffenen, die einem gesteigerten Schutz unterliegen. Erfolgt die Aufzeichnung dauerhaft während des gesamten Unterrichts und über einen längeren Zeitraum (z.B. über mehrere Unterrichtsstunden oder -tage), bedeutet dies einen erheblichen Eingriff in die Grundrechte der Betroffenen. Eine derartige „Kontrolle" wird – abgesehen vom Zweifel am pädagogischen Wert einer solchen Maßnahme – weder vom Schulgesetz noch durch andere Regelungen legitimiert. Sie kann auch nicht auf die Einwilligung der Betroffenen bzw. ihrer Erziehungsberechtigten gestützt werden.

Wenn überhaupt, darf die Videoaufzeichnung des Unterrichts – auch im Rahmen des „IntraActPlus-Konzepts" – nur im Ausnahmefall und zeitlich eng begrenzt erfolgen (z.B. Aufzeichnung von einzelnen, selektiven Unterrichtssituationen in einigen wenigen Unterrichtsstunden). Die so begrenzte Videoaufzeichnung des Unterrichts ist nur mit schriftlicher Einwilligung der Betroffenen (auch der Lehrkräfte sowie Erzieherinnen und Erzieher) zulässig; Personen, deren Einwilligung nicht vorliegt, dürfen nicht gefilmt werden. Die Betroffenen sind zuvor über die Bedeutung der Einwilligung aufzuklären, insbesondere den Verwendungszweck der Daten und bei beabsichtigten Übermittlungen auch über die Empfängerin oder den Empfänger der Daten (hier: z.B. die externen Lerntherapeuten). Sie sind unter Darlegung der Folgen darauf hinzuweisen, dass sie die Einwilligung verweigern können.[77] Da nicht auszuschließen ist, dass mit der Videoaufzeichnung auch sensitive personenbezogene Daten (z.B. Gesundheitsdaten) erhoben werden, muss sich die Einwilligung ausdrücklich auch auf diese Daten beziehen.[78]

Unsere Empfehlung, die Videoaufzeichnungen im Unterricht so zu reduzieren, dass eine „umfassende Leistungs- und Verhaltenskontrolle" ausgeschlossen ist, und von den Betroffenen im Vorfeld der Maßnahme eine informierte Einwilligung in die Datenverarbeitung einzuholen, hat die Schule umgesetzt. Ebenso wurde zugesagt, die erhobenen (Video-) Daten unmittelbar nach deren Auswertung zu löschen und nicht bis zum Ende des Schuljahres 2009/2010 zu speichern.

77 § 6 Abs. 3 BlnDSG
78 § 6 Abs. 5 Satz 3 BlnDSG

11. Wirtschaft

11.1 Rasterung auf Zuruf – Deutsche Telekom und Deutsche Bahn

Auch wenn die Deutsche Telekom AG (DT AG) der Datenschutzkontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterliegt, führte die Spitzelaffäre bei der DT AG zu verschiedenen Kontrollen, die in unsere Zuständigkeit fielen. Sie sind noch nicht abschließend bewertet. Allerdings können wir einen Zwischenbericht geben.

Die Kontrollen wurden teilweise dadurch erschwert, dass sich wichtige Unterlagen bei der Staatsanwaltschaft befinden. Wir haben ein Wirtschaftsberatungsunternehmen kontrolliert, das Überwachungsaufgaben von der DT AG und anderen Unternehmen erhielt und sie von einer Berliner Detektei durchführen ließ. Auch die Arbeitsweise der Detektei wurde überprüft.

Das Wirtschaftsberatungsunternehmen nahm bis 2003 von verschiedenen Unternehmen Überwachungsaufträge an. Allerdings wechselte 2003 das Management, und das Geschäftsfeld „Überwachungen“ wurde aufgegeben. Das Wirtschaftsberatungsunternehmen erhielt nur die Aufträge von den verschiedenen Unternehmen. Die eigentliche Bespitzelungsarbeit wurde von der Detektei ausgeführt. Diese wiederum schaltete für bestimmte besonders problematische Überwachungsmaßnahmen mehrere kleine Ein-Mann-Detekteien ein. Die jeweiligen Auftraggeber für die Ermittlungen interessierten sich nur für Ergebnisse. Innerhalb der „Informationskette“ Unternehmen – Wirtschaftsberatungsunternehmen – Detektei – Unterdetektei stellte sich niemand die Frage, ob der jeweils andere in der Kette Informationen rechtswidrig oder rechtmäßig erlangt hatte. Dies ging einher mit dem Bestreben, möglichst wenig schriftlich festzuhalten und wie im Fall der Detektei sämtliche Informationen nach Berichterstellung zu vernichten. So störte es auch niemanden, dass die Detektei die illegale Beschaffung von Informationen von der Bundesversicherungsanstalt für Angestellte und dem Kraftfahrt-Bundesamt in Rechnung stellte.

Unternehmen können im Einzelfall durchaus rechtmäßig Kontrollen durchführen, etwa um eine Diebstahlsserie aufzuklären. Solche Kontrollen setzen aber als notwendige Bedingung die Überprüfung des berechtigten Interesses voraus. Uns lagen keine Hinweise darauf vor, dass die beteiligten Unternehmen jeweils das berechtigte Interesse des Auftraggebers überprüft haben.

Die überprüfte Detektei hat zusammen mit anderen Detekteien im Auftrag des Wirtschaftsberatungsunternehmens einen Journalisten observiert (Tagesablauf, Bewegungsabläufe usw.). Der Journalist stand im Verdacht, von Telekom-Mitarbeitern und -Managern wichtige Informationen erhalten zu haben. Selbst wenn man ein berechtigtes Interesse der Telekom an Informationen über den Journalisten annehmen würde, war der Inhalt des Abschlussberichts rechtswidrig, da er auch Informationen über das Privatleben des Journalisten, insbesondere über seine Frau und Kinder, enthielt. In einem anderen Fall wurde der Großaktionär eines M-Dax-Unternehmens bespitzelt, da man ihm vorwarf, eine feindliche Übernahme zu planen.

Ein weiteres auf Überwachungen spezialisiertes Recherche-Unternehmen, das in vertraglicher Verbindung zur DT AG stand, konnte nicht überprüft werden, da es seinen Sitz nach Brandenburg verlegt hatte. Da dieses Unternehmen nicht nur bei der DT AG, sondern auch bei der Deutschen Bahn AG (DB AG) unter Vertrag stand, überprüften wir deren Zusammenarbeit mit diesem Unternehmen. Dessen Haupttätigkeit bestand in der Rasterung großer Datenbestände mit Hilfe von Spezialsoftware.

Auch bei der DB AG bestand offenbar ein erhebliches Interesse der Beteiligten, möglichst keine Spuren zu hinterlassen. So erteilten die verantwortlichen Mitarbeiter der DB AG ihre Aufträge fast ausschließlich mündlich. Selbst auf ein kaufmännisches Bestätigungsschreiben wurde verzichtet. Die Aufträge waren nur aufgrund der Berichte des beauftragten Unternehmens zu rekonstruieren. Sie wurden nach Art eines Nachrichtendienstes mit Projektnamen wie „Eichhörnchen“, „Uhu“, „Thymian“ oder „Traviata“ versehen. Hier einige Beispiele für Ermittlungsaufträge der DB AG, für die insgesamt rund 800.000 Euro gezahlt wurden:

- 774 Führungskräfte und 500 Ehepartner wurden hinter ihrem Rücken überprüft. Kontrolliert wurde das wirtschaftliche Engagement dieses Personenkreises außerhalb der Deutschen Bahn Gruppe. Die DB AG erhielt detaillierte Angaben zu den jeweiligen wirtschaftlichen Aktivitäten, also Position, Firmensitz, Gründungsdatum, Stammkapital, Jahresumsatz, Bonität, Mitarbeiterzahl, bei Gesellschaften auch Namen und Vornamen der Gesellschafter sowie Zweck und Ausrichtung des Unternehmens.
- Ein Mitarbeiter der DB AG hatte den Vorstandsvorsitzenden dieses Unternehmens eines Steuerdelikts bezichtigt und sich in einem Schreiben an mehrere Finanzbehörden gewandt. Dabei offenbarte er Informationen, zu denen etwa 40 Mitarbeiter Zugang hatten. Die DB AG übermittelte Namen, Vornamen, Personalnummer und zahlreiche dienstliche E-Mails der Betroffenen – darunter auch solche an den Betriebsrat – an das Ermittlungsbüro. Dieses beauftragte einen Schriftstilgutachter, um den Täter zu ermitteln.
- Wegen des Verdachts einer Vorteilsannahme wurden vier Mitarbeiter überprüft. Dazu kopierte die DB AG deren Festplatten und deren im Netz gespeicherte Dateien. Die Maßnahme erfolgte ohne Kenntnis der Betroffenen. Zusätzlich wurden ihre Büros nach Beweismaterial durchsucht. Die Informationen wurden dem Ermittlungsbüro übermittelt. Diese überprüften den Lebensstil eines Betroffenen, seine privaten Geld- und Kontobewegungen, seine Reisetätigkeiten und Familienverhältnisse. Außerdem erfolgte eine Analyse der im Internet gesuchten Seiten.

Keine dieser Überwachungsmaßnahmen war rechtmäßig, denn sie wurden ohne konkreten Verdacht veranlasst. Hinsichtlich der zu ziehenden Konsequenzen ist das Verfahren noch nicht abgeschlossen.

Es bestehen keine Zweifel, dass Wirtschaftsunternehmen ein berechtigtes Interesse daran haben, Wirtschaftskriminalität, den Verrat von Geschäftsgeheimnissen und Korruption zu bekämpfen. Dies ändert aber nichts daran, dass die Maßnahmen dagegen rechtmäßig sein und die schutzwürdigen Interessen der Betroffenen in ausreichender Form berücksichtigen müssen. Hierzu bedarf es in vielen großen deutschen Unternehmen einer neuen Datenschutzkultur. Überwachungsaufträge an Detekteien sind stets schriftlich zu dokumentieren.

11.2 Überraschende Abbuchungen

Aus der Praxis

Viele Bürgerinnen und Bürger haben sich darüber beschwert, dass ihnen per Lastschrift Geld für eine Fernsehzeitschrift abgebucht wurde, die sie nicht bestellt hatten. Die Mehrzahl der Betroffenen hatte kurz vorher einen Abonnement-Vertrag mit einem Privatsender gekündigt, der neben bestimmten Fernsehsendungen auch die Lieferung der Fernsehzeitschrift umfasste. Die Betroffenen hatten dem Privatsender eine Einzugsermächtigung eingeräumt. Sie zahlten für das Gesamtpaket, den Geldbetrag für die Fernsehzeitschrift überwies der Privatsender an den Zeitschriftenverlag. Dieser erhielt bei Abschluss eines Abonnements die Namen und die Anschriften der Betroffenen, um sie beliefern zu können. Nach der Kündigung des Abonnements übermittelte der Privatsender dem Verlag zusätzlich die Bankverbindungsdaten, um ihm die weitere Einziehung des für die Fernsehzeitschrift fälligen Betrages zu ermöglichen.

Die beiden beteiligten Unternehmen hielten ihre Verfahrensweise für rechtmäßig: Nach der Kündigung beim Privatsender würde der Vertrag mit dem Verlag bestehen bleiben. Dieser benötige die Bankverbindungsdaten für die Geldabbuchung.
Der Privatsender hatte für den Abschluss des Abonnement-Vertrages je nach Vertriebskanal unterschiedliche Formulare entwickelt. Keines dieser Formulare reichte aus, um die Übermittlung der Bankdaten im Falle einer Abonnement-Kündigung zu rechtfertigen. Die ohnehin sehr verbraucherunfreundliche Vertragsgestaltung[79] rechtfertigt nur dann Datenflüsse, wenn diese ausreichend transparent gemacht wurden. Dies setzt Folgendes voraus:

- Die Abonnentinnen und Abonnenten müssen bei Vertragsschluss die Information erhalten, dass sie nicht nur mit dem Privatsender, sondern auch mit dem Verlag einen Vertrag abschließen.
- Die Betroffenen müssen in ausreichender Weise darauf hingewiesen werden, dass sie das Gesamtabonnement nur dadurch beenden können, dass sie beim Privatsender den Fernsehvertrag und beim Verlag die Fernsehzeitschrift kündigen.

79 Wozu benötigt man eine Fernsehzeitschrift für ein Fernsehprogramm, welches man gerade gekündigt hat?

- Die Übermittlung der Bankverbindung setzt voraus, dass nicht nur dem Privatsender, sondern im Falle einer Kündigung auch dem Verlag der Bankeinzug gestattet worden ist.
- Teilweise ließ sich der Privatsender für die Übermittlung der Bankverbindungsdaten eine datenschutzrechtliche Einwilligung geben. Diese war aber unwirksam, da die Einwilligungserklärung im Text nicht hervorgehoben war.[80]
- Die Vertragsbedingungen sollten zur Schaffung ausreichender Transparenz nicht nur im Kleingedruckten stehen. Die Gestaltung des Formulars sollte sicherstellen, dass der Inhalt des Vertrages lesbar und verständlich ist.

Der Verlag wurde aufgefordert, gegenüber seinem Vertragspartner datenschutzgerechte Formulare einzufordern. Falls dies nicht gelingt, ist das Vertragsverhältnis mit dem Privatsender zu beenden.

Hinzu kam, dass es bei dem Privatsender in der Vergangenheit zu gravierenden Computerfehlern gekommen war, die dazu führten, dass viele Kundinnen und Kunden trotz Kündigung im Datenbestand des Privatsenders gespeichert blieben. Hierunter fiel auch der Sohn eines Kunden, der gegenüber dem Privatsender den Tod seines gleichnamigen Vaters bekannt gegeben hatte. Seine Bankverbindung hatte er dem Privatsender nur mitgeteilt, um eventuell zuviel bezahlte Geldbeträge zurückzuerhalten. Der Datensatz wurde dem Verlag übersandt, der davon ausging, dass der Vater umgezogen sei und das Komplett-Paket gekündigt hatte. Folglich erhielt nun der Sohn die Fernsehzeitschrift, und der fällige Geldbetrag wurde von seinem Konto abgebucht.

Unsere Beanstandung hat dazu geführt, dass der Privatsender und der Zeitschriftenverlag ihr datenschutzunfreundliches Komplett-Paket nicht mehr anbieten.

80 § 4 a Abs. 1 letzter Satz BDSG

11.3 Institutsübergreifende Warnmeldungen bei Berliner Banken

Aus der Praxis

Verschiedene Berliner Banken haben sich darauf verständigt, bei tatsächlich oder vermeintlich auffälligem Kundenverhalten institutsübergreifend zu warnen. Gemeldet werden der Name, das Geburtsdatum, die Adresse sowie das Delikt, das den Betroffenen vorgeworfen wird, etwa Kartenbetrug, Phishing, Kartenmissbrauch (mit gefälschten Unterlagen). Eingemeldet werden auch Personen, deren Identität missbraucht wurde. Für die Verdächtigen hat die Warnmeldung zur Folge, dass sie mit keiner der beteiligten Banken in Geschäftskontakt treten können. Häufig verlieren sie auch ihr Girokonto. Da die Banken über die Warnmeldung nicht informieren, ist für die Betroffenen nicht nachvollziehbar, warum sie kein Girokonto eröffnen können. Die Daten der Betroffenen werden nach zehn Jahren gelöscht. Das Warnsystem wurde bei einem Treffen der Berliner Banken vereinbart. Genauere Verfahrensregelungen wurden nicht geschaffen.

Die Daten empfangenden Banken haben ein berechtigtes Interesse, sich vor krimineller Kundschaft zu schützen.[81] Die Datenübermittlung erfolgt ohne eindeutige Erkenntnisse darüber, ob sich die zweifelhafte Kundin bzw. der zweifelhafte Kunde auch an andere Banken wendet. Dies erscheint allerdings hinnehmbar, sofern der Verdacht nicht fernliegend ist, dass die Person auch gegenüber anderen Banken in gleicher oder ähnlicher Weise auffällig werden könnte.

Die Datenübermittlung ist aber nur dann rechtmäßig, wenn kein Grund zu der Annahme besteht, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben. Danach ist die Übermittlung bei harten Negativmerkmalen rechtmäßig. Diese liegen vor, wenn die Betroffenen rechtskräftig verurteilt wurden. Im Übrigen ist eine institutsübergreifende Warnmeldung nur dann zulässig, wenn ein hinreichend erhärteter Tatverdacht besteht. Hierzu sollte das warnende Institut zuvor auch Anzeige wegen der vermuteten Straftat gestellt haben. Grundsätzlich muss eine Interessenabwägung unter Berücksichtigung der Interessen der Betroffenen stattfinden, bevor eine Meldung erfolgt. Die Banken sollten über verfahrenssichernde Compliance-

81 § 28 Abs. 3 Satz 1 Nr. 1 BDSG

Regelungen verfügen, die auch die Dokumentation der Gründe für die Warnmeldung vorsehen, um eine Nachprüfung zu ermöglichen.

Den Betroffenen ist grundsätzlich die Möglichkeit einzuräumen, der Erfassung wirksam zu widersprechen. Hierzu müssten sie über die geplante Datenübermittlung informiert werden. Es sollte die Löschung der Daten vorgesehen sein, falls die Betroffenen freigesprochen oder das Verfahren mangels Tatverdachts eingestellt wird. Die Betroffenen sollten hierauf hingewiesen werden. Falls eine vorherige Mitteilung im Einzelfall nicht möglich ist (z.B. im Eilt-Fall), sind die Betroffenen nach § 33 Bundesdatenschutzgesetz (BDSG) zu benachrichtigen, sofern nicht ausnahmsweise auf eine Benachrichtigung verzichtet werden kann. Widerspruchsmöglichkeit und Benachrichtigung sind insbesondere erforderlich, wenn die gespeicherten Daten Dritte betreffen, deren Identität missbraucht wurde.

Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Das Warnerfordernis dürfte sich deutlich vor Ablauf der von den Banken praktizierten Löschungsfrist erledigt haben. Da es bei den Warnmeldungen um Straftaten geht, ist außerdem das Bundeszentralregistergesetz zu beachten. Danach sind Angaben zu Straftaten, die im Bundeszentralregister bereits getilgt sind, unzulässig.

Die Banken wurden aufgefordert, das Warnsystem umzustrukturieren oder völlig aufzugeben.

Das von den Berliner Banken praktizierte institutsübergreifende Warnsystem bei auffälligem Kundenverhalten ist rechtswidrig.

11.4 Datenerhebung bei „einseitigem Due-Diligence-Verfahren“

Aus der Praxis

Einige Unternehmen, Investmentbänker und Risikofonds sind ständig auf der Suche nach lohnenden Investitionsmöglichkeiten. Im Fokus stehen insbesondere unterbewertete Unternehmen, lukrative Unternehmensteile oder Gesellschaften, die sich in einer wirtschaftlichen Notlage befinden und deshalb zum „Ausschlachten“ eignen. Da solche „Heuschrecken“ häufig auch feindliche Übernahmen vorbereiten, findet hier kein geordnetes Due-Diligence-Verfahren statt. Vielmehr wird versucht, hinter dem Rücken der Unternehmensleitung an Informationen darüber zu gelangen, ob die geplante Investition lohnend ist. Die nötigen Ermittlungen werden teils von dem Investor selbst durchgeführt, teils werden Investmentbanken, Wirtschaftsberater, Detekteien oder Auskunfteien eingeschaltet. In welchem Umfang dürfen Investoren im Vorfeld einer Übernahme Informationen über ein Unternehmen, gesetzliche Vertreter des Unternehmens und leitende Angestellte einholen?

