Berliner Beauftragter für
Datenschutz und Informationsfreiheit


# Datenschutz und Informationsfreiheit

## Bericht 2009

Berlin

# BERICHT

## des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2009

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 **29. April 2009** vorgelegten Jahresbericht 2008 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2009 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2009“) veröffentlicht.

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

## Impressum


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

# Inhaltsverzeichnis

# Einleitung

2009 hat der Datenschutz erheblich an Bedeutung gewonnen. Nachdem das ganze Ausmaß der massiven unzulässigen Überwachung von Beschäftigten und Außenstehenden bei der Deutschen Bahn bekannt geworden war, trat der Vorstandsvorsitzende des Unternehmens zurück. Nach Abschluss unserer Überprüfung dieser Vorgänge haben wir ein Bußgeld in Höhe von 1.123.503,50 Euro gegen das Unternehmen verhängt[1]. Dies ist das höchste Bußgeld, das eine deutsche Aufsichtsbehörde für den Datenschutz bisher festgesetzt hat. Der neue Unternehmensvorstand hat nicht nur die Geldbuße akzeptiert und bezahlt, sondern darüber hinaus den Datenschutz zu einer seiner obersten Prioritäten erklärt. Der Datenschutz ist jetzt auf höchster Ebene in einem eigenen Vorstandsressort angesiedelt. Das Unternehmen hat sich zum Ziel gesetzt, nicht nur die vorgeschriebenen Maßnahmen gegen künftige datenschutzrechtliche Verstöße zu treffen, sondern darüber hinaus in Sachen Datenschutz eine Modellfunktion zu übernehmen. Wenn die Deutsche Bahn als wohl größter privater Arbeitgeber in Deutschland die Ankündigung wahrmacht, beim Schutz der Beschäftigtendaten neue, positive Maßstäbe zu setzen, so hätte dies Auswirkungen auf die gesamte Berliner und darüber hinaus auf die Wirtschaft und Verwaltung in ganz Deutschland.

Diese Änderung der Unternehmenskultur ist die richtige Konsequenz aus einer beschämenden Praxis der Überwachung von Beschäftigten und Dritten in der Vergangenheit. Die Zahlung der hohen Geldbuße tritt daneben in den Hintergrund, ist aber ein wichtiges Signal. In Zukunft kann sich kein Unternehmensvorstand mehr leisten, den Datenschutz zu unterschätzen.

Wir geben uns allerdings nicht der Illusion hin, dass allein mit Hilfe von Bußgeldbescheiden die „Datenschutz-Welt“ in Ordnung gebracht werden kann. Das zeigen Äußerungen von führenden Vertretern amerikanischer Internet-Unternehmen. So hat der Chef von Google, Eric Schmidt, in schöner Offenheit gesagt: „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht gar nicht erst tun.“ Aus diesem Satz spricht nicht nur eine erschreckende Anmaßung, sondern er beschreibt präzise,

1 Vgl. 10.1

was der Kern des Datenschutzes ist: Wenn es nach Google (und anderen Unternehmen) geht, sollte kein Mensch mehr irgendwelche Geheimnisse vor irgendwem haben. Er sollte sich so verhalten, dass alle es wissen können (denn mit Hilfe von Google werden alle es wissen). In einer solchen Gesellschaft will aber niemand leben. Datenschutz im Internet und in der realen Welt ist die Voraussetzung dafür, dass wir uns frei bewegen können. Datenschutz schützt keine Daten, sondern das Grundrecht jedes einzelnen Menschen auf Verhaltensfreiheit. Verhaltensfreiheit gibt es nur, wenn jeder selbst entscheidet, was mit seinen Daten geschieht.

Die Hoffnung, dass der Gesetzgeber in Deutschland die richtigen Konsequenzen aus den Datenskandalen der zurückliegenden Zeit ziehen würde, hat sich leider nicht erfüllt. Für eine umfassende Modernisierung war vor dem Ende der letzten Legislaturperiode keine Zeit mehr. Die punktuellen Änderungen im Bundesdatenschutzgesetz haben zwar kleine Fortschritte gebracht, aber ihrerseits neue Fragen für die Praxis aufgeworfen[2]. Die umfassende Neuordnung des Datenschutzrechts und seiner Ausrichtung auf die Informationsgesellschaft des 21. Jahrhunderts ist eine Aufgabe, der sich der Gesetzgeber jetzt stellen muss. Der Beschäftigtendatenschutz sollte dabei in einem eigenen Gesetz verankert und nicht länger im Bundesdatenschutzgesetz versteckt werden. Die Datenschutzbeauftragten werden zur Neuordnung des Datenschutzrechts in Kürze Vorschläge vorlegen.

Trotz der gravierenden verfassungsrechtlichen Einwände, die die Datenschutzbeauftragten schon 2008 erhoben hatten, ist das Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) im April in Kraft getreten[3]. Damit entsteht seit dem 1. Januar 2010 erstmals eine zentrale Datei aller Beschäftigten in Deutschland, obwohl nur für einen Bruchteil von ihnen diese Speicherung erforderlich ist. Denn aus dieser Datenbank sollen Entgeltbescheinigungen für die Rentenversicherung, die Finanzämter und Arbeitsagenturen abgerufen werden können, wenn die betroffene Person solche Bescheinigungen benötigt. Die beabsichtigte Entlastung der Arbeitgeber von der Ausstellung der nötigen Bescheinigungen im Einzelfall rechtfertigt eine solche zentrale Vorratsdatenspeicherung nicht. Erst kurz vor der Einrichtung dieser

2 Vgl. 2.1

3 BGBl. I 2009, S. 634

Datenbank wurde das ganze Ausmaß dieser verfassungsrechtlich problematischen Datenbank öffentlich kontrovers diskutiert, nachdem bekannt geworden war, dass auch an die Speicherung von so sensitiven Beschäftigtendaten wie Abmahnungen, Kündigungsgründen und der Beteiligung an Arbeitskampfmaßnahmen gedacht war. Es ist zu hoffen, dass die bevorstehende Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung in der Telekommunikation dem Bundesgesetzgeber auch Hinweise dafür geben wird, welche Korrekturen am ELENA-Verfahrensgesetz notwendig sind.