Der Schutzzweck des Bundesdatenschutzgesetzes beschränkt sich zwar auf natürliche Personen, bezieht sich also nicht auf Aktiengesellschaften und andere juristische Personen. Geschützt wird aber das informationelle Selbstbestimmungsrecht von Einzelhandelskaufleuten und von natürlichen Personen (wie Gesellschafter, Geschäftsführer, Aufsichtsrat), deren Wirken für das Übernahmeziel von Bedeutung ist.

Sowohl nach § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG als auch nach § 29 Abs. 2 Satz 1 Nr. 1 a) BDSG (bei Einschaltung einer Auskunftei) setzt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ein berechtigtes Interesse des Investors voraus. Bei Bonitätsprüfungen vor Abschluss eines Vertrages wird das berechtigte Interesse nur dann angenommen, wenn der Vertrag kurz vor dem Abschluss steht und die Frage der Bonität die letzte Hürde für den Vertragsschluss darstellt. Würde man dies auf Firmenübernahmen übertragen, so hätten Investoren bei feindlichen Übernahmen kein berechtigtes Interesse an Vor-abinformationen. In einer freien Marktwirtschaft wird man aber im Zeitalter des Investmentbanking und der „Heuschrecken“ auch ein berechtigtes Interesse an feindlichen Übernahmen anerkennen müssen.

Da hier die Datenerhebung und -verarbeitung deutlich im Vorfeld eines Übernahmevertrages erfolgt, sind die schutzwürdigen Interessen der Betroffenen jedoch besonders zu berücksichtigen. Bei der Recherche sollte grundsätzlich auf personenbezogene Daten verzichtet werden, soweit sie nicht allgemein zugänglich sind.[82] Auf die Überprüfung der Bonität und des Privatlebens von natürlichen Personen ist demgegenüber zu verzichten.

Im Vorfeld einer feindlichen Übernahme dürfen Investoren nur personenbezogene Daten erheben und verarbeiten, die allgemein zugänglich sind.

11.5 Alles aus einer Hand? – Der „Einheitliche Ansprechpartner“ nach der EU-Dienstleistungsrichtlinie

Künftig sollen Unternehmerinnen und Unternehmer in Berlin nicht mehr eine Vielzahl von Behörden aufsuchen müssen, um Genehmigungen zu erhalten. Sie sollen vielmehr alle Verfahren und Formalitäten, die für die Aufnahme und Ausübung ihrer Dienstleistungstätigkeit erforderlich sind, zentral über einen Einheitlichen Ansprechpartner abwickeln können. Das betrifft insbesondere das Abgeben, Stellen oder Veranlassen von Erklärungen, Anmeldungen und Genehmigungsanträgen sowie die Vornahme von Registereintragungen. Zudem soll der Einheitliche Ansprechpartner als umfassende Auskunftsstelle zu allen bestehenden Anforderungen, Zuständigkeiten und weiteren Beratungsmöglichkeiten fungieren. Er ist damit als **integrierender Vermittler** zwischen den verschiedenen zuständigen Stellen der Verwaltung (z.B. Genehmigungsbehörden) und den Dienstleistenden konzipiert. Er soll zudem eine vollständig elektronische Verfahrensabwicklung (über das Internet) ermöglichen. Für Berlin ist geplant, den Einheitlichen Ansprechpartner bei der Senatsverwaltung für Wirtschaft, Technologie und Frauen einzurichten. Er soll durch bezirkliche „Kopfstellen“ unterstützt werden. Eine enge Verzahnung mit bestehenden Angeboten und Leistungen der Wirtschaftsförderung ist beabsichtigt.

82 § 28 Abs. 1 Satz 1 Nr. 3 BDSG

Hintergrund dieses neuen Organisationskonzepts ist die **EU-Dienstleistungsrichtlinie**[83], die bis Ende 2009 von den Mitgliedstaaten in nationales Recht umzusetzen ist. Durch die Beseitigung von Binnenmarkthindernissen im Dienstleistungsbereich soll Europas Wettbewerbsfähigkeit gestärkt werden. Dazu sollen schwerfällige Verwaltungsverfahren vereinfacht werden. Zu den Maßnahmen der Verwaltungsvereinfachung, die durch die Richtlinie vorgegeben werden, gehören die Förderung von E-Government und die Einführung von Einheitlichen Ansprechpartnern für grenzüberschreitende Dienstleistungsanbieter und -empfänger. In Deutschland ist vorgesehen, die neuen behördlichen Infrastrukturen nicht nur für Staatsangehörige von EU-Staaten einzurichten, sondern auch Deutschen zur Verfügung zu stellen.

Zur Wahrnehmung seiner weit gefassten Servicefunktionen wird der Einheitliche Ansprechpartner in großem Umgang personenbezogene Daten der Dienstleistenden erheben und verarbeiten müssen. Seine Tätigkeit erfordert in der Regel eine eigene Aktenführung. Eine Beschränkung auf die bloße Durchleitung von Informationen an die zuständigen Fachbehörden ohne eigene Kenntnisnahme der Inhalte wird nur in Einzelfällen möglich sein.

Die Vernetzung der zuständigen Stellen über den Einheitlichen Ansprechpartner und seine Vermittlerposition für eine Vielzahl unterschiedlicher Fachverfahren stehen in einem erheblichen Spannungsverhältnis zu den Schutzmechanismen der informationellen Selbstbestimmung. Die Prinzipien der Zweckbindung, der Transparenz der Datenverarbeitung und -nutzung sowie die **informationelle Gewaltenteilung** werden durch die verfahrensübergreifende Konzentration personenbezogener Daten beim Einheitlichen Ansprechpartner in Frage gestellt. Schon bei der Datenerhebung besteht die Gefahr, dass die betroffenen Unternehmen nicht klar erkennen können, für welchen einzuleitenden Verwaltungsvorgang und damit für welchen Zweck bestimmte Informationen benötigt werden und an welche zuständige Stelle die Daten ggf. weitergeleitet werden.

Um ein ausreichendes Schutzniveau für die Betroffenen sicherzustellen, müssen daher Kompensationsmöglichkeiten gesucht und bei der rechtlichen und

83 Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27. Dezember 2006, S. 36)

technischen Gestaltung der Verfahren berücksichtigt werden. Hierbei kann an Überlegungen angeknüpft werden, die bereits bei der Einrichtung der Berliner **Bürgerämter** angestellt wurden.[84] In ihrer integrativen Wirkung und der an den Lebenslagen der Bürger orientierten Aufgabenwahrnehmung ähneln diese stark dem Einheitlichen Ansprechpartner.

Derzeit wird von der federführenden **Senatsverwaltung für Wirtschaft, Technologie und Frauen** im Rahmen des Gesamtprojekts „Umsetzung der EU-Dienstleistungsrichtlinie in Berlin“ das Profil des Einheitlichen Ansprechpartners erarbeitet, um die gesetzlichen Voraussetzungen für dessen Tätigkeit zu schaffen. Wir sind in beratender Funktion in das Projekt einbezogen und haben im Hinblick auf die Einrichtung des Einheitlichen Ansprechpartners u.a. folgende Forderungen vorgetragen:

- Für den Umgang mit personenbezogenen Daten durch den Einheitlichen Ansprechpartner ist eine **bereichsspezifische normenklare gesetzliche Grundlage** zu schaffen. Dabei ist insbesondere klarzustellen, in welcher Tiefe (Inhalt, Umfang, Ausmaß) durch den Ansprechpartner – in Abgrenzung zu den letztendlich entscheidenden Stellen – Daten verarbeitet werden sollen.
- Bereits bei der Normsetzung sind die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten und Vorgaben für eine datenschutzfreundliche Gestaltung der Verfahren zu formulieren.
- Die Befugnisse zur Datenerhebung und -verarbeitung müssen – um doppelte Datenverarbeitung zu vermeiden oder wenigstens zu minimieren – auf die für die Aufgabenwahrnehmung des Einheitlichen Ansprechpartners zwingend **erforderlichen Daten** beschränkt werden. Die Aufgaben müssen dem Ansprechpartner gesetzlich zugewiesen und möglichst präzise gefasst werden.
- Es sind eigene Regelungen zur **Datenübermittlung** zwischen Einheitlichem Ansprechpartner und etwaigen Daten empfangenden Stellen zu treffen.
- Eine enge **Zweckbindung** ist gesetzlich festzuschreiben.

84 Vgl. JB 2001, 3.5; Gesetzliche Regelungen zur Datenverarbeitung durch die Bürgerämter finden sich in § 37 Abs. 4 Bezirksverwaltungsgesetz.

- Für die **Löschung** der Daten beim Einheitlichen Ansprechpartner sind eindeutige Fristen vorzusehen. So ist nach Abschluss eines Genehmigungsverfahrens in der Regel nur noch der Zugriff auf einen Kerndatensatz nötig.
- Es sind Regelungen erforderlich, die eine hohe **Transparenz** der Verarbeitungsvorgänge für die betroffenen Bürgerinnen und Bürger gewährleisten.
- Die Rechte auf **Auskunft, Berichtigung und Löschung** müssen den von der Datenverarbeitung betroffenen Personen auch gegenüber dem Einheitlichen Ansprechpartner zustehen.

Die Schaffung von „Einheitlichen Ansprechpartnern" läuft zentralen Schutzprinzipien des Datenschutzrechts zuwider und schwächt die auf Aufgabenteilung der Verwaltung aufbauenden Schutzmechanismen. Um dennoch ein ausreichendes Datenschutzniveau für die Betroffenen sicherzustellen, müssen Kompensationsmöglichkeiten gefunden und in bereichsspezifischen gesetzlichen Regelungen für den Umgang mit personenbezogenen Daten verankert werden.

12. Europäischer und internationaler Datenschutz

12.1 Europäische Union

Am 27. November hat der Rat der Innen- und Justizminister den **EU-Rahmenbeschluss** über den Schutz personenbezogener Daten verabschiedet, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[85] Zwar ist zu begrüßen, dass nach mehrjährigen Verhandlungen nun ein gemeinsamer Rahmen für diesen Bereich beschlossen wurde. Gleichwohl ist zu bemängeln, dass damit nur der Datenaustausch zwischen den Behörden der EU-Mitgliedstaaten geregelt wird, nicht jedoch die Datenverarbeitung durch Polizei- und Strafverfolgungsbehörden auf nationaler Ebene. Da die übermittelten Daten im Empfängerland mit den dort erhobenen Daten zusammengeführt werden, gelten für diese Datenarten verschiedene Datenschutzstandards. Die Ausgestaltung der Rechte von Betroffenen auf Auskunft, Löschung und Berichtigung soll laut Rahmenbeschluss dem jeweiligen nationalen Gesetzgeber überlassen sein. Dadurch ist ein einheitlicher Datenschutzstandard in der EU nicht zu erreichen. Darüber hinaus gibt es im Bereich der Zusammenarbeit der EU-Mitgliedstaaten in der sog. 3. Säule (Gemeinsame Innen- und Rechtspolitik) kein unabhängiges Gremium mit Datenschutzbeauftragten aus den Mitgliedstaaten, das zumindest beratend tätig werden könnte.[86] Deshalb können Rechtsakte und Maßnahmen zur polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene ohne Beteiligung von Datenschutzgremien verabschiedet werden.

Die EU-Regelung zum Datenschutz bei Polizei und Justiz ist nicht mehr als ein erster Schritt und dringend ergänzungsbedürftig.

85 ABl. L 350 vom 30. Dezember 2008, S. 60 ff.

86 Anders als beim Datenschutz in der sog. 1. Säule (Wirtschaft): Hier nimmt die Art. 29-Datenschutzgruppe diese Aufgabe wahr.

Das europaweite Koordinierungsverfahren der Datenschutzaufsichtsbehörden zur Anerkennung von **verbindlichen Unternehmensregelungen** hat eine neue Qualität erreicht: Mehrere europäische Aufsichtsbehörden haben sich mit einer politischen Erklärung zur gegenseitigen Anerkennung **(Mutual Recognition)** der durch die federführende Aufsichtsbehörde geprüften Unternehmensregelung verpflichtet. Neben Deutschland handelt es sich um Frankreich, Großbritannien, Irland, Island, Italien, Lettland, Liechtenstein, Luxemburg, Malta, Niederlande, Norwegen, Slowenien, Spanien, Tschechien und Zypern. Die Zahl der beteiligten Aufsichtsbehörden wird hoffentlich noch steigen. Nach Sinn und Zweck der politischen Erklärung wird künftig darauf vertraut, dass die federführende Aufsichtsbehörde die Prüfung ordnungsgemäß nach den bekannten, EU-weit einheitlichen Standards vollzogen hat. Die Unternehmensregelung selbst muss also nicht mehr von den übrigen europäischen Datenschutzbehörden auf Datenschutzkonformität geprüft werden. Dies führt für alle Beteiligten zu einer Straffung des Verfahrens, das bislang auch unter dem erheblichen Abstimmungsaufwand unter den Datenschutzbehörden litt. Die Unternehmen werden nun schneller in die Lage versetzt, globale Datenflüsse aus Europa nach einheitlichen Standards zu veranlassen.

Diese Neuerung entspricht zwar nicht der ursprünglichen Grundidee der EU-weiten Koordinierung der Anerkennung von Unternehmensregelungen, kommt ihr aber sehr nahe. Danach sollte ein weltweit tätiges Unternehmen nur **einen** Antrag auf Genehmigung bei der federführenden Datenschutzbehörde eines Mitgliedstaats stellen können, was zur „automatischen" Erteilung von Genehmigungen durch die übrigen Aufsichtsbehörden in Europa führen sollte.[87] Dem stehen allerdings die nationalen Verwaltungsverfahrensgesetze entgegen, die unterschiedliche Genehmigungsvoraussetzungen – aber eben keinen Automatismus – vorsehen. Die am neuen Verfahren beteiligten Behörden werden diese Bedingungen formulieren und von vornherein offen legen, damit die Unternehmen wissen, welche wenigen nationalen Anforderungen im jeweiligen Mitgliedstaat nach Anerkennung der Unternehmensregelung zu erfüllen sind. In Deutschland muss der Genehmigungsantrag zumindest die Datenkategorien, den Zweck und das Ziel der Übermittlung umfassen.

87 Dazu bereits JB 2004, 4.7.1

Diese Entwicklung wurde begünstigt durch drei weitere Arbeitspapiere der Art. 29-Datenschutzgruppe, zu deren Beachtung als Prüfungsmaßstab sich die am gegenseitigen Anerkennungsverfahren beteiligten Aufsichtsbehörden verpflichtet haben. Die Arbeitspapiere dienen primär der Erleichterung für Unternehmen bei der Anwendung von verbindlichen Unternehmensregelungen[88] bzw. bei einer erstmaligen Erstellung[89]. Zusätzlich ist die Art. 29-Datenschutzgruppe bestrebt, häufig gestellte Fragen von Unternehmen entsprechend den gesammelten Erfahrungen in einem weiteren Arbeitspapier zu beantworten, das fortgeschrieben wird.[90]

Für Berliner Unternehmen, die die Genehmigung der Datenübermittlung auf der Grundlage von verbindlichen Unternehmensregelungen oder Datenexportverträgen nach § 4 c Abs. 2 Bundesdatenschutzgesetz (BDSG) bei uns beantragen, gibt es erstmals eine Gebührenregelung, die einen Rahmen von 6.000 bis 18.000 Euro vorsieht.[91] Die Gebührenobergrenze wird aber nicht ausgeschöpft werden müssen, wenn die Unternehmensregelung bereits von der federführenden Aufsichtsbehörde im neuen europäischen Koordinierungsverfahren überprüft oder ein Standardvertrag der Europäischen Kommission vom Unternehmen nur geringfügig abgewandelt wurde.

Die Entwicklungen zu einer effektiveren Zusammenarbeit der europäischen Aufsichtsbehörden bei der EU-weiten Anerkennung von verbindlichen Unternehmensregelungen sind sehr zu begrüßen.

Daneben hat die Art. 29-Datenschutzgruppe wieder mehrere Arbeitspapiere und Stellungnahmen verfasst. So hat sie ein **Arbeitspapier zum Schutz der personenbezogenen Daten von Kindern**[92] herausgegeben, das sich haupt-

88 Arbeitsdokument WP 153 vom 24. Juni 2008: Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR), vgl. Dokumentenband 2008, S. 79

89 Arbeitsdokument WP 154 vom 24. Juni 2008: Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR), vgl. Dokumentenband 2008, S. 90

90 Arbeitsdokument WP 155 ref. 02, i. d. F. vom 10. Dezember 2008: Frequently Asked Questions (FAQs) related to Binding Corporate Rules

91 Tarifstelle 9104 b), Gebührenverzeichnis der Verwaltungsgebührenordnung i. d. F. vom 9. September 2008, GVBl. S. 254 ff. (262)

92 Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) vom 18. Februar 2008, WP 147

sächlich an Schulbehörden richtet, aber auch an Schülerinnen und Schüler, die frühzeitig lernen müssen, die eigenen Daten zu schützen und die Privatsphäre Dritter zu respektieren. Die Gruppe hat auch Stellung genommen zu **Datenschutzfragen im Zusammenhang mit Suchmaschinen**[93]. Diese sind zu einem festen Bestandteil des Alltags der Menschen geworden, die das Internet und Technologien zur Informationsgewinnung nutzen. Darüber hinaus wurden neue Anforderungen an die **Information von Fluggästen** bezüglich der Übermittlung ihrer PNR-Daten[94] an US-amerikanische Behörden formuliert[95]. Informationspflichtig sind primär die Fluggesellschaften, soweit sie Flüge in die USA anbieten, aber auch Reisebüros, die USA-Flüge verkaufen. Rechtzeitig zu den Olympischen Spielen in Peking hat die Art. 29-Datenschutzgruppe zum **Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code** Stellung genommen. Danach sind die Athleten verpflichtet, den Anti-Doping-Organisationen regelmäßig bestimmte Daten zu übermitteln, die anschließend zusammen mit anderen, auch sensiblen Daten in der in Kanada geführten Datenbank ADAMS gespeichert werden.[96] Wer sich den weit reichenden Kontrollen – aus welchen Gründen auch immer – entzieht, muss damit rechnen, dass er im Internet indirekt als Dopingsünder angeprangert wird.

12.2 AG „Internationaler Datenverkehr“

Die AG „Internationaler Datenverkehr“ des Düsseldorfer Kreises hat sich unter unserem Vorsitz mit Verfahrensfragen zu den im letzten Jahr[97] erörterten Fragestellungen befasst, die sich bei **Datenübermittlungen durch deutsche Unternehmen an US-Behörden** sowie **an US-Unternehmen im Vorfeld von Rechtsstreitigkeiten („Discovery“)** ergeben.

93 Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen vom 4. April 2008, WP 148, vgl. Dokumentenband 2008, S. 41

94 JB 2007, 10.1

95 Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden vom 24. Juni 2008, WP 151

96 Stellungnahme 3/2008 zum Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code vom 1. August 2008, WP 156, vgl. Dokumentenband 2008, S. 104

97 JB 2007, 10.3

Nach Auffassung des Bundesamts für Justiz sollte in der ersten Fallkonstellation deutschen Unternehmen empfohlen werden, die US-Behörden auf den Rechtshilfeweg zu verweisen. Diese müssen ein hinreichend konkretes Rechtshilfeersuchen beim Bundesamt für Justiz stellen, das ggf. auf Präzisierung drängt, um sog. „Fishing Expeditions“ zu vermeiden. Denn solche Fischzüge, bei denen US-Behörden Informationen sammeln, ohne den Sachverhalt hinreichend zu konkretisieren, sind offenbar recht häufig. Das Bundesamt beauftragt dann die Staatsanwaltschaft mit der Erhebung der begehrten Informationen im betroffenen deutschen Unternehmen, was als ein erster Filter für die Erforderlichkeit bei der Datenerhebung angesehen werden kann. Vor Herausgabe der Informationen an die ersuchende US-Behörde berücksichtigt das Bundesamt zumindest Gesichtspunkte des Kernbereichsschutzes mit Bezug zum Datenschutz (zweiter Filter).

In Hinblick auf die zweite Fallgruppe ist nach Mitteilung des Bundesamts für Justiz zwar nach § 14 Abs. 2 Ausführungsgesetz (AG) zum Haager Beweisaufnahmeübereinkommen (HBÜ) der Erlass einer Rechtsverordnung möglich, durch die Ausnahmen vom in Abs. 1 enthaltenen „Erledigungsverbot“ geregelt werden können. Eine solche Verordnung ist aber nicht zu erwarten. Anders als in der ersten Fallgruppe sind im Rechtshilfeverfahren, auf das ausländische Unternehmen verwiesen werden sollten, nicht das Bundesamt für Justiz zuständig, sondern die Landesjustizverwaltungen.

Die AG „Internationaler Datenverkehr“ hat sich auch mit dem Entwurf internationaler Wirtschaftsverbände von sog. **Alternativen Standardvertragsklauseln für die Auftragsdatenverarbeitung** befasst. Darin geht es primär um die Möglichkeit der Einbeziehung von Subunternehmern durch den Datenimporteur. Die AG hat hierzu die Auffassung vertreten, dass sichergestellt sein muss, dass der Subunternehmer die gleichen Pflichten erfüllt wie der Datenimporteur und dass die für den Datenexporteur zuständige Aufsichtsbehörde auch zur Überprüfung der Datenverarbeitung beim Subunternehmer befugt ist. Wir haben die deutsche Position zum Vertragsentwurf in die Art. 29-Datenschutzgruppe eingebracht.

Nachdem die AG „Internationaler Datenverkehr“ im letzten Jahr ein **Positionspapier** zu besonderen Fragestellungen beim internationalen Datenverkehr sowie eine **Handreichung zur rechtlichen Bewertung von Fallgruppen zur**

internationalen Auftragsdatenverarbeitung erarbeitet hatte[98], hat der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) hierzu ein „Echo" gegeben, das eine teilweise abweichende Beurteilung insbesondere bei Einschaltung von Subunternehmern beinhaltet. Die AG hat sich hiermit im Detail auseinandergesetzt und eine umfangreiche Erwiderung erarbeitet, die auch einige Missverständnisse ausräumt. Eine Änderung des Positionspapiers oder der Handreichung ist nicht beabsichtigt.

98 Dokumentenband 2007, S. 28 ff.

13. Organisation und Technik

13.1 Schadenerzeugender Code – Neue Entwicklungen

Früher herrschte die Meinung vor, dass jemand, der keine E-Mail-Anhänge ausführt, keine Hacker-, Crack- oder Schmuddelseiten besucht und seinen PC regelmäßig durch Updates auf den neuesten und sichersten Stand bringt, kaum einem Virenangriff ausgesetzt werden kann. Doch die Bedrohungen, welche von Viren, Trojanern, Spionageprogrammen und anderen schadhaften Codes ausgehen, sind oft nur noch einen Mausklick entfernt.

Die wohl folgenreichste Entwicklung betrifft die Motivation der Cyber-Kriminellen. Nicht mehr Ruhm und Ehre in der Hacker- oder Virenprogrammiererszene stehen heutzutage auf dem Spiel, sondern viel Geld. Es geht um die Gewinnung von persönlichen und vertraulichen Daten (z.B. Kontozugangsdaten), da sich damit viel Geld ergaunern lässt.

Eine weitere wesentliche Veränderung hat sich bei der Verbreitung der schadenerzeugenden Programme ergeben. Inzwischen werden die modernen Schädlinge hauptsächlich über gekaperte bzw. nachgemachte Internetauftritte oder verseuchte Banner verteilt, auf die man etwa bei Besuch oder Nutzung der Internet-Blockbuster wie Facebook, Google, MySpace, Wikipedia oder Youtube stoßen kann (sog. Drive-by-Download). Hierbei reicht unter Umständen der Besuch einer manipulierten Internetseite aus, damit schadhafter Code auf den Computer übertragen wird. Dabei werden zumeist Sicherheitslücken im Browser oder in Browser-Plug-ins ausgenutzt. Neu ist diese Bedrohung nicht, jedoch hat sie enorm zugenommen. Eine Fachzeitschrift schreibt, dass Google rund drei Millionen Drive-By-Download-Adressen in seinem Index gefunden hat[99]. Ein Angriff erfolgt in mehreren Stufen. Beim Besuch einer manipulierten Webseite wird ein Java-Script oder ActiveX-Programm ausgeführt, das eine Sicherheitslücke z.B. des Browsers ausnutzt. Anschließend erfolgt der Download eines Schadprogramms, das dann sein Unwesen (Herunterladen weiterer

99 Drive-by-Downloads: Infektion beim Surfen. In: Computer Magazin 6/2008, S. 82

Programme usw.) treibt. Aber auch die Lücken in anderen beliebten Programmen wie z.B. Reader oder Media Player, die sich auch in den Browser integrieren lassen, werden gerne ausgenutzt. Cyber-Kriminelle arbeiten ständig an einer Weiterentwicklung ihrer Schadprogramme, damit nicht nur die Verschleierung, sondern auch die Verbreitung verstärkt wird. Nach einer Studie des Computer-Bild-Sicherheitscenters spricht man von einer Zunahme schadhafter Codes im Zeitraum Mai bis September um 44 %. Symantec veröffentlichte im April eine Statistik, die Ende 2007 ca. 500.000 neue Bedrohungen aufweist. Inzwischen soll die Millionenmarke durchbrochen sein. Am häufigsten kommen weiterhin die Trojaner (Programme, die hauptsächlich der Spionage dienen) vor, die eine Steigerungsrate von 37 % aufweisen. Waren die Rootkits (Programme, die hauptsächlich der feindlichen Computerübernahme, z.B. für Denial-Of-Service-Angriffe zur Versendung von Spams oder Trojanern, dienen) bisher kaum anzutreffen, so wird in diesem Zeitraum eine Zunahme von 1.236 % verzeichnet.

Auf die Frage, wie man sich gegen diese neuen Entwicklungen schützen kann, lautet unsere Empfehlung wie schon seit Jahren, dass auf den aktuellen Status sämtlicher Soft- und Hardware ebenso geachtet werden sollte wie darauf, dass auf dem PC ein ständig aktualisiertes Schutzpaket aus Virenschutz, Anti-Spywaresoftware und Firewall installiert ist[100]. Daneben kann der Schutz durch alternative Browser mit Sicherheitserweiterungen, Deaktivierung von Javascript oder AktiveX oder durch Intrusion-Prevention-Technologien erweitert werden.

Schadsoftware stellt weiterhin eine bedeutende Bedrohung dar, die nach wie vor erhebliche Aufmerksamkeit erfordert. Der Aufwand wird jedoch dadurch honoriert, dass die Gefahr zwar nicht gebannt, aber zukünftig besser beherrschbar ist.

100 Unser Ratgeber zum Datenschutz 4: Computerviren & andere Softwareangriffe, http://www.datenschutz-berlin.de/content/veroeffentlichungen/ratgeber

13.2 Behördliche Datenschutzbeauftragte

13.2.1 Gesprächskreis der bezirklichen Datenschutzbeauftragten

Erneut trafen sich die Datenschutzbeauftragten der Bezirksämter zu mehreren Gesprächsrunden, um sich über Datenschutzfragen auszutauschen.

Aus dem Kreis der Teilnehmerinnen und Teilnehmer kam eine für die Praxis nützliche Initiative, eine Arbeitsgruppe unter unserer Beteiligung mit dem Ziel zu bilden, Handreichungen, Checklisten und Prüfhilfen für diejenigen Aufgaben zu erstellen, die den behördlichen Datenschutzbeauftragten vom Berliner Datenschutzgesetz vorgegeben werden. So wurden für die gesetzlich geforderte und von den behördlichen Datenschutzbeauftragten durchzuführende Vorabkontrolle allgemeine Hinweise, ein Ablaufplan und eine Checkliste entwickelt. Für die Dateibeschreibung nach § 19 Berliner Datenschutzgesetz (BlnDSG) wurde zu dem von der Senatsverwaltung für Inneres entwickelten Formular eine Anleitung zum Ausfüllen mit Erläuterungen erstellt. Auch für die vorgeschriebene Risikoanalyse, die vor dem Einsatz oder einer wesentlichen Änderung einer automatisierten Datenverarbeitung zu erstellen und Grundlage des erforderlichen Sicherheitskonzepts ist, entwickelte die Arbeitsgruppe für die verantwortliche Stelle eine Checkliste, die sich an den Bedrohungen und den in Frage kommenden Gegenmaßnahmen für die gesetzlichen Zielvorgaben (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz) orientiert. Die Checkliste ist für die Datenschutzbeauftragten gleichzeitig eine nützliche und die Arbeit erleichternde Hilfestellung bei der Überprüfung der angelieferten Risikoanalysen.

Die Papiere sollen eine möglichst standardisierte Vorgehensweise aller bezirklichen Datenschutzbeauftragten ermöglichen, auch mit dem Ziel, dass sie nicht eigene Prüflisten für hausinterne Prüfzwecke entwickeln müssen.

Unsere bereits in 2006[101] entwickelte Idee, in jeder Verwaltung behördliche Informationsfreiheitsbeauftragte einzuführen, deren Funktion von den behördlichen Datenschutzbeauftragten übernommen werden könnte, wurde eingehend diskutiert – nicht zuletzt, weil das Abgeordnetenhaus den Senat aufgefordert hat, er möge eine Prüfbitte auch an die Bezirksämter mit dem Ziel richten, dass die behördlichen Datenschutzbeauftragten zugleich die (koordinierende) Funktion eines Informationsfreiheitsbeauftragten wahrnehmen.[102]

Inzwischen hat sich mehrheitlich eine Vorgehensweise herauskristallisiert, die sich an unseren Vorschlägen orientiert. Danach werden behördliche Datenschutzbeauftragte als Koordinatoren für die Informationsfreiheit vorgesehen. Zusätzlich existieren innerhalb der meisten Bezirksämter Ansprechpersonen für die Belange der Informationsfreiheit in den einzelnen Fachämtern. Mit diesen Ansprechpersonen arbeiten die bezirklichen Datenschutzbeauftragten in ihrer Eigenschaft als Informationsfreiheitsbeauftragte zusammen. Die Anträge auf Informationszugang werden jedoch von den jeweils zuständigen Stellen bearbeitet. Die Informationsfreiheitsbeauftragten werden nur beratend tätig und sind erste Ansprechpersonen bei möglichen Zweifelsfragen, die mit uns zu klären sind. Daneben fertigen sie die jährlichen Statistiken über die im Bezirksamt eingereichten Anträge an.

Einzelne Bezirksdatenschutzbeauftragte beurteilen die Durchführung der Aufgabe anders. Sie meinen, das Amt der Informationsfreiheitsbeauftragten solle nicht mit dem der behördlichen Datenschutzbeauftragten verknüpft, sondern vielmehr beim Rechtsamt angesiedelt werden, da die Informationsfreiheit überwiegend Rechtsfragen aufwirft.

Ein Vorteil der Koordinatorenlösung[103] ist, dass man über die im Haus vorhandenen Anträge die Übersicht behält, was auch die Statistikführung vereinfacht. Konsens herrschte insofern, als die Aufgabe zur Vermeidung einer unterschiedlichen Anwendung des Informationsfreiheitsgesetzes in allen Bezirken bei einer bestimmten Stelle angesiedelt sein sollte; andernfalls würden womöglich

101 JB 2006, 11.3

102 Vgl. Anlage 1; zum Ergebnis der landesweiten Umfrage vgl. Abghs.-Drs. 16/2050

103 Sie wird auch vom Senat „grundsätzlich als sachgerecht angesehen und unterstützt", ebenso die Benennung der koordinierenden Person uns gegenüber; vgl. Abghs.-Drs. 16/2050.

unterschiedliche Rechtsauffassungen und Entscheidungen unnötigerweise für Verwirrung sorgen.

13.2.2 Workshop der Datenschutzbeauftragten der Gerichte

Auch mit den Datenschutzbeauftragten der Amtsgerichte findet mindestens zweimal im Jahr ein Gedankenaustausch statt, bei dem Datenschutzprobleme bei der ordentlichen Gerichtsbarkeit erörtert werden.

Im Amtsgericht Lichtenberg wurde geplant, für die Zugangskontrolle der Beschäftigten Geräte mit einem biometrischen Fingerabdruck-Erkennungssystem aufzustellen. Wir haben von diesem Vorhaben abgeraten, weil derartige Systeme technologiebedingt nicht fehlerfrei arbeiten. Die Geräte, die sich zurzeit auf dem Markt befinden, sind noch zu ungenau bzw. haben zu hohe Fehlerraten. Sie können nur dann als sicher angesehen werden, wenn zusätzlich ein maschinenlesbarer Ausweis oder die Eingabe eines Passworts verwendet wird[104].

Wenn biometrische Erkennungssysteme für die Zutrittskontrolle eingesetzt werden sollen, sind sie mit einem kausalen Authentisierungsmittel, wie z. B. einem maschinenlesbaren Ausweis oder einem Passwortverfahren, zu ergänzen, weil technologiebedingte Fehlerraten bei biometrischen Systemen unberechtigten Zugang oder unberechtigte Zurückweisung nicht ausschließen können.

Im Zusammenhang mit der elektronischen Aktenführung beim Handels-, Genossenschafts- und Vereinsregister ergab sich die Frage, was mit den ursprünglichen Papierdokumenten geschehen soll, die eingescannt wurden und nun nicht mehr gebraucht werden. Es handelt sich dabei um erhebliche Mengen, denn insbesondere beim Handelsregister werden sogar noch Unterlagen aus den 20er und 30er Jahren des 20. Jahrhunderts aufgehoben.

104 JB 2007, 2.4

Es gibt derzeit keine landesrechtliche Bestimmung, die eine Aufbewahrungsfrist für solche Dokumente vorsieht. Auch aus dem Berliner Datenschutzgesetz lassen sich keine Fristen herleiten. Maßgeblich ist in diesem Fall § 17 Abs. 3 BlnDSG, wonach personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Für Berlin liegt ein Entwurf für ein Schriftgutaufbewahrungsgesetz vor.[105] Danach dürfte im Justizbereich zwar weiterhin nach dem Grundsatz der Erforderlichkeit aufbewahrt werden. Die Justizverwaltung kann aber durchaus auch bestimmte Fristen vorgeben. Das Gesetz soll auch für öffentliche Register gelten.

13.3 Aktenfund bei einem Elektronik-Discounter

Aus der Praxis

Ein Aktenfund war besonders symptomatisch für den Umgang mit personenbezogenen Daten bei Discountern, die aufgrund ihres Geschäftsmodells einem strikten Sparzwang unterliegen und deshalb bei Anschaffungen für Maßnahmen des Datenschutzes, z. B. moderne Aktenvernichter, ungern Geld in die Hand nehmen. Ein Bürger hatte das Ordnungsamt auf Müllsäcke hingewiesen, die er auf dem Bahngelände hinter der Filiale eines Elektronik-Discounters entdeckt hatte. In den Säcken befanden sich Unterlagen mit Personenbezug aus dem Filialbereich, u. a Personaleinsatzplanungen, Warenwirtschafts- und Kassenunterlagen, Kontoauszüge, Garantieregistrierungen. Das Ordnungsamt leitete den Vorgang an die Polizei weiter, die wiederum uns einschaltete.

Bei unserem Kontrollbesuch fanden wir immer noch Unterlagen vor, die in aufgerissenen Säcken weit verstreut umherlagen. Bei dem anschließenden Gespräch mit dem Filialleiter führte dieser die „wilde Entsorgung“ auf Nach-

105 Entwurf eines Gesetzes zur Aufbewahrung von Schriftgut der Justiz des Landes Berlin (SchrAG), vgl. Abghs.-Drs. 16/1686

lässigkeiten bestimmter Mitarbeiter zurück. Nach seinen Worten hatten diese die Anweisung erhalten, angesammelte Unterlagen, die nicht mehr benötigt werden, in dem dafür vorhandenen Aktenvernichter zu entsorgen. Um sich die mühselige Arbeit zu ersparen, größere Mengen zu zerschnitzeln, wurden diese offensichtlich in Plastiksäcke verpackt und im Gestrüpp auf dem Bahngelände abgestellt. Wie wir feststellten, war der vorhandene Vernichter veraltet und entsprach nicht der vorgeschriebenen Stufe der Norm DIN 32757. Außerdem stellte sich heraus, dass nicht alle Beschäftigten auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz (BDSG) verpflichtet wurden.

Wir empfahlen dem Filialleiter, die Verpflichtungen umgehend nachzuholen und die restlichen Unterlagen auf dem Bahngelände zu beseitigen. Des Weiteren schlugen wir vor, Aktenvernichtungsgeräte, die der DIN-Norm entsprechen sollten, sukzessive in allen Räumen aufzustellen, in denen personenbezogene Daten verarbeitet werden.

Der von uns eingeschaltete Konzerndatenschutzbeauftragte wies auf eine Reihe sofort eingeleiteter Maßnahmen hin und versicherte, dass nunmehr die Verpflichtung auf das Datengeheimnis zusammen mit einer Belehrung unverzüglich umgesetzt worden sei. Die Filialleiter seien zudem angewiesen worden, ihre Beschäftigten über das Problem der Papierentsorgung zu unterrichten; außerdem sollen sie ihm (dem Konzerndatenschutzbeauftragten) künftig die Datenschutzverpflichtungen ihrer Beschäftigten zuleiten.

Unsere Empfehlung zum Einsatz veralteter Aktenvernichter soll konzernweit umgesetzt werden. Zusätzlich wurde mit einem Aktenentsorgungsunternehmen ein Entsorgungsvertrag für die Fälle geschlossen, bei denen besonders große Mengen Papiermaterial anfallen. Konzernweit wurden Organisationsanweisungen zum Umgang mit nicht mehr benötigten Unterlagen verteilt, und darüber hinaus war bis Ende des Jahres die Durchführung von Webschulungen für alle Filialleitungen geplant.

Es muss immer etwas passieren, was den Ruf und die Zuverlässigkeit eines Unternehmens in Frage stellt, bevor man an den sorgfältigen Umgang mit personenbezogenen Unterlagen denkt, die nicht mehr gebraucht werden. Da das Unternehmen erfreuliche Konsequenzen gezogen hat, verzichten wir an dieser Stelle darauf, seinen Namen zu nennen.

13.4 Die Abgabe gebrauchter Computer

Die Datenschutzfragen bei der Abgabe gebrauchter Computer an Dritte stellen sich immer, wenn ein gebrauchter Computer durch einen neuen ersetzt werden soll und der alte Computer noch gut genug ist, um anderen zu dienen, er also verschenkt oder verkauft wird. Eine ähnliche Situation ergibt sich, wenn ein Computer zur Reparatur gegeben werden muss.

13.4.1 Verschenken oder Verkaufen gebrauchter Computer

Durch das Internet sind wir auf die hilfreiche Aktion „Computer für bedürftige Menschen“ aufmerksam geworden. Der Berliner Verein repariert mit den Kursteilnehmenden ausrangierte und defekte Computer, die dann an gemeinnützige Organisationen und an Menschen verschenkt werden, die sich keinen Computer leisten können. So sehr wir solche Aktionen befürworten: Es müssen bestimmte Maßnahmen getroffen werden, um nicht in eine Datenschutzfalle zu geraten. Denn wer möchte schon „seinen Computer und alle darauf gespeicherten Daten“ verschenken?

Dabei reicht es nicht aus, mit den Systembefehlen des Betriebssystems alle Dateien mit persönlichen Daten, die installierte Software, den elektronischen Papierkorb, Cookies, temporäre Daten usw. zu löschen oder gar die Festplatte zu formatieren. Dass dies ausreicht, ist leider ein verbreiteter Irrtum, denn grundsätzlich reichen Löschaktionen bzw. Formatierungen mit den Systembefehlen des Betriebssystems nicht aus, um die Daten ein für alle Mal unschädlich zu machen. Es gibt nämlich frei verfügbare Tools, die eine Wiederherstellung derart gelöschter Dateien ermöglichen. Für den Fall, dass eine versehentlich gelöschte Datei gerettet werden soll, ist dies zwar durchaus positiv.

Werden jedoch die Daten einer verkauften „fremden“ Festplatte mit sensiblen personenbezogenen Daten wiederhergestellt, so ist dem Missbrauch dieser Daten Tür und Tor geöffnet. Es gibt grundsätzlich zwei Maßnahmen für das sichere Löschen:

1. Das mehrfache Überschreiben mit Zufallszahlen hilft selbst gegen ausführliche Analysen in Speziallaboren[106]. Hier kann von einer datenschutzgerechten Löschung gesprochen werden. Wir haben dies auch dem Verein empfohlen, der die dafür notwendigen Löschtools kostenlos im Internet finden kann[107]. Der Verein teilte uns mit, dass er entsprechend verfahren wird.
2. Sofern die Festplatte defekt ist oder das oben beschriebene Löschen zu aufwändig erscheint oder wenn die Daten so schutzwürdig sind, dass an der ausreichenden Wirkung der Löschtools Zweifel bestehen, gibt es die Möglichkeit, die Festplatte physisch zu zerstören und damit unbrauchbar zu machen.

Wer ältere bzw. benutzte Computer verkauft, verschenkt oder entsorgt, sollte die auf der Festplatte gespeicherten Daten durch mehrfaches Überschreiben datenschutzgerecht löschen. Tools sind im Internet frei verfügbar.

13.4.2 Computer in der Reparatur

Unverhofft kommt oft! Nichts geht mehr. Der Computer muss zur Reparatur gebracht werden. Was sollte dabei vorher beachtet werden?

Aus dem Schneider sind alle, die grundsätzlich vertrauliche (ob personenbezogene oder anderweitig schutzbedürftige) Daten ohnehin verschlüsselt gespeichert haben. Die benötigte Software, die allen aktuellen Ansprüchen genügt, ist im Internet sogar frei verfügbar. Die Datensicherung sollte regelmäßig durchgeführt und an einem sicheren – nur für Befugte zugreifbaren – Ort aufbewahrt werden. Dies hilft dabei, die Benutzung mit einem anderen verfügbaren Computer fortzusetzen. Sofern es noch möglich ist, die Festplatte vor der Abgabe des Rechners zur Reparatur zu formatieren oder gar wie beschrieben[108] zu löschen, kann auch in solchen Fällen die Arbeit an einem anderen Computer

106 Vgl. Faltblatt der LDA Brandenburg: Verräterische Spuren auf Festplatten – Hinweise zum sicheren Löschen von Daten
107 Wir empfehlen eine Internetsuche, z.B. mit den Stichwörtern Eraser, Shredder oder Wipe.
108 Vgl. 13.4.1

fortgesetzt werden. Die Reparatur selbst sollte, wenn möglich, vor Ort und unter Aufsicht durchgeführt werden. Diese Möglichkeit besteht zwar hauptsächlich bei größeren betrieblichen IT-Infrastrukturen, aber selbst für private Computer-Nutzende gibt es Reparaturdienste, die Hausbesuche machen.

Muss der Computer jedoch zum Händler gebracht werden, ist Folgendes zu beachten: Grundsätzlich sollte das Serviceunternehmen auf seine Verschwiegenheitspflicht hingewiesen und ggf. die Allgemeinen Geschäftsbedingungen daraufhin geprüft werden. Ansonsten sollte ein Passus in den Reparaturauftrag aufgenommen werden, der das Unternehmen zur Verschwiegenheit verpflichtet. Die sensiblen Daten oder die komplette Festplatte sollten vor der Reparatur gesichert werden (Backup, Image oder einfache Kopie der Dateien). Das ist natürlich nur möglich, wenn auf die Festplatte noch zugegriffen werden kann. Im Anschluss sollten zumindest die sensitiven Daten gelöscht werden (Vorsicht: Auch temporäre Daten, Datensicherungsdateien, Cookies, Caches, Links usw. können sensitive Daten enthalten). Hierzu empfehlen wir die erwähnte datenschutzgerechte Löschung[109], bei der zumindest die Daten mehrfach überschrieben werden. Besser ist natürlich, wenn die komplette Festplatte datenschutzgerecht gelöscht wird. Sollte sie derartige Defekte aufweisen, dass sie ausgetauscht werden muss, sollte vorher schriftlich vereinbart werden, dass sie datenschutzgerecht entsorgt oder der Besitzerin bzw. dem Besitzer des Computers zurückgegeben wird.

Bei der Herausgabe eines Computers zur Reparatur müssen hinreichende Maßnahmen ergriffen werden, um sich gegen den Missbrauch der Daten abzusichern. Das Spektrum der Maßnahmen reicht vom Vertrauen auf die Einhaltung schriftlich fixierter Garantien bis zum vorherigen Ausbau der Festplatte bzw. ihrer physischen Zerstörung.

109 Vgl. Fußnote 106

14. Telekommunikation und Medien

14.1 Europäische Union: Novellierung der Telekommunikations-Datenschutzrichtlinie

Die Überarbeitung des Regulierungsrahmens für elektronische Kommunikationsnetze und -dienste in der Europäischen Union ist weiter vorangeschritten. Über Vorarbeiten der Europäischen Kommission hatten wir bereits im Jahr 2006 berichtet[110]. Sie hat im November 2007 einen Vorschlag zur Änderung der Telekommunikations-Datenschutzrichtlinie 2002/58/EG vorgelegt[111]. Er verpflichtet die Diensteanbieter, die betroffenen Teilnehmer und die nationale Regulierungsbehörde unverzüglich über Sicherheitsverletzungen zu benachrichtigen, die zu Zerstörung, Verlust, Veränderung, unbefugter Weitergabe oder unberechtigtem Zugang zu personenbezogenen Daten bei der Bereitstellung öffentlich zugänglicher Kommunikationsdienste führen. Das Europäische Parlament möchte den Vorschlag dahingehend ändern, dass die Regulierungsbehörden zwar regelmäßig, die Betroffenen aber nur noch in Ausnahmefällen benachrichtigt werden[112]. Der Gemeinsame Standpunkt des Rates sieht demgegenüber zwar eine parallele Benachrichtigung von Betroffenen und Aufsichtsbehörde vor, beschränkt sie aber auf Sicherheitsvorfälle, die die Privatsphäre der Nutzer in ernsthafter Weise gefährden[113]. Wann dies der Fall ist, soll die nationale Aufsichtsbehörde bestimmen können.

Im Europäischen Parlament hatte der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) eine weit reichende Änderung vorgeschlagen, die es „jeder natürlichen oder juristischen Person" ermöglicht, Verkehrsdaten zum Zweck der Gewährleistung von Datensicherheit zu verarbeiten[114]. Der Rat will solche Befugnisse auf die von der Richtlinie betroffenen Anbieter

110 JB 2006, 10.1.1.

111 KOM (2007) 698 endg. vom 13. November 2007

112 Legislative Entschließung des Europäischen Parlaments T6-0452/2008 vom 24. September 2008, Abänderungen 187/REV, 184, 124/125

113 Ratsdokument 15899/08 vom 20. November 2008, S. 9 f.

114 Bericht des federführenden Ausschusses für Binnenmarkt und Verbraucherschutz A6-0318/2008 vom 18. Juli 2008, S. 90, amendment 130

und auf das unbedingt notwendige Maß beschränken[115]. Die Vorschläge des LIBE-Ausschusses sind das Ergebnis intensiver Lobbyarbeit der Softwareindustrie. So hatte sich die Business Software Alliance (BSA), ein Interessenverband von Softwareherstellern, sowohl für eine weit reichende Befugnis für jedermann zur Verarbeitung personenbezogener Daten zu Sicherheitszwecken stark gemacht als auch für eine Beschränkung der Definition personenbezogener Daten in der Telekommunikations-Datenschutzrichtlinie.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im November[116] entschieden gegen die Aufnahme von generellen Ermächtigungen zur Verarbeitung von Verkehrsdaten zur Gewährleistung der Sicherheit durch beliebige natürliche oder juristische Personen ausgesprochen und die Bundesregierung aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat die Zustimmung zu verweigern.

Bereits im Mai hatte die Art. 29-Datenschutzgruppe im Überprüfungsverfahren der Richtlinie 2002/58/EG Stellung genommen[117]. Darin unterstützt sie die von der Kommission vorgeschlagenen Regelungen zur Information der Betroffenen über Sicherheitsvorfälle und empfiehlt, diese Pflichten auch auf Anbieter von Diensten der Informationsgesellschaft im Allgemeinen auszuweiten. Die nationalen Regulierungsbehörden sollen im öffentlichen Interesse unter bestimmten Umständen ermächtigt werden, die Öffentlichkeit über eine Sicherheitsverletzung in Kenntnis zu setzen oder die betroffenen Unternehmen zu verpflichten, dies zu tun.

Nachdrücklich wendet sich die Art. 29-Datenschutzgruppe gegen jede Einschränkung des Begriffs „personenbezogene Daten“ in der Datenschutzrichtlinie für elektronische Kommunikation und weist darauf hin, dass dadurch eine Lücke beim Schutz natürlicher Personen in einem Kernbereich der elektronischen Kommunikation entstünde (und in der Folge auch bei Diensten der Informationsgesellschaft und des E-Government, die auf elektronischen

115 Ratsdokument 15899/08, S. 14

116 Entschließung der 76. Konferenz, vgl. Dokumentenband 2008, S. 28

117 Stellungnahme 2/2008 vom 15. Mai 2008 zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), WP 150

Diensten basieren), was aus Sicht des Datenschutzes inakzeptabel wäre. Schließlich spricht sich die Gruppe für die Anwendung des Prinzips der Datenvermeidung und den Einsatz datenschutzfreundlicher Technologien durch die für die Datenverarbeitung Verantwortlichen aus und fordert den europäischen Gesetzgeber auf, dieses Prinzip in der Richtlinie stärker hervorzuheben.

Auch zu Datensicherheitszwecken dürfen Daten nur im Rahmen des unbedingt Erforderlichen verarbeitet werden. Nur Anbieter dürfen entsprechende Befugnisse zur Sicherung ihrer eigenen informationstechnischen Systeme erhalten. Inakzeptabel wären eine Blankettbefugnis für jedermann oder eine Beschränkung des Begriffs „personenbezogene Daten" in der Richtlinie.

14.2 Datenschutz und Urheberrecht

Am 1. September ist das „Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums[118] in Kraft getreten. Damit werden Rechteinhabern erstmals Auskunftsansprüche gegen Anbieter von Telekommunikationsdiensten unter Verwendung von Verkehrsdaten für deren private Rechtsverfolgung eingeräumt. Nach dem neu gefassten § 101 Abs. 9 Urheberrechtsgesetz (UrhG) ist vor Erteilung solcher Auskünfte eine richterliche Anordnung erforderlich, deren Kosten der Verletzte trägt. Voraussetzung für die Anordnung ist, dass eine widerrechtliche Verletzung des Urheberrechts im gewerblichen Ausmaß vorliegt. Dieses kann sich sowohl aus der Anzahl der Rechtsverletzungen als auch der Schwere der Rechtsverletzung ergeben[119]. Die sog. „Vorratsdaten"[120] dürfen für die Erteilung solcher Auskünfte auch weiterhin nicht genutzt werden[121].

Bei Vorliegen der gesetzlichen Voraussetzungen können nun die personenbezogenen Daten zu IP-Adressen an die Rechteinhaber zur Durchsetzung von Schadensersatzansprüchen mitgeteilt werden. Offen ist, welche Praxis sich

118 BGBl. I, S. 1191

119 § 101 Abs. 1 UrhG

120 Vgl. dazu 6.1

121 Vgl. Pressemitteilung des Bundesministeriums der Justiz vom 29. August 2008: Gesetz zum Schutz des geistigen Eigentums tritt in Kraft

in der Rechtsprechung bei der Auslegung der neuen Vorschriften durchsetzen wird. Gegenwärtig setzen Gerichte die Hürden für die Erteilung einer richterlichen Anordnung unterschiedlich hoch, weil sie die Frage, wann eine Verletzung des Urheberrechts im gewerblichen Ausmaß vorliegt, uneinheitlich beurteilen.

14.3 Bewertungsportale im Internet

Aus der Praxis

Ein Verein betreibt eine Plattform im Internet, auf der Lehrveranstaltungen von Professorinnen und Professoren an deutschen, österreichischen und schweizerischen Hochschulen bewertet werden können. Darüber hatten sich zahlreiche Betroffene bei uns beschwert.

Über dieses Angebot und unsere datenschutzrechtliche Bewertung hatten wir bereits 2007 berichtet[122]. Nachdem wir vergeblich versucht hatten, den Verein zu einer rechtskonformen Umgestaltung seines Angebots zu bewegen, haben wir nun Bußgelder gegen ihn verhängt: Er unterlässt bisher die vorgeschriebene Benachrichtigung der betroffenen Dozentinnen und Dozenten und lässt sich nicht das berechtigte Interesse derjenigen darlegen, die Daten aus dem Internet-Angebot abrufen. Auch eine zumindest stichprobenhafte Prüfung, ob ein berechtigtes Interesse überhaupt vorliegt, erfolgt nicht. Der Anbieter hat gegen den Bußgeldbescheid Einspruch eingelegt. Die Entscheidung des Amtsgerichts bleibt abzuwarten. Wir prüfen derzeit weitere aufsichtsbehördliche Maßnahmen.

Die obersten Aufsichtsbehörden für den Datenschutz in der Wirtschaft haben zur Problematik von Internet-Portalen zur Bewertung von Einzelpersonen Stellung genommen und darauf hingewiesen, dass es sich bei Beurteilungen in Internet-Portalen häufig um sensitive Informationen und subjektive Werturteile über die Betroffenen handelt, ohne dass die Urheber erkennbar sind. Die Aufsichtsbehörden stimmen darin überein, dass die Anbieter solcher Portale die gesetzlichen Bestimmungen über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten haben. Bei der vorgeschriebenen Rechts-

122 JB 2007, 12.2.3

güterabwägung ist den schutzwürdigen Interessen der bewerteten Person Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen[123].

Die Veröffentlichung personenbezogener Daten in Bewertungsportalen im Internet ist nur zulässig, wenn die Regelungen des Bundesdatenschutzgesetzes zur geschäftsmäßigen Datenverarbeitung eingehalten werden, sofern die Betroffenen nicht eingewilligt haben.

14.4 Private Nutzung von Internet und E-Mail in der Verwaltung

In einem Schreiben an den Vorsitzenden des IT-Koordinierungsgremiums der Berliner Verwaltung problematisierte der Rechnungshof von Berlin die nach seiner Auffassung ausufernde Nutzung dienstlicher Internetanschlüsse für private Informationsgewinnung und dienstlicher E-Mail-Accounts für den Empfang und die Versendung privater Nachrichten. Der Rechnungshof beklagte, dass es zu diesen Fragen keine eindeutige Regelung im Lande gebe. Einerseits gebe es eine verbindliche Untersagung in den IT-Standards der Berliner Verwaltung, bei der es sich um eine Verwaltungsvorschrift handelt. Andererseits gebe es nur eine grundsätzliche Untersagung in einer Rahmendienstvereinbarung zwischen dem Senat und dem Hauptpersonalrat des Landes, was so zu interpretieren sei, dass Ausnahmeregelungen denkbar sind.

Der Unterausschuss „Datenschutz und Informationsfreiheit“ des Abgeordnetenhauses bat uns zu ermitteln, wie die Situation beim Bund und in den anderen Bundesländern ist. Bei der Umfrage stellte sich heraus, dass der Bund und die meisten Bundesländer kein generelles Verbot der privaten Internet-Nutzung dienstlicher Anschlüsse vorsehen und stattdessen gewisse Ausnahmen für eine geringfügige private Nutzung des Internets zulassen. Eine private Nutzung dienstlicher E-Mail-Accounts wird allerdings restriktiver gesehen, weil im

123 Beschluss vom 17./18. April 2008, vgl. Dokumentenband 2008, S. 35

Rahmen der geringfügigen privaten Nutzung des Internets die Verwendung privater Webmail-Accounts ermöglicht wird, um private Nachrichten abzusetzen. Einige wenige Bundesländer weichen davon ab und sehen ein Verbot der privaten Nutzung des Internets vor.

Der Staatssekretär der Senatsverwaltung für Inneres beklagte, dass in dem Schreiben des Rechnungshofs die Beschäftigten des Landes Berlin dem Verdacht ausgesetzt werden, das Internet im Dienst zu überwiegend privaten Zwecken zu nutzen, und bezweifelte die methodische Herangehensweise des Rechnungshofs, die zu einer verzerrten Darstellung der privaten Nutzung des Internets führte. Er bat uns um unsere Einschätzung.

Da der Vorgang das Verhältnis der beiden unabhängigen Kontrollbehörden des Landes miteinander berührt, haben wir zunächst mit dem Rechnungshof Kontakt aufgenommen. Es stellte sich heraus, dass der Rechnungshof selbst in dem Schreiben kein Prüfergebnis, sondern die Ergebnisse seiner Untersuchungen eher als einen Hinweis auf Tendenzen sieht. Mehr Bedeutung hatte für den Rechnungshof die Tatsache, dass es im Land zwei „konkurrierende" Regelungen gibt.

Sie unterscheiden sich in Bezug auf die Verbindlichkeit. Da eine Rahmendienstvereinbarung eine untergesetzliche Rechtsvorschrift mit Vorrang gegenüber Verwaltungsvorschriften ist, teilen wir die Einschätzung der Senatsverwaltung für Inneres, dass die konsequente Anwendung und Umsetzung der Internet-Rahmendienstvereinbarung die einzig verbindliche Handlungsgrundlage bei missbräuchlicher Nutzung des Internets durch Beschäftigte bildet. Jedoch haben wir uns dem Wunsch des Rechnungshofs angeschlossen, dass der Unterschied zwischen den IT-Standards und der Rahmendienstvereinbarung beseitigt werden sollte. Wir hielten dabei die Anpassung der Regelungen in den IT-Standards an die der Rahmendienstvereinbarung bei der Festlegung der neuen IT-Standards für eine geeignete Lösung.

Bei der Diskussion um die IT-Standards 2009 kam der Einwand, dass bei einer Erlaubnis der ausnahmsweisen und zeitlich beschränkten privaten Nutzung das ITDZ bzw. die dies gestattenden Behörden in die Rolle eines E-Mail- bzw. Internet-Providers geraten würden, was zur Vorratsdatenspeicherung und Bereithaltung von Schnittstellen für die Sicherheitsbehörden verpflichten

würde. Diese Befürchtung ist jedoch unbegründet. Die in § 113 a Telekommunikationsgesetz (TKG) enthaltenen Speicherungspflichten richten sich an Anbieter „öffentlich zugänglicher Telekommunikationsdienste für Endnutzer". Ausweislich der amtlichen Begründung[124] besteht für den „nicht öffentlichen" Bereich, also für Anbieter, die ihre Dienste nicht für die Öffentlichkeit erbringen, keine Speicherungspflicht. Die amtliche Begründung nennt in einer beispielhaften Aufzählung unternehmensinterne Netze, Nebenstellenanlagen und E-Mail-Server von Universitäten „ausschließlich für dort immatrikulierte Studierende oder Bedienstete". Eine Verpflichtung zur Speicherung von Daten nach § 113 a TKG besteht jedenfalls für öffentliche Stellen des Landes Berlin nicht, die ihren Beschäftigten (und nur diesen) entsprechende Einrichtungen zur Verfügung stellen. Unbeachtlich ist dabei, ob eine private Nutzung dieser dienstlich zur Verfügung gestellten Einrichtungen gestattet ist oder nicht. Auch das ITDZ bietet keine öffentlichen Telekommunikationsdienste für Endnutzer an und unterliegt insofern auch nicht den Speicherungsverpflichtungen aus § 113 a TKG. Die Vorschriften der Telekommunikations-Überwachungsverordnung (TKÜV) gelten ebenfalls nur für Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden.

Im Ergebnis wurde der strittige Passus aus den IT-Standards 2009 ganz gestrichen, so dass nun eindeutig die Regelung der Rahmendienstvereinbarung gilt.

Ein striktes Verbot der privaten Nutzung dienstlicher Internetanschlüsse zur Gewinnung von Informationen aus dem World Wide Web ist kaum durchzusetzen und zu kontrollieren und kann die Beschäftigten unter Umständen in Konflikte bringen, wenn sie bei wichtigen privaten Anliegen wegen des Verbots nicht legal handeln können. Die Rahmendienstvereinbarung sieht allerdings Maßnahmen vor, um beim Verdacht extensiver privater Nutzung einschreiten zu können.

124 BR-Drs. 275/07, S. 161

14.5 PrivacyBox

Der Verein German Privacy Foundation e.V. hat den Online-Dienst „PrivacyBox“ in einer gemeinsamen Pressevorführung mit uns vorgestellt. Er ermöglicht Personen oder Organisationen, insbesondere Journalistinnen und Journalisten, eine anonyme vorratsdatenfreie Kontaktmöglichkeit zur Verfügung zu stellen. Dazu legen sich die interessierten Personen unter einem Pseudonym auf privacybox.de Postfächer an, die entweder über ein E-Mail-Programm abgerufen werden können oder eingehende Nachrichten verschlüsselt an gewählte E-Mail-Adressen weiterleiten. Nachrichten senden die Informanten anonym über ein Webformular an das gewählte Pseudonym, wobei die Nachrichten nur verschlüsselt übertragen und gespeichert werden. Das Pseudonym kann z. B. im Impressum der jeweiligen Zeitschrift veröffentlicht werden.

Ziel dieses Online-Dienstes ist es, trotz der ab Januar 2009 verpflichtenden, aber zumindest teilweise verfassungswidrigen Vorratsdatenspeicherung[125] Publizierende und insbesondere ihre Informanten schützen zu können. Zur Sicherstellung der Anonymität wird den Informanten außerdem die Verwendung von Anonymisierungsdiensten[126] für den Zugriff auf die Webseite der PrivacyBox empfohlen, auch wenn der Verein für 2009 zusichert, keine personenbezogenen Verkehrsdaten wie die IP-Adressen zu speichern.

125 Vgl. 6.1
126 JB 2007, 2.2

15. Informationsfreiheit

15.1 Entwicklungen für und gegen mehr Transparenz

Der Ministerausschuss des Europarats hat am 28. November den **Entwurf einer Konvention über den Zugang zu amtlichen Dokumenten**[127] beschlossen. Damit ist erstmals weltweit ein völkerrechtlich verbindlicher Vertrag zur Informationsfreiheit auf den Weg gebracht worden. Nach Inkrafttreten sind alle Vertragsstaaten verpflichtet, jedem Menschen ein allgemeines Recht auf gebührenfreien Zugang zu Behördeninformationen einzuräumen, ohne dass dies begründet werden muss. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) hat auf eine schnelle Ratifizierung durch den Bundestag gedrungen und die wenigen Bundesländer ohne Informationsfreiheitsgesetze[128] aufgefordert, ihre Haltung zu revidieren.[129]

Die Europäische Kommission hat Vorschläge zur Änderung der Verordnung 1049/2001[130] über den freien Zugang zu Dokumenten der Europäischen Union (**„EU-Transparenz-Verordnung“**) vorgelegt. Marginalen Verbesserungen stehen dabei massive Einschränkungen der Informationsfreiheit gegenüber. So wird der Zugang zu EU-Dokumenten davon abhängig gemacht, ob sie vorher übermittelt oder registriert worden sind. Informationen sollen auch nach Verfahrensabschluss selbst dann zurückgehalten werden, wenn an ihrer Offenlegung ein überwiegendes öffentliches Interesse besteht. Es steht zu befürchten, dass damit das Handeln der EU, das in der Öffentlichkeit ohnehin als wenig transparent gilt, noch undurchschaubarer wird. Deshalb hat die IFK in einer Entschließung an das Europäische Parlament und den Rat appelliert, den Vorschlägen der Kommission nicht zu folgen und stattdessen das Transparenzniveau

127 Englische Fassung abrufbar unter www.datenschutz-berlin.de/content/informationsfreiheit/europa-international.

128 Dies sind Baden-Württemberg, Bayern, Hessen, Niedersachsen und Sachsen.

129 Entschließung vom 4. Dezember 2008: Die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich unterzeichnen und ratifizieren!, vgl. Dokumentenband 2008, S. 149

130 ABl. L 145 vom 31. Mai 2001, S. 43; JB 2007, 13.1

bei den EU-Institutionen deutlich zu erhöhen.[131] Dass ein solcher Appell überhaupt erforderlich wurde, verwundert insbesondere deshalb, weil die Überprüfung der EU-Transparenz-Verordnung im Jahre 2007 als Teil der „Europäischen Transparenzinitiative" gestartet worden war.[132]

Immerhin führte diese Initiative dazu, dass die Europäische Kommission die **Empfänger von EU-Subventionen** im Internet veröffentlicht. Sie hat eine Datenbank mit detaillierten Angaben zur Verteilung der vergebenen Fördermittel angelegt.[133] Die Daten werden von den EU-Mitgliedstaaten aufgeliefert mit Ausnahme derjenigen über die Agrarsubventionen. Hierzu hat die Bundesanstalt für Landwirtschaft und Ernährung eine eigene Datenbank eingerichtet[134], um der Verpflichtung nach dem neuen Agrar- und Fischereifonds-Informationen-Gesetz (AFIG) nachzukommen.[135] Die Informationen umfassen die Namen der Empfänger von Mitteln und deren Höhe.

Ebenfalls im Rahmen der „Europäischen Transparenzinitiative" hat die Europäische Kommission ein sog. **Register der Interessenvertreter (Lobbyistenregister)**[136] eingeführt. Damit wird die Öffentlichkeit darüber informiert, wer die EU-Institutionen bei der Entscheidungsfindung beeinflusst. Die Eintragung in das Register ist freiwillig. Ist sie erfolgt, müssen die Interessenvertreterinnen und -vertreter aber einen Verhaltenskodex befolgen. Ein Verstoß kann zur vorübergehenden Streichung oder zum endgültigen Ausschluss aus dem Register führen. Mittlerweile sind mehr als 800 Lobbyisten angemeldet.

Auch die Bundesregierung hat sich entschlossen, die **Einflussnahme Externer auf die Entscheidungen der Verwaltung** transparent zu machen. Sie hat daher am 18. Juni die Allgemeine Verwaltungsvorschrift zum Einsatz von außerhalb des öffentlichen Dienstes Beschäftigten (externen Personen) in der Bundesverwaltung beschlossen, die den vorübergehenden Einsatz externer Personen

131 Entschließung vom 30. Juni 2008: Die Europäische Union braucht nicht weniger, sondern mehr Transparenz, vgl. Dokumentenband 2008, S. 148

132 JB 2007, 13.1

133 http://ec.europa.eu/grants/beneficiaries_de.htm

134 http://www.agrar-fischerei-zahlungen.de/afig/

135 AFIG vom 26. November 2008, BGBl. I, S. 2330

136 https://webgate.ec.europa.eu/transparency/regrin/welcome.do

in der Bundesverwaltung im Interesse des Vertrauens in die Integrität und die Funktionsfähigkeit der Verwaltung einheitlich und verbindlich regelt. Entsprechend der Verwaltungsvorschrift, die dem Bundesministerium des Innern (BMI) eine regelmäßige (jährliche) Berichtspflicht gegenüber dem Haushalts- und dem Innenausschuss auferlegt, hat das BMI bereits im September einen ersten Bericht vorgelegt.[137] Leider hat die Bundesverwaltung weder die Verwaltungsvorschriften noch den Bericht[138] veröffentlicht. Mehr **Transparenz bei Lobbyisten** ist als vertrauensbildende Maßnahme nicht nur auf EU- und Bundes-, sondern auch auf Landesebene wünschenswert.

Das Informationsbedürfnis der Öffentlichkeit ist naturgemäß am größten, wenn es um den Einsatz öffentlicher Mittel geht, die auf gesetzlicher Grundlage (als Steuer oder Beitrag) erhoben werden. Deshalb hat das Bundesverfassungsgericht entschieden, dass die gesetzliche Pflicht der Krankenkassen, die Höhe der jährlichen **Vergütung ihrer Vorstandsmitglieder** im Bundesanzeiger und in ihrer Mitgliederzeitschrift zu veröffentlichen[139], verfassungsgemäß ist.[140] Da die Informationen nicht die engere Privatsphäre der Beschwerdeführer (Vorstandsmitglieder einer gesetzlichen Krankenversicherung), sondern ihren beruflichen Bereich betrafen, war das Interesse der Beitragszahlenden und der Öffentlichkeit höher zu bewerten als das Interesse der Beschwerdeführer an der Geheimhaltung ihrer Vergütungen als Vorstandsmitglieder.

Am 1. Mai ist das Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformationen (Verbraucherinformationsgesetz – VIG) in Kraft getreten[141], nachdem es nach dem Veto des Bundespräsidenten nachgebessert worden war[142]. Hierzu hat das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz eine bürgerfreundliche Informationsbroschüre veröffent-

137 Erster Bericht über den Einsatz externen Personen in der Bundesverwaltung vom 22. September 2008 (Berichtszeitraum: 1. Januar bis 31. August 2008)

138 Zur Begründung vgl. Antwort des Staatssekretärs Dr. Beus auf die Frage des Abgeordneten Volker Beck. In: BT-Drs. 16/10520, S. 3 f. Der Bericht ist abrufbar unter www.spiegel.de/media/0,4906,19010,00.pdf.

139 § 35 a Abs. 6 S. 2 SGB IV

140 Beschluss vom 25. Februar 2008 – 1 BvR 3255/07

141 Artikel 1 des Gesetzes zur Neuregelung des Rechts der Verbraucherinformationen vom 5. November 2007, BGBl. I, S. 2558

142 JB 2006, 11.1

licht[143], die den Weg zu gewünschten Informationen beschreibt. Zur Umsetzung des Gesetzes im Land Berlin hat die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz ein Rundschreiben herausgegeben[144]. Obwohl es sowohl Aussagen zur Informationsfreiheit als auch zum Datenschutz enthält, wurden wir bei der Erstellung nicht beteiligt und erst auf Nachfrage in Kenntnis gesetzt. Bemerkenswert ist, dass das Verhältnis des Landesgesetzes von 2003[145] zum neuen Bundesgesetz nicht erwähnt wird.

Die IFK hat für den Bereich der Finanzverwaltung eine Entschließung für mehr Transparenz gefasst[146], nachdem das Bundesverfassungsgericht den Anspruch auf Informationen aus der eigenen Steuerakte für verfassungsrechtlich geboten erklärt hat[147]. Denn nichts anderes kann für die Anwendung der Informationsfreiheitsgesetze (IFG) gelten, die jedem Menschen einen Anspruch auf Zugang zu Informationen bei Behörden sichern. Die Finanzverwaltungen müssen auch diese Gesetze beachten.

Erfreulich ist, dass mit Sachsen-Anhalt[148] und Rheinland-Pfalz[149] nunmehr elf Bundesländer über ein Informationsfreiheitsgesetz verfügen, wobei auch Rheinland-Pfalz (wie derzeit noch Hamburg und Thüringen) keinen Informationsfreiheitsbeauftragten vorsieht.

143 www.bmelv.de →Service→Publikationen

144 Rundschreiben GesUmV-IV-1/2008 zur Umsetzung des Gesetzes zur Neuregelung des Rechts der Verbraucherinformation im Land Berlin vom 11. September 2008

145 Gesetz zur Information der Verbraucherinnen und Verbraucher im Lebensmittelverkehr im Land Berlin vom 15. Mai 2003, GVBl. S. 174

146 Entschließung vom 11. Juni 2008: Transparenz in der Finanzverwaltung, vgl. Dokumentenband 2008, S. 147

147 Beschluss vom 10. März 2008 – 1 BvR 2388/03

148 Informationszugangsgesetz Sachsen-Anhalt (IZG LSA) vom 19. Juni 2008, GVBl. LSA S.242

149 Landesgesetz zur Einführung des Rechts auf Informationszugang vom 26. November 2008, GVBl. Rhl-Pf S. 296

15.2 Informationsfreiheit in Berlin

15.2.1 Allgemeine Entwicklungen

Mit Freude kann vom Ende einer fast unendlichen Geschichte berichtet werden: Unsere mehr als vierjährigen Bemühungen um eine bürger- und behördenfreundlichere Gebührenregelung für Amtshandlungen nach dem Berliner Informationsfreiheitsgesetz (Tarifstelle 1004) waren erfolgreich. Zu den wesentlichen Änderungen gehören die Einführung einer Gebührenstaffel und die Herabsetzung der Gebühr für eine Kopie auf 15 Cent.[150] Wir haben die Berliner Verwaltung mit einem Rundschreiben auf diese informationszugangsfreundliche Neuerung hingewiesen. Um den Vorgaben des neuen Verbraucherinformationsgesetzes Rechnung zu tragen, wurde die Tarifstelle 1004 kurz darauf erneut geändert[151]. Danach ist der Zugang zu Informationen über Verstöße gegen dieses Gesetz gebührenfrei. Zu begrüßen ist, dass die neue Gebührenregelung einheitlich für das IFG sowie für Umwelt- und Verbraucherinformationen gilt, was bundesweit bislang einmalig ist.

Ebenfalls zu begrüßen ist die zweite umfangreiche Evaluation zur Anwendung des IFG, die es seit Inkrafttreten gegeben hat[152]. Sie umfasst eine Aufstellung der Anfragen und Bescheide der Berliner Verwaltung von 2005 bis 2008. [153] Auch wir haben dazu Zahlen geliefert, insbesondere über unsere Kontrolltätigkeit in Bezug auf einzelne Verwaltungen.

Schließlich befürworten wir die neue Pflicht der Senatsmitglieder, dem Abgeordnetenhaus über alle Nebenbeschäftigungen mit erzielten Vergütungen zu berichten[154]. Allerdings ist unverständlich, warum dies nicht auch für Staatssekretärinnen und Staatssekretäre gelten soll.

150 26. Verordnung zur Änderung der Verwaltungsgebührenordnung vom 1. April 2008, GVBl. S. 97

151 27. Verordnung zur Änderung der Verwaltungsgebührenordnung vom 9. September 2008, GVBl. S. 254

152 Zur ersten Umfrage der Senatsverwaltung für Inneres: JB 2001, 4.9; JB 2000, 3.5

153 Antwort des Senators für Inneres und Sport auf die Kleine Anfrage des Abgeordneten Kai Gersch (FDP), Abghs.-Drs. 16/11789

154 Abghs.-Drs. 16/1900

Negativ zu bewerten ist die Ablehnung des Antrages auf Zulassung eines Volksbegehrens „Schluss mit Geheimverträgen – Wir Berliner wollen unser Wasser zurück“[155]. Damit sollte eine vorbehaltlose Offenlegung der Verträge mit privatrechtlichen und öffentlich-rechtlichen Wasserversorgungsunternehmen erreicht werden. Der Senat hielt die formalen Voraussetzungen für die Zulassung des Volksbegehrens zwar für erfüllt, den vorgelegten Gesetzentwurf aber für verfassungswidrig. Zum einen würden Geheimhaltungsinteressen (Betriebs- und Geschäftsgeheimnisse) betroffener Privater außer Acht gelassen. Zum anderen läge in der Unwirksamkeit von Verträgen, die der Gesetzentwurf für nicht offen gelegte Vereinbarungen vorsah, ein Verstoß gegen den Vertrauensschutz und die Eigentumsgarantie. Fest steht, dass das Anliegen des Volksbegehrens berechtigt ist: Wer mit dem Staat Geschäftsbeziehungen eingeht, muss sich darüber im Klaren sein, dass staatliches Handeln besonderen Kontrollrechten unterliegt und damit Verträge nicht grundsätzlich geheimhaltungsbedürftig sind[156]. Nach dem Scheitern des Volksbegehrens bleibt zu wünschen, dass das Land Berlin ein verfassungskonformes Gesetz zumindest für künftige Verträge auf den Weg bringt.

Eine weitere Verbesserung im Land Berlin könnte dadurch erzielt werden, dass fachliche Weisungen, Dienst- und Verwaltungsvorschriften umfassend über ein zentrales Internet-Portal verfügbar gemacht werden. Das betrifft auch Rundschreiben wie solche zur Umsetzung von Gesetzen[157]. Wir unterstützen deshalb die entsprechende Forderung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in seinem Vorschlag für eine „Charta des digitalen Datenschutzes und der Informationsfreiheit“[158]. Mehrere Bundesländer haben ein solches Online-Portal bereits entwickelt. In Bayern sind seit Anfang des Jahres nur noch diejenigen Verwaltungsvorschriften gültig, die online verfügbar sind; alle übrigen Vorschriften sind außer Kraft getreten („Sunset“).[159] In Bran-

155 Abghs.-Drs. 16/1303

156 Vgl. bereits die Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 11. Juni 2007: Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken!, Dokumentenband 2007, S. 107

157 Vgl. Fußnote 144

158 Aus Anlass des Dritten Nationalen IT-Gipfels am 20. November 2008, vgl. Ziff. 6 des Vorschlags, abrufbar unter http://www.bfdi.bund.de/cln_007/nn_533554/SharedDocs/Publikationen/Allgemein/Charta-Vorschlag-DigitalerDatenschutz.html

159 http://www.verwaltung.bayern.de/Bereinigung-veroeffentlichter-verwaltungsvorschriften-.633.htm

denburg wurde mit der Datenbank BRAVORS ein **Bra**ndenburgisches **Vor**schriften**s**ystem eingeführt.[160] In Bremen wird eine vergleichbare Datenbank als zentrales elektronisches Informationsregister vorbereitet, das nach Informationsfreiheitsgesetz sogar verpflichtend ist.[161] Auch auf Bundesebene ist eine Sammlung mit Verwaltungsvorschriften online verfügbar.[162]

15.2.2 Smiley-System in Pankow – Ein gutes Pilotprojekt

Im Sommer wurden wir durch Pressemeldungen darauf aufmerksam, dass der Bezirk Pankow für 2009 nach dänischem Vorbild ein sog. Smiley-System für von der Lebensmittelüberwachung gut bewertete Gaststätten plant. Die schlecht bewerteten sollen im Internet gelistet sein. Wir haben deshalb sowohl aus Informationsfreiheits- als auch aus Datenschutzgründen um Darstellung des Planungskonzepts gebeten.

Danach ist die Teilnahme am Smiley-System für gut oder sehr gut bewertete Lebensmittelbetriebe freiwillig. Die teilnehmenden Gaststätten treffen eine schriftliche Vereinbarung mit dem Land Berlin, vertreten durch das Bezirksamt Pankow. Darin sollen auch die Veröffentlichung des Betriebs im Internet und die Einzelheiten der Verwendung der amtlichen Bescheinigung durch den Betrieb festgelegt werden, die mit einem Smiley versehen wird. Wir haben empfohlen, die Mustervereinbarung um eine Regelung zu ergänzen, die verdeutlicht, dass bei Beendigung der Teilnahme und nach Rückgabe der Bescheinigung die Löschung der Angaben im Internetangebot des Bezirks zu veranlassen ist.

Die im Rahmen des Projekts zugleich geplante Veröffentlichung von schlecht bewerteten Betrieben im Internet ist unter den Voraussetzungen des § 5 Abs. 1 Satz Verbraucherinformationsgesetz (VIG) zulässig. Wir begrüßen, dass das Ermessen der Verwaltung von vornherein dahingehend ausgeübt werden soll, dass nur gravierende Verstöße gegen das Lebensmittel- und Futtermittelrecht öffentlich zugänglich gemacht werden. Das gilt umso mehr, als die Bestandskraft

160 http://www.landesrecht.brandenburg.de

161 § 11 Abs. 5 BremIFG

162 http://www.verwaltungsvorschriften-im-Internet.de

der Entscheidung über den Verstoß keine Voraussetzung für den Informationszugang ist.[163] Allerdings besteht eine gesetzestechnische Unstimmigkeit insofern, als Informationen über nichtbestandskräftige Verstöße nur dann zugänglich gemacht werden sollen, wenn sie im Verwaltungs(zwangs)verfahren festgestellt bzw. verfolgt werden, nicht aber dann, wenn deshalb ein Ordnungswidrigkeitenverfahren betrieben wird. Zur Vermeidung des damit einhergehenden erheblichen Pflegeaufwandes bei der Internet-Listung haben wir empfohlen, in jedem Fall eine Bemerkung „nicht bestandskräftig" anzubringen. Damit sind einerseits auch laufende Ordnungswidrigkeitenverfahren abgedeckt, ohne sie als solche konkret zu benennen. Andererseits wird in rechtsstaatlich angemessener Weise verdeutlicht, dass gegen die amtliche Feststellung des Verstoßes vorgegangen wird.

Das gesamte Verfahren sollte durch Veröffentlichung im Internet transparent gemacht werden. Damit ist bereits begonnen worden.[164]

Das Smiley-System im Bezirk Pankow ist ein wesentlicher Schritt zu mehr Transparenz und Verbraucherschutz und begegnet keinen datenschutzrechtlichen Bedenken.

15.3 Einzelfälle

Aus der Praxis

Informationszugang bei der Bildungsverwaltung

Ein Journalist beantragte bei der Senatsverwaltung für Bildung, Wissenschaft und Forschung die Übersendung einer elektronischen Kopie der Schulinspektionsberichte, die das Qualitäts- und Unterrichtsprofil der jeweiligen Schule darstellen. Die Senatsverwaltung lehnte den Antrag unter Hinweis auf den laufenden Prozess der Willensbildung und auf den Schutz personenbezogener Daten der Lehrerinnen und Lehrer ab. Die Untersuchung von Stärken und Schwächen einer Schule, der Schulorganisation, der Umset-

163 § 2 Satz 1 Nr. 1b) VIG
164 http://www.berlin.de/ba-pankow/verwaltung/ordnung/smiley.html

zung des staatlichen Unterrichts- und Erziehungsauftrags sowie des pädagogischen Verhaltens sollen unbefangen erfasst und bewertet werden. Eine solche Schulevaluation wäre jedoch nur dann zielführend, wenn die den Lehrkräften zugesagte Vertraulichkeit der Datenverarbeitung gewahrt bleibt. Die Berichte über schlecht bewertete Schulen enthielten mindestens personenbezogene Daten über die Schulleitung bzw. ließen Rückschlüsse zu. Der Petent hat sich Hilfe suchend an uns gewandt.

Wir haben die Auffassung der Senatsverwaltung im Ergebnis geteilt. Danach bestand kein Anspruch auf Einsichtnahme in die einzelnen Schulinspektionsberichte nach dem IFG. Dies folgt aus § 9 Abs. 5 Schulgesetz für das Land Berlin (SchulG). Danach veröffentlicht die Schulaufsichtsbehörde „regelmäßig, spätestens alle fünf Jahre, einen Bildungsbericht, in dem, differenziert nach Bezirken, Schularten und Bildungsgängen, über den Entwicklungsstand und die Qualität der Schulen berichtet wird; die Evaluationsergebnisse sind darin in angemessener Weise darzustellen."

Diese Regelung, die erst in 2004 im Zuge einer umfassenden Schulreform in das SchulG eingefügt worden ist, geht als jüngere und speziellere Bestimmung dem allgemeinen Informationszugangsrecht nach dem IFG von 1999 vor. Denn der Gesetzgeber hat gerade für den Schulsektor eine eigene den Informationszugang regelnde Bestimmung schaffen wollen. Sie ist insofern „informationszugangsfreundlich", als der Staat von sich aus (pro-aktiv), d.h. ohne dass es eines Antrages bedarf, für Transparenz im Hinblick auf die Schulqualität in Berlin sorgen muss. Andererseits hat der Gesetzgeber bewusst darauf verzichtet, dass der Staat auch die einzelnen Schulinspektionsberichte offen legen muss, auch weil ein sog. Schulranking vermieden werden sollte. Dieser Wille des Gesetzgebers kann nicht durch einen allgemeinen Informationszugangsanspruch nach IFG „unterlaufen" werden. Ein über § 9 Abs. 5 SchulG hinausgehender Informationszugangsanspruch, der die Offenlegung der einzelnen Schulinspektionsberichte beinhaltet, ist nach dem eindeutigen Wortlaut des Gesetzes nicht begründet.

Außerdem wurde bei der Senatsverwaltung für Bildung, Wissenschaft und Forschung Akteneinsicht in die Ergebnisse zum mittleren Schulabschluss (MSA) nach der 10. Klasse beantragt. Dabei ging es um Informationen, wie gut oder schlecht die Schülerinnen und Schüler an den einzelnen Schulen im Durchschnitt diesen Schulabschluss geschafft haben. Der Antrag wurde unter Hinweis auf den laufenden Prozess der Willensbildung sowie auf den Schutz personenbezogener Daten der Lehrkräfte abgelehnt, weil sich aus den Ergebnissen in den einzelnen Prüfungsfächern leicht Rückschlüsse auf die Lehrkräfte und deren Unterrichtsqualität ziehen lassen. Der Petent hat Widerspruch gegen die Ablehnung eingelegt und uns um Unterstützung gebeten.

Für die MSA-Prüfungen gilt nach § 9 Abs. 6 SchulG die Vergleichsauswertungsverordnung (VergleichsVO). Darin ist das Verfahren von Auswertungen bei Vergleichs- und zentralen Prüfungsarbeiten einschließlich der Verarbeitung von personenbezogenen Daten geregelt. Nach § 3 Abs. 10 VergleichsVO stellt die Schule „die zusammengefassten Ergebnisse der Lerngruppen und der Schule allen schulischen Gremien zur Verfügung. Nur die Schule darf diese Ergebnisse veröffentlichen, sofern es die Schulkonferenz mit einer Mehrheit von Zweidritteln der stimmberechtigten Mitglieder beschließt." Aus der gesetzgeberischen Historie zum SchulG ergibt sich, dass der Berliner Gesetzgeber ein sog. Schulranking vermeiden wollte. Dieser Wille würde unterlaufen, wenn Dritte Informationen nach dem IFG erhalten, die nur unter den Voraussetzungen der (insofern jüngeren) schulrechtlichen Bestimmungen offen gelegt werden dürfen. Wir haben der Senatsverwaltung für Bildung, Wissenschaft und Forschung gleichwohl empfohlen, dem Widerspruch zumindest teilweise dadurch abzuhelfen, dass der Antrag des Petenten an die Schulen weitergeleitet wird mit der Bitte um Herbeiführung einer Entscheidung nach § 3 Abs. 10 VergleichsVO. Darüber hinaus haben wir empfohlen, die Antworten „gebündelt" dem Antragsteller zu übermitteln.

Die schulrechtlichen Bestimmungen zur Qualitätssicherung und Evaluation sowie zur Veröffentlichung der Berichte verdrängen das IFG, das deshalb nicht anwendbar ist.

Informationszugang bei der Senatsverwaltung für Stadtentwicklung

Die Petentin beantragte als Anbieterin meteorologischer Dienste bei der Senatsverwaltung für Stadtentwicklung die Übersendung einer Kopie des Kooperationsvertrages mit dem Deutschen Wetterdienst (DWD). Die Senatsverwaltung lehnte dies mit der Begründung ab, dass der Vertragspartner nicht dem IFG unterliege und auch keine Zustimmung zur Offenlegung vorliege. Hiergegen legte die Petentin Widerspruch ein und bat uns um Unterstützung.

Bei dem DWD handelt es sich um eine teilrechtsfähige Anstalt des öffentlichen Rechts im Geschäftsbereich des Bundesministeriums für Verkehr, Bau- und Stadtentwicklung. Er unterliegt deshalb dem IFG des Bundes. Wir haben die Senatsverwaltung davon überzeugen können, dass es nicht informationszugangsfreundlich ist, wenn öffentlich-rechtliche Vertragspartner – jeweils unter Hinweis auf das für den anderen nicht geltende eigene Informationsfreiheitsgesetz – Informationen zurückhalten. Mindestens in Fällen, in denen auch die andere Stelle einem Informationsfreiheitsgesetz unterliegt, muss von einer Pflicht der Berliner Stelle zur Einholung der Zustimmung der anderen öffentlichen Stelle nach § 10 Abs. 3 Nr. 2 IFG ausgegangen werden. Die Senatsverwaltung hat daraufhin beim DWD die Zustimmung eingeholt, nachdem sie entsprechend unserer Empfehlung dort darauf hingewiesen hatte, dass sie selbst keinen Grund für die Verweigerung der Offenlegung sehe. Die Petentin hat schließlich sogar eine Kopie von beiden Vertragspartnern erhalten.

Eine Pflicht zur Einholung der Zustimmung nach § 10 Abs. 3 Nr. 2 IFG ist jedenfalls dann anzunehmen, wenn die andere öffentliche Stelle zwar nicht dem IFG, aber einem Informationsfreiheitsgesetz eines anderen Landes oder des Bundes unterliegt.

Aus der Praxis

Informationszugang bei der AOK Berlin

Ein Rechtsanwalt hat sich für einen inzwischen eingestellten Pflegebetrieb bei der AOK Berlin nach den Namen von Informanten erkundigt, die die AOK über Mängel im Pflegebetrieb benachrichtigt hatten. Die AOK hat den Antrag auf Einsicht der Akten zur Qualitätsprüfung des Pflegebetriebs abgelehnt, da die betroffenen Angestellten die Einwilligung verweigert haben.

Da der Pflegebetrieb eingestellt worden war, war auch das Qualitätsprüfungsverfahren beendet. Deshalb kam ein Akteneinsichtsrecht für Beteiligte nach § 25 Sozialgesetzbuch X (SGB X) nicht in Betracht. Nach Abschluss des Verfahrens der Qualitätsprüfung unterlagen die Akten zwar dem allgemeinen Informationszugangsrecht nach § 3 Abs. 1 IFG. Allerdings waren die Namen der Informanten mangels Einverständnis nicht zu offenbaren. Dem stand die Regelung des § 6 Abs. 2 Satz 1 Nr. 1 b) IFG nicht entgegen. Nach dieser Bestimmung stehen der Offenbarung bestimmter personenbezogener Daten schutzwürdige Belange der „Anzeigenerstatter" in der Regel nicht entgegen. Dabei handelt es sich um eine „widerlegbare Vermutung". Im vorliegenden Fall war von solchen schutzwürdigen Belangen der Informanten auszugehen, weil sie aufgrund der gegebenen Hinweise möglicherweise mit erheblichen Nachteilen rechnen müssen. Der Schutz der Informanten war auch nach Beendigung des Arbeitsverhältnisses (wegen Insolvenz des Betriebes) aufrechtzuerhalten, insbesondere für den Fall, dass nachvertragliche Vereinbarungen mit den Betroffenen bestanden. Bei der Abwägung war auch zu berücksichtigen, dass die Pflegekassen in gewissem Umfang auf vertrauliche Hinweise angewiesen sind, um die Qualität der Pflege zu sichern. Die AOK Berlin hat daher im Ergebnis zu Recht die Identität der Anzeigenerstatter nicht offen gelegt.

Die Identität von Hinweisgebern ist nach § 6 Abs. 2 Satz 1 Nr. 1 b) IFG zwar in der Regel, nicht aber in jedem Fall zu offenbaren.

16. Was die Menschen von unserer Tätigkeit haben

Der Presse entnahmen wir, dass die Senatsverwaltung für Finanzen beabsichtigte, sich an den Planungen zum Aufbau von Internetportalen zu beteiligen, bei denen es möglich sein soll, anonym und verschlüsselt Hinweise auf „Steuersünder" zu geben. Da eine solche Datei die Gefahr begründen würde, dass alle Steuerpflichtigen dem Risiko unberechtigter Anzeigen ausgesetzt würden, haben wir die Senatsverwaltung davon überzeugt, von dem Projekt Abstand zu nehmen.

Der Kunde einer Videothek wurde vor der Ausleihe darauf hingewiesen, dass er sich diesen Film vor sechs Monaten schon einmal ausgeliehen habe. Die Videothek sah in der Information einen besonderen Kundenservice. Hierfür würde die Videothek die ausgeliehenen Filme der einzelnen Kundinnen und Kunden dauerhaft speichern. Der Bürger fühlte sich zu Recht als „gläserner Kunde". Wir haben bei der Videothek durchgesetzt, dass der „Erinnerungsservice" nur mit vorheriger Einwilligung der Kundschaft erfolgt. Sie hat jetzt die Wahl, ob sie den Service in Anspruch nehmen möchte oder nicht.

Ein Betroffener beschwerte sich über die unverlangte Zusendung eines Newsletters und bemängelte, dass in der zugesandten E-Mail auch keine Möglichkeit zur Abbestellung vorgesehen war. Das Unternehmen hat eingeräumt, in diesem Einzelfall versehentlich eine Werbe-E-Mail an einen „nicht-validierten Nutzer" verschickt zu haben. Gewöhnlich würden Newsletter nur an Kundinnen und Kunden versandt, die ihre Registrierung nochmals per E-Mail ausdrücklich bestätigen (sog. „Double-Opt-In"). Die internen Abläufe wurden überprüft, um solche Versehen künftig zu vermeiden. Zusätzlich wird das Unternehmen auf unser Betreiben hin künftig Nachrichten um eine einfache elektronische Möglichkeit zur Abbestellung ergänzen.

Der Abonnent eines Newsletters hatte diesen gekündigt, erhielt von dem Unternehmen aber weiterhin Werbeschreiben. Über die SPAM-Versendung des Unternehmens beschwerte er sich bei uns. Unsere Ermittlungen ergaben,

dass das Unternehmen die personenbezogenen Daten des ehemaligen Kunden zwar in seinem regulären Datenbestand gelöscht hatte. Nach einer Datenpanne verwendete es aber eine veraltete Sicherheitskopie, in der der Petent noch als aktueller Kunde geführt wurde. Wir sorgten nicht nur dafür, dass der Kunde erneut aus dem Datenbestand entfernt wurde, sondern hielten das Unternehmen auch an, künftig nur aktuelle Sicherheitskopien zu verwenden.

Ein Anbieter von Telemedien speichert zu Zwecken der Datensicherheit für einen kurzen Zeitraum, unter welchen IP-Adressen sich die Nutzenden auf der Plattform des Anbieters angemeldet haben. Ein Nutzer begehrte Auskunft über die dort zu seiner Kennung gespeicherten IP-Adressen, um festzustellen, ob ein Dritter sich unberechtigt Zugang zu seinen auf der Plattform gespeicherten personenbezogenen Daten verschafft hatte, um eventuell Strafanzeige stellen zu können. Der Anbieter verweigerte die Auskunft mit dem Hinweis, er dürfe nach den Datenschutzregelungen des Telemediengesetzes Auskünfte für Zwecke der Strafverfolgung nur den Strafverfolgungsbehörden selbst erteilen. Wir haben den Anbieter darauf hingewiesen, dass diese Auffassung unzutreffend ist. Daraufhin erhielt der Betroffene die gewünschte Auskunft.

Ein Betreiber eines Internet-Finanzinformationsdienstes hatte einen Nutzer wegen Verstoßes gegen die Nutzungsbedingungen von der weiteren Teilnahme an dem Dienst ausgeschlossen und die Nutzerkennung gesperrt. Der Betroffene verlangte daraufhin Auskunft von dem Anbieter über die dort zu seiner Person gespeicherten Daten. Die Auskunft wurde verweigert. Der Anbieter machte geltend, er sei hierzu nicht verpflichtet, da die Daten nur noch aufgrund der Aufbewahrungsvorschriften im Wertpapierhandelsgesetz gespeichert seien. Unsere Überprüfung ergab jedoch, dass diese Vorschriften hier nicht anwendbar waren. Dem Betroffenen wurde daraufhin die gewünschte Auskunft erteilt.

In den Jobcentern wird vermehrt Sicherheitspersonal eingesetzt. Mehrere Bürgereingaben belegten die Unsicherheit darüber, ob dies datenschutzrechtlich zulässig ist. Der Einsatz von Sicherheitspersonal in der Eingangszone und den Sachbearbeiterbüros ist im Einzelfall zulässig, wenn eine Situation eskaliert bzw. wenn konkrete Hinweise auf eine Gefährdung der Beschäftigten des Jobcenters bestehen. Kundinnen und Kunden, die im selben Raum (in Hörweite) beraten werden, von denen aber keine Gefahr zu erwarten ist, können allerdings nicht

verpflichtet werden, ein Mithören der Sicherheitsbeauftragten bei der Beratung zu dulden. Insoweit müssen sie die Möglichkeit haben, ohne Sicherheitspersonal beraten zu werden. Seine Anwesenheit muss dann auf die Gänge des Hauses beschränkt bleiben. Wir haben diese Verfahrensweise den Jobcentern empfohlen und so zur Schaffung von Rechtssicherheit beigetragen.

Ein Jobcenter hat sich an die Vermieterin eines Leistungsempfängers gewandt, um Auskünfte über ein streitiges Untermietverhältnis zu erhalten. Dies verstößt gegen das Gebot der Direkterhebung bei Betroffenen. Nach unserem Hinweis hat das Jobcenter den Datenschutzverstoß eingesehen. Überdies hat es seine Belegschaft noch einmal für den Datenschutz sensibilisiert, damit in Zukunft derartige Verstöße vermieden werden.

Der Ermittlungsdienst eines Bezirksamtes wollte mit einem unangekündigten Hausbesuch die Wohnverhältnisse einer Bürgerin prüfen. Sie hat den Mitarbeitern des Bezirksamtes den Zutritt verwehrt und uns um Prüfung der Rechtslage gebeten. Die Durchführung eines unangekündigten Hausbesuchs ist datenschutzrechtlich unzulässig, denn es werden Grundrechte der Betroffenen in erheblichem Maße verletzt. Eine ausdrückliche Rechtsgrundlage für die Durchführung von Hausbesuchen gibt es nicht[165]. Deshalb darf sich die Zutrittsverweigerung nicht negativ auf die Leistungsgewährung auswirken. Wir haben das Bezirksamt davon überzeugt, künftig unangekündigte Hausbesuche zu unterlassen.

Bei der Prüfung der Anträge von selbständig tätigen Leistungsempfängerinnen und -empfängern verlangten Jobcenter teilweise umfassende Geschäftsunterlagen. Wir konnten bewirken, dass dort künftig abgestuft vorgegangen wird. Zunächst werden die relevanten Unterlagen von den Leistungsempfängerinnen oder -empfängern angefordert, wobei sie auf die Möglichkeit des Schwärzens hinzuweisen sind. Ist dies den Betroffenen wegen der Menge der Unterlagen nicht zumutbar, hat das Jobcenter die Möglichkeit, bei einem persönlichen Gespräch die gesamten Geschäftsunterlagen zu sichten und relevante Papiere zu kopieren. Auch hier sollten Schwärzungen vorgenommen werden. Kann die Menge der Unterlagen im Termin nicht abschließend gesichtet werden, ist es zulässig, ausnahmsweise die gesamten Geschäftsunterlagen zu kopieren.

165 Vgl. Sozialgericht Lübeck, Beschluss vom 14. Februar 2008 – S 27 AS 106/08 ER

Schwärzungen muss dann das Jobcenter selbst vornehmen und die nicht erforderlichen Unterlagen anschließend vernichten. Durch dieses „Stufenmodell" ist eine praxisnahe und datenschutzkonforme Vorgehensweise gewährleistet.

Eine Bürgerin wollte mit ihrem ausländischen Ehemann, der in einem Asylbewerberheim lebte, eine gemeinsame Wohnung beziehen. Das Vorhaben wurde neben weiteren Punkten im Jobcenter besprochen. Über das Gespräch wurde ein Vermerk gefertigt, der umfassende Daten über die Bürgerin und ihren persönlichen und beruflichen Werdegang enthielt. Nach Rücksprache mit der für den Ehemann zuständigen Ausländerbehörde hat der Mitarbeiter des Jobcenters den Gesprächsvermerk unverschlüsselt per E-Mail an die Ausländerbehörde geschickt. Sowohl die Übermittlung des Vermerks als solche, als auch die Versendung als unverschlüsselte Mail waren unzulässig und wurden von uns beanstandet. Darauf hat das Jobcenter sehr schnell reagiert und eine Regelung darüber getroffen, wer über das Versenden von Sozialdaten entscheiden darf. Die Teamleiterinnen und -leiter wurden erneut zum Datenschutz geschult, und das Jobcenter hat eine Dienstanweisung zur Verschlüsselung von E-Mails erlassen. Somit konnten wir für die Zukunft eine datenschutzgerechte Vorgehensweise beim Jobcenter bewirken.

Mehrere Bürgerinnen und Bürger beschwerten sich bei uns über einen Fragebogen, auf dem sie intime Angaben zu ihrem Gesundheitszustand machen sollten. Der Fragebogen wurde ihnen von einem Unternehmen zugeschickt, das sie im Auftrag ihrer gesetzlichen Krankenkasse mit Hilfsmitteln (Inkontinenzprodukte) versorgen sollte. Wir konnten eine Neugestaltung des Formulars erreichen. Ein zugehöriges Anschreiben klärt jetzt über den Zweck und die Erforderlichkeit der Erhebung der sensitiven Daten auf. Es wird zudem ausdrücklich darauf hingewiesen, dass die Angaben freiwillig sind.

Eine Einrichtung der Berliner Drogenhilfe wandte sich an uns und bat um Beratung. Die Einrichtung wird durch die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz finanziell gefördert. Im Rahmen der haushaltsrechtlich vorgesehenen Prüfung der zweckgerechten Verwendung der Fördermittel wurde sie aufgefordert, umfangreiche Unterlagen - darunter auch Belege über Einzahlungen (Kontoauszüge) - im Original einzureichen. Auf den Kontoauszügen befanden sich zum Teil auch die Namen der Klienten, die das Hilfeangebot in Anspruch nehmen. Diese Daten wollte die

Therapieeinrichtung zu Recht nicht preisgeben. Wir konnten erreichen, dass die Verwendungsnachweise der Senatsverwaltung vorerst nur in Kopie und mit entsprechenden Schwärzungen zur Verfügung gestellt werden müssen. So werden die hochsensiblen Daten von Drogenabhängigen nicht preisgegeben.

Eine Bürgerin beschwerte sich darüber, dass ein Berliner Krankenhaus einen Bericht über ihre stationäre Behandlung in Form eines Arztbriefes entgegen ihrem ausdrücklichen Wunsch an die sie einweisende Ärztin geschickt hat. Das Krankenhaus musste diesen Vorwurf bestätigen und hat den Brief von der Ärztin zurückgefordert. Wir haben der Krankenhausleitung empfohlen, den Patientenwillen im Hinblick auf Datenübermittlungen künftig in der Patientenakte so zu dokumentieren, dass alle an der Behandlung teilnehmenden Mitarbeiter ihn problemlos nachvollziehen und auch beachten können.

Immer häufiger wird vor kostspieligen ärztlichen oder zahnärztlichen Behandlungen, die mit Vorleistungen des ärztlichen Personals verbunden sind, eine Prüfung der Bonität der Behandlungsbedürftigen durch eine Anfrage bei einer Handels- oder Wirtschaftsauskunftei durchgeführt. Mit dieser Anfrage wird zwangsläufig auch die der ärztlichen Schweigepflicht unterliegende Tatsache offenbart, dass sich eine bestimmte Person in ärztlicher Behandlung befindet. In zwei Fällen konnten wir die betroffenen Bürger darüber aufklären, dass ein solches Vorgehen nur mit ihrer Einwilligung zulässig ist.

Zahlreiche Bürgerinnen und Bürger wandten sich an uns, weil sie Unterstützung bei Auskunftsbegehren gegenüber Polizei und Verfassungsschutz erhofften. Wir haben erreicht, dass sie vollständig Auskunft erhielten und nicht mehr erforderliche Daten bei den Sicherheitsbehörden gelöscht wurden.

Petentinnen und Petenten haben sich bei uns darüber beschwert, dass sie bei der Anmeldung zu Kursen an einer bezirklichen Musikschule im Internet in einem Pflichtfeld das genaue Geburtsdatum angeben mussten. Dies ist zum Zeitpunkt der Vormerkung für einen Musikkurs weder für die Einteilung in altersgerechte Lerngruppen noch für die Frage erforderlich, ob ein entsprechendes Unterrichtsangebot überhaupt (noch) zur Verfügung steht. Hierfür ist die Altersangabe in Jahren ausreichend. Erst wenn es zum Vertragsschluss kommt, ist das genaue Gburtsdatum des Vertragspartners (Schülerin, Schüler oder Ansprechperson) zur Feststellung der Geschäftsfähigkeit erforderlich. Die

Musikschule hat auf unseren Hinweis mitgeteilt, dass sie künftig im Internetformular bei der Vormerkung zum Musikschulunterricht auf die Abfrage des Geburtsdatums verzichten und nur eine allgemeine Altersabfrage nach Jahren vornehmen wird.

Jährlich wenden sich einige Dutzend Bürgerinnen und Bürger telefonisch, aber auch schriftlich, mit der Frage an uns: „Das Amt für Statistik will mich zum Mikrozensus zwingen. Ist das rechtmäßig?“ Durch die gezielten Anfragen zum Verfahren und zum Auftreten der „Interviewer“ konnten wir prüfen, ob die Vorgaben des Mikrozensusgesetzes eingehalten werden. Den Betroffenen können wir allerdings meist nicht helfen, da eine gesetzliche Auskunftspflicht besteht und die Verfassungsmäßigkeit des Mikrozensus bereits mehrfach überprüft wurde. Immerhin haben wir die Betroffenen über die Rechtslage informiert.

Eine erhebliche Unsicherheit haben wir im Umgang mit Mieterdaten festgestellt, wenn Grundstückseigentümer ein Anwesen – unter Beibehaltung der Mietverträge – verkauften. So beschwerten sich Mietparteien mehrere Male, dass ihnen eine Veräußerungsanzeige zugegangen sei, der neben dem vollständigen notariellen Kaufvertrag auch eine Liste beigefügt war, in der einzelne Mieterinnen und Mieter namentlich mit ihren angeblichen Mietrückständen aufgeführt waren. Der Gesetzgeber geht in § 569 i. V. m. § 577 Bürgerliches Gesetzbuch (BGB) davon aus, dass der mit der Veräußerungsanzeige beabsichtigte Schutz der Mieterinteressen auch ohne die Übermittlung von Vertragsdaten Dritter erreicht werden kann. Deshalb enthalten diese Vorschriften keine Befugnis zur Datenübermittlung. Wir bewirkten mit Unterstützung der Senatsverwaltung für Justiz, dass die Notarkammer ihre Mitglieder auf die Rechtslage hinwies.

Mehrere Tageszeitungen veröffentlichten in ihrem Internetauftritt Handelsregisterdaten. Dabei konnte man mit einer Suchmaske nicht nur nach Firmen, sondern auch nach Personennamen suchen. Da man hierdurch die wirtschaftliche Betätigung von Menschen nachvollziehen konnte, bestand die Gefahr, dass wirtschaftliche Persönlichkeitsprofile hergestellt werden. Wir haben gemeinsam mit dem für das Handelsregister zuständigen Amtsgericht bewirkt, dass diese Veröffentlichungspraxis geändert wurde.

Eine Bürgerin beschwerte sich darüber, dass ihr beim Akteneinsichtstermin im Bezirksamt Reinickendorf das Fotografieren der nach Informationsfreiheitsgesetz (IFG) vorgelegten Unterlagen untersagt wurde. Wir waren – wie das Bezirksamt – der Auffassung, dass das IFG eine solche Vervielfältigungsmöglichkeit formal nicht vorsieht. Gleichwohl konnten wir das Bezirksamt davon überzeugen, dass mitgebrachte Vervielfältigungsgeräte wie Fotoapparate und Scanner eine Verringerung des Aufwandes für beide Seiten bedeuten: Die Bürgerin erspart sich die für Kopien anfallende Gebühr, der Staat das Kopieren sowie das Einziehen der Gebühr. Das Bezirksamt folgte unserer Empfehlung, die Vervielfältigung künftig zu gestatten, wenn die Voraussetzungen für die Herausgabe von Kopien nach § 13 Abs. 5 IFG vorliegen.

17. Aus der Dienststelle

17.1 Entwicklungen

Die Zahl der Eingaben von Bürgerinnen und Bürgern hat bei uns einen neuen Höchststand erreicht. Dies beruht vor allem auf einem Anstieg der Beschwerden gegen private Datenverarbeiter. Dabei wurden die zunehmenden telefonischen Anfragen nicht erfasst. Insgesamt ist festzustellen, dass die Mitarbeiterinnen und Mitarbeiter der Dienststelle die permanent wachsenden Aufgaben der Beratung, Kontrolle und Verfolgung von Ordnungswidrigkeiten kaum noch angemessen erfüllen können. Deshalb ist eine moderate Erweiterung der Personalkapazität dringend geboten, um den Auftrag der Verfassung von Berlin (Art. 47) zur Wahrung des Rechts auf informationelle Selbstbestimmung weiterhin erfüllen zu können. Zudem sind neue Aufgaben bereits absehbar, die bei Verabschiedung eines Datenschutz-Auditgesetzes auf Bundesebene auf die Dienststelle zukommen würden.[166]

17.2 Zusammenarbeit mit dem Abgeordnetenhaus

Der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses hat die Stellungnahme des Senats zum Jahresbericht 2006 abschließend beraten und außerdem zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit erörtert. Seine parteiübergreifend beschlossenen Empfehlungen sind in den Beschluss des Abgeordnetenhauses vom 10. Juli[167] eingegangen.

17.3 Zusammenarbeit mit anderen Stellen

Die enge Kooperation mit anderen Beauftragten für Datenschutz und Informationsfreiheit ist eine wesentliche Voraussetzung dafür, dass aktuelle Fragen

166 Vgl. Tabelle nächste Seite
167 Vgl. Anlage 1

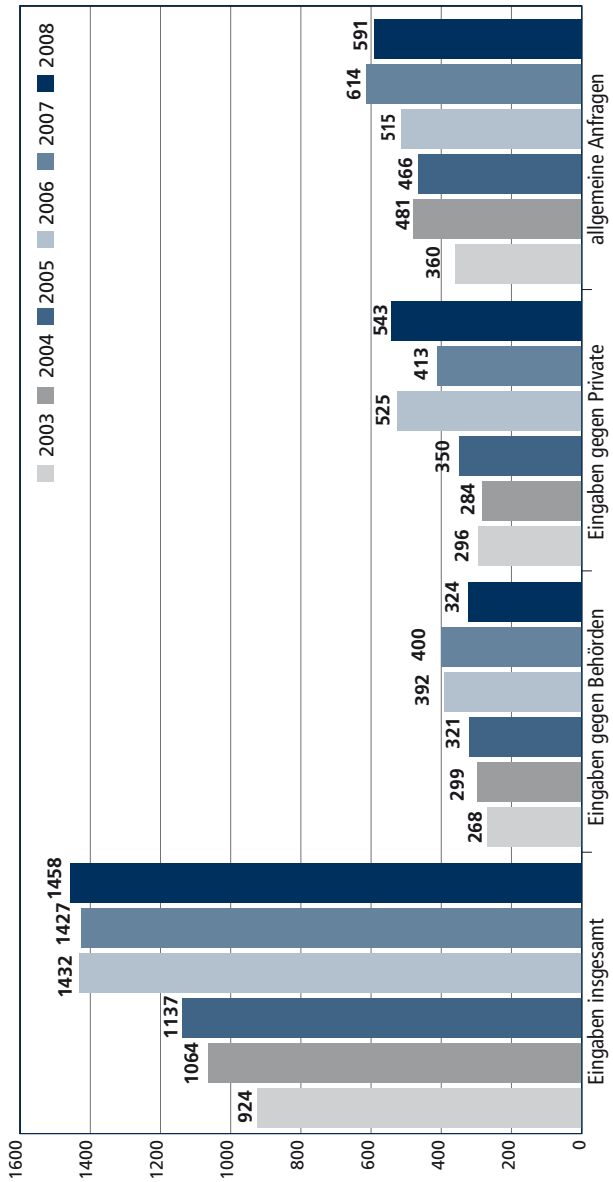

Tabelle 1: Anzahl der Bürgereingaben im Jahresvergleich 2003–2008

möglichst einheitlich beantwortet und die Antworten auch öffentlich gemacht werden. Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder,** die den Datenschutz im Bereich der öffentlichen Verwaltung zum Gegenstand hat, tagte unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 3./4. April in Berlin und am 6./7. November in Bonn. Sie fasste zahlreiche Entschließungen, die aktuelle, aber auch grundlegende Fragen des Datenschutzes betreffen. Hervorzuheben ist die sog. Berliner Erklärung vom 4. April[168]. Für das Jahr 2009 hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit den Konferenzvorsitz übernommen.

Die nicht mehr zeitgemäße Aufspaltung der Datenschutzkontrolle zwischen dem öffentlichen und dem nicht-öffentlichen Bereich spiegelt sich darin wieder, dass neben der Datenschutzkonferenz der **„Düsseldorfer Kreis" der Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft** besteht, der unter dem Vorsitz des Hessischen Ministeriums des Innern und für Sport am 17./18. April und am 13./14. November in Wiesbaden tagte. Dabei wurden fünf Beschlüsse zu Fragen des Datenschutzes im Internet und beim Versandhandel, aber auch zur Datenschutzgesetzgebung gefasst. Für das Jahr 2009 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern den Vorsitz in diesem Gremium übernommen.

Die **Konferenz der Informationsfreiheitsbeauftragten,** die am 11. Juni unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes und am 3./4. Dezember unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern tagte, hat drei Entschließungen zur Transparenz in der Finanzverwaltung und zur Stärkung der Informationsfreiheit auf europäischer Ebene gefasst[169]. Im ersten Halbjahr 2009 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Sachsen-Anhalt den Vorsitz dieser Konferenz übernommen.

Wir vertreten die Datenschutzbeauftragten und die Aufsichtsbehörden der Bundesländer in der **Arbeitsgruppe nach Artikel 29 der Europäischen Datenschutzrichtlinie**. Diese Arbeitsgruppe hat u.a. eine Stellungnahme zu

168 Vgl. Dokumentenband 2008, S. 9
169 Vgl. a. a. O., S. 147

Datenschutzfragen im Zusammenhang mit Suchmaschinen beschlossen, die zu einem Wettbewerb um besseren Datenschutz unter den Suchmaschinenanbietern beitrug[170].

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die französische Commission Nationale de l'Informatique et des Libertés luden vom 15. – 17. Oktober zur **30. Internationalen Konferenz der Datenschutzbeauftragten** im Europarat in Straßburg ein. Anlass war zugleich das 30-jährige Bestehen der beiden nationalen Datenschutzbehörden. Dabei wurden Entschließungen zum Schutz der Privatsphäre von Kindern im Internet, zum Datenschutz in sozialen Netzwerkdiensten und zur Dringlichkeit der Erarbeitung internationaler Normen zum Schutz der Privatsphäre verabschiedet. **Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group")** tagte unter unserem Vorsitz am 3./4. März in Rom und am 16. Oktober in Straßburg. Sie verabschiedete Arbeitspapiere zum Datenschutz in sozialen Netzwerkdiensten („Rom Memorandum") und zur Umsetzung und Anwendung der Europaratskonvention Nr. 185 zur Computerkriminalität[171].

Die **Europäische Konferenz der Informationsfreiheitsbeauftragten** fand am 29. September auf Einladung der slowenischen Informationsfreiheitsbeauftragten in Brdo pri Kranj statt.

17.4 Öffentlichkeitsarbeit

Zum zweiten Mal wurde am 28. Januar der vom Europarat initiierte und nun jährlich Ende Januar stattfindende Europäische Datenschutztag begangen.[172] Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte beschlossen, an diesem Tag die neuen Entwicklungen des Internetzeitalters wie soziale Netzwerke und Bewertungsplattformen zu thematisieren, die insbesondere von der Jugend genutzt werden, ohne dass sie sich der damit

170 Vgl. a. a. O., S. 41
171 Vgl. a. a. O., S.129
172 Bereits JB 2007, 14.4

einhergehenden Gefahren bewusst ist. Das Interesse an diesen Themen, die unter dem Motto „Web 2.0 – Datenschutz 2.0“ zusammengefasst waren, zeigte die außergewöhnlich hohe Zahl von Teilnehmenden an der Veranstaltung. Sie fand mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in der Robert-Jungk-Oberschule statt und bestand aus mehreren Workshops und einer Podiumsdiskussion.

Die Vorbereitungen für den 3. Europäischen Datenschutztag wurden bereits getroffen. Er steht unter Motto „Der ideale Angestellte, der genormte Arbeitnehmer: Wie viel darf mein Arbeitgeber über mich wissen?“

Daneben haben wir uns 2008 wieder an mehreren öffentlichen Veranstaltungen beteiligt:

- Tag der offenen Tür der Polizei bei der Wasserschutzpolizei am 25. Mai
- Tag der offenen Tür des Abgeordnetenhauses am 7. Juni
- YOUNG IFA am 3. September
- Brandenburg-Tag am 6. September
- Wannsee-Forum am 24. September
- Jugendverbraucherschutztag im Freizeit- und Erholungszentrum Wuhlheide am 1. Oktober
- Jugendmesse YOU vom 24. – 26. Oktober
- Netd@ys und Jugendnetz am 18. November
- 8. Berliner Jugendforum im Abgeordnetenhaus am 6. Dezember

Die verstärkte Präsenz der Dienststelle bei diesen Veranstaltungen war nur durch zusätzliches Engagement der Mitarbeiterinnen und Mitarbeiter möglich. Daneben haben wir in mehreren Berliner Schulen mit Schülerinnen und Schülern Fragen des Datenschutzes diskutiert. Dies werden wir auch in Zukunft im Rahmen unserer Möglichkeiten fortsetzen.

Berlin, 29. April 2009

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Anhang

Anhang 1:
Beschlüsse des Abgeordnetenhauses vom 10. Juli 2008

Anhang 2:
Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 10. Juli 2008 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2006

Anhang 3:
Auszug aus dem Geschäftsverteilungsplan

Beschlüsse des Abgeordnetenhauses vom 10. Juli 2008

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2006

Zu: Warum sagt mir keiner was? - Das Recht auf Einsicht in die Patientenakte (5.2.1, Drs. S. 96 ff.)

Der Senat wird aufgefordert, in einem mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit abzustimmenden Schreiben die Ärztekammer Berlin und die Berliner Krankenhausgesellschaft darauf hinzuweisen, dass deren Mitglieder ihren Patienten auf Antrag Einsicht in die sie betreffende ärztliche Behandlungsdokumentation (Patientenakte) zu gewähren haben. Das Recht der Patienten auf Akteneinsicht darf nur unter besonderen Voraussetzungen eingeschränkt werden.

Zu: Einführung des Fallmanagements in der Eingliederungshilfe (5.1.2, Drs. S. 89 ff.)

Der Senat wird aufgefordert, dafür zu sorgen, dass bei der Einführung eines Fallmanagements in ausgewählten Leistungsbereichen des SGB XII (Sozialhilfe) der Datenschutz für die betroffenen Leistungsempfänger gewahrt bleibt. Die durch das Fallmanagement bedingte intensivere Zusammenarbeit zwischen Sozialämtern, Gesundheitsämtern und freien Trägern von Hilfeleistungen darf nicht zu einem Austausch von Sozialdaten führen, der über das Maß des für die eigentliche Leistungsgewährung Erforderlichen hinausgeht.

Zu: Verkauf der Berliner Bank (7.2.1, Drs. S. 144 f)

Der Senat wird aufgefordert, beim Verkauf landeseigener Unternehmen (z. B. Banken, Wohnungsgesellschaften) sicherzustellen, dass personenbezogene Daten

insbesondere von Kunden und Beschäftigten vor Beginn des Bieterverfahrens ausgesondert und nur diejenigen Unternehmensunterlagen offenbart werden, die der Kaufinteressent zur Einschätzung der finanziellen Situation des potenziellen Kaufobjekts benötigt.

Zu: Der Albtraum einer zentralen Schülerdatenbank (6.3.2, Drs. S. 130 ff.)

Der Senat wird aufgefordert, bei der Umstellung auf eine Schülerindividualstatistik ab dem Schuljahr 2008/2009 die Grundsätze der strikten Trennung von Statistik und Verwaltungsvollzug sowie der statistischen Geheimhaltung zu beachten und datenschutzgerechte Lösungsvorschläge in die Beratungen der Kultusministerkonferenz der Länder einzubringen.

Zu: Rundfunkgebühr für internetfähige PCs (10.3.2, Drs. S. 190 f)

Der Senat wird aufgefordert, darauf hinzuwirken, dass das gegenwärtige System der Rundfunkgebühren so überarbeitet wird, dass die Verarbeitung personenbezogener Daten von Rundfunkteilnehmern auf das erforderliche Mindestmaß reduziert wird.

Zu: Weitergabe von vertraulichen Informationen an Dritte durch die Justizvollzugsanstalt Tegel (4.3.4, Drs. S. 78 ff.)

Der Senat wird aufgefordert, dafür zu sorgen, dass Justizvollzugsanstalten auch weiterhin bei Stellungnahmen gegenüber Strafvollstreckungskammern personenbezogene Daten von (Mit-)Gefangenen nur im erforderlichen Umfang übermitteln.

Zu: Allgemeines Gleichbehandlungsgesetz (7.3.1, Drs. S. 148 f)

Der Senat wird aufgefordert, dafür zu sorgen, dass die wegen des Allgemeinen Gleichbehandlungsgesetzes (AGG) erforderliche Verarbeitung personenbezogener Daten von (künftigen) Beschäftigten berlinweit nach einheitlichen Maßstäben erfolgt.

Zu: Videoaufnahmen der Polizei bei Hausdurchsuchungen und Versammlungen? (3.3.1, Drs. S. 57 f)

Der Senat wird aufgefordert, durch eine Dienstanweisung sicherzustellen, dass Bild- und Tonaufnahmen von Versammlungen nur in anonymisierter Form für Ausbildungs- und Schulungszwecke verwendet werden. Personenbezogene Bild- und Tonaufnahmen von Versammlungen dürfen nur im Rahmen der gesetzlichen Bestimmungen gespeichert und verwendet werden.

Zu: Informationsfreiheit im Land Berlin (hier: Behördliche Informationsfreiheitsbeauftragte) (11.3, Drs. S. 195, 197)

Der Senat wird aufgefordert zu prüfen, ob der behördliche Datenschutzbeauftragte zugleich die (koordinierende) Funktion eines behördlichen Informationsfreiheitsbeauftragten wahrnehmen kann, der als solcher auch dem Berliner Beauftragten für Datenschutz und Informationsfreiheit benannt wird. Der Senat wird aufgefordert, eine entsprechende Prüfbitte an die Bezirksämter zu richten und dem Ausschuss für Inneres, Sicherheit und Ordnung bis zum 31. Dezember 2008 zu berichten.

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 10. Juli 2008 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2006

Frau Präsidentin,
meine Damen und Herren,

der Datenschutz ist in letzter Zeit in fast aller Munde. Die veröffentlichten Berichte über die Ausspähung von Mitarbeitern in Supermarkt-Filialen wie auch von Journalisten, die über die Telekom berichteten, erinnern schon in ihrer Diktion fatal an die Sprache der Zuträger des Ministeriums für Staatssicherheit und haben die Öffentlichkeit aufgerüttelt. Allenthalben und mit Recht fordern Politiker aufgrund der massiven Verletzung des Fernmeldegeheimnisses bei der Telekom jetzt eine Stärkung des Datenschutzes. Dazu gehören selbst solche Politiker, die für die drastische Beschneidung von datenschutzrechtlichen Sicherungen im staatlichen Bereich bei gleichzeitiger Ausweitung der Befugnisse von Sicherheitsbehörden und Geheimdiensten eintreten. Wie lange das Interesse der Bundespolitik am Datenschutz anhalten wird, vermag ich nicht zu beurteilen.

Ich bin aber sehr dankbar dafür, dass das Berliner Abgeordnetenhaus seit jeher den Datenschutz auch unabhängig von der Aufdeckung skandalöser Zustände und in parteiübergreifender Sachlichkeit in einem eigenen Unterausschuss für Datenschutz und Informationsfreiheit behandelt. Dieser Unterausschuss hat zu meinem Jahresbericht 2006 die neun Beschlussempfehlungen des Innenausschusses vorbereitet, die Ihnen heute vorliegen.

Sie betreffen so unterschiedliche Themen wie

- das Recht auf Einsicht in Patientenakten,
- das Sozialgeheimnis in der Eingliederungshilfe,
- den Datenschutz beim Verkauf landeseigener Unternehmen,
- die Pläne für eine zentrale Schülerdatenbank für statistische Zwecke,
- die Datenverarbeitung zur Einziehung der Rundfunkgebühren,

- den Datenschutz im Strafvollzug,
- die Umsetzung des Allgemeinen Gleichbehandlungsgesetzes im Land Berlin,
- die Verwendung von polizeilichen Bild- und Tonaufnahmen bei Versammlungen und
- einen Prüfauftrag an den Senat zur Übertragung der koordinierenden Funktion des behördlichen Informationsfreiheitsbeauftragten an den jeweiligen behördlichen Datenschutzbeauftragten.

Die Liste dieser Themen macht nicht nur deutlich, wie intensiv sich der Unterausschuss mit den praktischen Problemen des Datenschutzes und der Informationsfreiheit auseinandergesetzt hat, die 2006 festgestellt worden sind. Sie belegt zugleich die Entschlossenheit aller Fraktionen dieses Hauses, den Berliner Beauftragten für Datenschutz und Informationsfreiheit bei der Erfüllung seiner Aufgaben zu unterstützen. Auch dafür bin ich dankbar.

In einem weiteren Punkt hatte der Unterausschuss zunächst empfohlen, den Senat zu einer Bundesratsinitiative mit dem Ziel der Einführung eines Rechts jedes Steuerpflichtigen auf Einsicht in seine Steuerakte aufzufordern. Diese Empfehlung wurde im Innenausschuss zurückgezogen, nachdem sich abzeichnete, dass die Bundesregierung einer entsprechenden Aufforderung des Bundesverfassungsgerichts vom März dieses Jahres durch eine Regelung im Jahressteuergesetz 2009 Folge leisten würde. Inzwischen hat das Bundesministerium der Finanzen es sich jedoch anders überlegt und will die Aufforderung des Bundesverfassungsgerichts offenbar ignorieren. Die ursprüngliche Empfehlung des Unterausschusses wird also wieder aufzugreifen sein.

Frau Präsidentin, meine Damen und Herren,

die eingangs erwähnten Vorgänge bei der Telekom, die jetzt die Staatsanwaltschaft beschäftigen, betreffen auch mehrere in Berlin ansässige Unternehmen, die für die Telekom gearbeitet haben und der datenschutzrechtlichen Aufsicht des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterliegen. Unsere Überprüfungen in dieser Sache stehen erst am Anfang. Dennoch ist bereits absehbar, dass diese Vorgänge unabhängig von ihrer strafrechtlichen Bewertung auch Konsequenzen für das bundesweit geltende Datenschutzrecht

ebenso wie für die Datenschutzaufsicht in Berlin haben müssen. Ohne dem Ergebnis der Ermittlungen vorgreifen zu wollen, lässt sich bereits jetzt feststellen, dass über eine grundsätzliche Neuausrichtung des Datenschutzes nachgedacht werden muss. Neben der überfälligen Modernisierung des Bundesdatenschutzgesetzes sind eine strengere Kontrolle der Detekteien, die Schließung möglicher Strafbarkeitslücken, ein bundeseinheitliches Datenschutzaudit, aber auch die Stärkung der externen wie der unternehmensinternen Datenschutzkontrolle geboten. Alle diese Maßnahmen werden kriminelles Handeln auch in Zukunft nicht völlig ausschließen, wohl aber wesentlich erschweren.

Ich kann die notwendigen Konsequenzen aus den Ereignissen der letzten Monate hier nur kurz skizzieren, werde sie aber zu gegebener Zeit in konkrete Vorschläge fassen. Für deren Umsetzung hoffe ich auf Ihrer aller Unterstützung.

Vielen Dank für Ihre Aufmerksamkeit.

Auszug aus dem Geschäftsverteilungsplan

Stand: 31. Dezember 2008

An der Urania 4 – 10, 10787 Berlin
Telefon: (0 30) 1 38 89-0, Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de,
Internet: http://www.datenschutz-berlin.de

Berliner Beauftragter für Datenschutz und Informationsfreiheit	
App. 202	**Dr. Alexander Dix,** Berliner Beauftragter für Datenschutz und Informationsfreiheit
App. 400	Dipl.-Informatiker **Hanns-Wilhelm Heibey** ,Vertreter
App. 204	Anja-Maria Gardain, Pressesprecherin
App. 200	Sekretariat, Privacy and Information Magazine (PRIMA), Veranstaltungen, Dienstreisen für den Zentralen Bereich
ZENTRALER BEREICH	
App. 204	**Anja-Maria Gardain,** Bereichsleiterin AG: Internationaler und europäischer Datenschutz, Abgeordnetenhaus, Bezirksverordnetenversammlungen, Informationsfreiheit
Zentrale Aufgaben	
App. 211	AG: Telekommunikation, Tele- und Mediendienste Presse und Rundfunk
App. 310	Besondere Aufgaben, Veranstaltungen
App. 213	Redaktion von Veröffentlichungen, Bibliothek, Rechtsprechungssammlung, Intranet, Referendare, Konferenzvorbereitungen

Allgemeine Verwaltung	
App. 230	Beauftragte für den Haushalt, Haushaltsplanung und -bewirtschaftung, Personalangelegenheiten, Büroorganisation, Ausbilderin
App. 232	Sekretariat Allgemeine Verwaltung, Rechnungsstelle
BEREICH RECHT	
App. 300	**Dr. Thomas Petri**, Bereichsleiter, Vertreter des BlnBDI für den Bereich AG: Senatskanzlei (außer Kultur), Rechnungshof, Justiz, Grundsatzangelegenheiten des Datenschutz- sowie des Sicherheits- und Ordnungsrechts, Parteien, Nachrichtendienste, Integration (Ausländerrecht)
App. 302	Sekretariat
BürgerOffice	
App. 111	Leitung; Öffentlichkeitsarbeit AG: Finanzen, Schule
App. 112	AG: Inneres, Sport
App. 100	Archiv des Bereichs Recht, Schreibarbeiten
App. 104	Geschäftsstelle BürgerOffice, Eingangspost, Schreibarbeiten
App. 102	Geschäftsstelle BürgerOffice, Ausgangspost, Broschürenversand, Schreibarbeiten
Recht	
App. 305	AG: Wissenschaft, Forschung und Statistik
App. 309	AG: Wirtschaft, Zivilrecht, Verbraucherschutz
App. 311	AG: Arbeitnehmerdatenschutz, Wirtschaft, Personaldaten

App. 212	Stellvertretender Pressesprecher AG: Gesundheit, eGovernment
App. 318	AG: Jugend
App. 315	AG: Soziales
App. 304	AG: Stadtentwicklung, Kultur, Umwelt, Presserecht, Rundfunkgebühren
BEREICH INFORMATIK	
App. 400	Dipl.-Informatiker **Hanns-Wilhelm Heibey**, Bereichsleiter, Vertreter des BlnBDI als Dienststellenleiter und für den Bereich Q: Recht und Politik der Informationstechnik (u. a. Datenverarbeitung im Auftrag), Landesübergreifende Infrastrukturprojekte außer Netze, Elektronische Zahlungssysteme, Organisation von Rechenzentren, Proprietäre Betriebssysteme, Chipkarten, Koordination bei komplexen Beratungs- und Kontrollprojekten
App. 402	Sekretariat, Dienstreisen im Bereich Informatik und Recht, Erstellung und Pflege von Verteilerlisten
App. 408	Q: Berliner Landesnetz, Telekommunikationssysteme R: Inneres (außer Standesämter) I: Systemkoordination
App. 405	Q: Beratung der behördlichen und betrieblichen Datenschutzbeauftragten, Koordination der Kontrollen im privaten Bereich, Organisation des Datenschutzes, Unterrichtung nach § 24 Abs. 3 Satz 3 BlnDSG, Nichtautomatisierte Datenverarbeitung, Führung des Registers nach §§ 4d, 4e BDSG R: Verfassungsorgane, Senatskanzlei, Justiz, Betriebe, Finanzen, Wirtschaft I: Behördlicher Datenschutzbeauftragter
App. 404	Q: Datenschutz und IT-Sicherheit im Internet R: Schule, Bildung, Wissenschaft, Forschung

App. 411	Q: Informationstechnik im Gesundheitswesen, Kryptographie, Anonymisierung, Pseudonymisierung, Normung R: Gesundheitswesen
App. 406	Q: Microsoft-Betriebssysteme, Bürosysteme, Lokale Netze (u. a. kabellos), Mobile Computer R: Stadtentwicklung, Verkehr I: Informatik-Bibliothek, Virenschutzbeauftragter des Hauses
App. 407	Q: UNIX, LINUX, SAP R/3, Firewalls, Wartung und Fernwartung, Personalinformationssysteme R: Soziales, Inneres (Standesämter), Arbeit, Jugend I: IT-Haushalt
App. 410	Q: Biometrie, Überwachungssysteme (z. B. Videoüberwachung), Ubiquitous Technologies (u. a. RFID), Grundsatzfragen R: Kultur, Sport
App. 409	I: Systemverwaltung und Benutzerbetreuung, Anwendungsprogrammierung, Webmaster, TK-Anlage
Agenda:	AG= Arbeitsgebiet, Q = Querschnittszuständigkeit R = Ressortzuständigkeit, I = Interne Aufgaben

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

Veröffentlichungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte: Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über seine Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Seit 1990 wird der Tätigkeitsbericht von uns auch als Bürgerbroschüre veröffentlicht.

Dokumente zu Datenschutz und Informationsfreiheit: Die Bände dieser Schriftenreihe erscheinen jährlich als Anlage zu unseren Tätigkeitsberichten. Sie enthalten die bedeutsamen Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen des genannten Jahres.

Berliner Informationsgesetzbuch (BlnInfGB): In dieser Textsammlung werden von uns seit 1993 die wichtigsten datenschutzrechtlichen Regelungen für das Land Berlin herausgegeben. Derzeit sind folgende Bände aus dem Jahr 2008 verfügbar:
– Berliner Datenschutzgesetz
– Berliner Informationsfreiheitsgesetz, Bundesinformationsfreiheitsgesetz

Ratgeber zum Datenschutz: In dieser Reihe haben wir praktische Informationen zu einzelnen Fragen im Alltag zusammengestellt, die die Betroffenen in die Lage versetzen sollen, ihre Datenschutzrechte bzw. ihr Recht auf Informationsfreiheit eigenständig wahrzunehmen.

Hinweise zum Datenschutz: Während unserer Beratungen werden wir vielfach von Betroffenen oder Daten verarbeitenden Stellen um Hilfe oder Empfehlungen im Umgang mit personenbezogenen Daten gebeten. Einige unserer datenschutzrechtlichen Hinweise zu Standardproblemen sind als Veröffentlichungen erschienen.

Welche Broschüren wir im Einzelnen veröffentlicht haben, können Sie einer Übersicht auf unserer Website www.datenschutz-berlin.de entnehmen. Den überwiegenden Teil unserer Broschüren haben wir dort für Sie auch zum Download bereitgestellt. Eine Bestellung per Post ist gegen Einsendung eines an Sie selbst adressierten und mit 0,85 Euro frankierten DIN-A5-Umschlages möglich.

www.datenschutz-berlin.de

Datenmafia, Call-Center und Unschuldslämmer • Soziale Netzwerke – die Illusion der Intimität • Wartung und Fernwartung von informationstechnischen Systemen • Videoüberwachung – Big Brother überall? • Reform des Personenstandsrechts – Familienforscher atmen auf • Namensvetter in der Fluggäste-Datei • Fotoabgleich bei Verkehrsverstößen • Holpriger Start für die bundeseinheitliche Steuer-Identifikationsnummer • Kinderschutzgesetz: Eltern unter Generalverdacht? • Online-Gesundheitsakten • Praxisaufgabe oder Praxisübergabe – Wohin mit den Patientenakten? • Google Street View • Videoeinsatz bei der Evaluierung der Umweltzone • Intelligente Stromzähler • „Mein" Genom im Internet • Befragung über Unterrichtsstörer • Rasterung auf Zuruf – Deutsche Telekom und Deutsche Bahn • Überraschende Abbuchungen • Alles aus einer Hand? – Der „Einheitliche Ansprechpartner" nach der EU-Dienstleistungsrichtlinie • Aktenfund bei einem Elektronik-Discounter • Bewertungsportale im Internet • Smiley-System im Bezirk Pankow – ein gutes Pilotprojekt