Steuerhinterziehung ist eine Straftat, die verfolgt werden muss. Über die Frage, mit welchen Mitteln dies geschehen darf, wird nicht erst seit 2007 diskutiert. Damals kaufte der Bundesnachrichtendienst von einem Informanten Datenträger mit Informationen über mutmaßliche deutsche Steuerhinterzieher an, die ihr Geld „schwarz“ in Liechtenstein angelegt hatten. Diese Daten führten zu zahlreichen Steuerstrafverfahren. Auf den Datenträgern fanden sich allerdings auch Daten über steuerehrliche Bürgerinnen und Bürger, wie die Ermittlungen ergaben. Bevor das angerufene Bundesverfassungsgericht über die Rechtmäßigkeit dieser Datenerhebung und -verwertung entscheiden konnte, hat eine Landesregierung mit Rückendeckung der Bundesregierung weitere Datenträger mit Kontoinformationen Schweizer Banken über deutsche Kundinnen und Kunden angekauft, die Steuern hinterzogen haben sollen. Dieses Vorgehen wirft Fragen auf, die weit über die Bedeutung des Bankgeheimnisses hinausgehen. In einem Rechtsstaat dürfen Straftaten nur mit rechtsstaatlichen Mitteln verfolgt werden. Der regierungsamtliche Ankauf von Daten, die jedenfalls in rechtswidriger, möglicherweise oder sogar strafbarer Weise erlangt wurden, gehört nicht dazu. Der Staat erschüttert dadurch vielmehr das Vertrauen der Menschen in die Beachtung von Geheimhaltungsbestimmungen – auch zum Schutz personenbezogener Daten –, deren Bruch mit Strafe bedroht ist. Eine geradezu groteske Wendung nimmt die ganze Angelegenheit, wenn die Senatsverwaltung für Finanzen nach Presseberichten Auskünfte über die Höhe der insgesamt in Berlin aufgrund von Selbstanzeigen zu erwartenden Steuernachzahlungen mit Hinweis auf das „Steuergeheimnis“ ablehnt[4].

Auch ein weiteres Beispiel belegt, dass Informationsfreiheit noch immer keine Selbstverständlichkeit ist. Dass dies gerade auch in Zeiten der Terrorismusbe-

4 Berliner Zeitung vom 9. Februar 2010

kämpfung gilt, macht eine Entscheidung des Europäischen Gerichtshofs vom März deutlich[5]. Er gab einem Flugpassagier recht, den die Sicherheitsbehörden beim Check-in aufgefordert hatten, einen Tennisschläger aus seinem Handgepäck zu entfernen, der als gefährlicher Gegenstand nach europäischen Bestimmungen angesehen wurde. Auf die Frage des Passagiers, auf welche Rechtsgrundlage sich diese Maßnahme stütze, wurde ihm unter Hinweis auf die Geheimhaltung eine Antwort verweigert. Tatsächlich war der entsprechende Anhang zu einer EU-Verordnung nicht im Amtsblatt der Europäischen Union veröffentlicht worden. Dass ein Bürger, der sich an geheim gehaltene europäische Bestimmungen halten soll, vier Jahre lang bis zum Europäischen Gerichtshof prozessieren muss, um die Unzulässigkeit eines solchen Vorgehens bescheinigt zu bekommen, gibt allerdings zu denken.

5 Rechtssache C-345/06

# 1. Technische Rahmenbedingungen

## 1.1 Entwicklung der Informationstechnik

### 1.1.1 Intelligente Stromnetze – Smart Grids

**Was intelligente Stromnetze können sollen**

Im vorigen Jahr berichteten wir über intelligente Stromzähler, die sog. Smart Meters, weil der Stromversorger Vattenfall in Berliner Wohnanlagen solche Stromzähler erproben wollte, die den Anforderungen des neuen Energiewirtschaftsgesetzes genügen sollen[1]. Dabei geht es um Zähler, die – sofern technisch machbar und wirtschaftlich zumutbar – ab 30. Dezember 2009 in Neubauten und bei größeren Renovierungen einzubauen sind. Sie zeigen den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit an, können also wesentlich mehr verbrauchsbezogene Daten offenbaren als die bis heute eingesetzten sog. Ferraris-Zähler. Den übrigen Kundinnen und Kunden sollen diese Zähler zum freiwilligen Einbau angeboten werden. Des Weiteren sollen die Energieversorgungsunternehmen bis Ende 2010 den Verbraucherinnen und Verbrauchern einen Tarif anbieten, bei dem Anreize zur Energieeinsparung oder zur Steuerung des Energieverbrauchs durch die Wahl neuer Tarife gegeben werden sollen. Die neuen Zähler müssen diese Tarife abbilden können und die für die Tariffindung relevanten Verbrauchsdaten liefern. Wir kommen am Ende dieses Abschnitts auf die Weiterführung der Diskussion um die datenschutzgerechte Gestaltung der intelligenten Stromzähler zurück.

Die intelligenten Stromzähler sind jedoch eine erste konkrete Komponente der wesentlich umfassenderen Vision von intelligenten Stromnetzen (Smart Grids), über die inzwischen eine weltweite Diskussion eingesetzt hat. Die Befassung mit dem Thema bewirkt teilweise euphorische Vorhersagen über die segensreichen Auswirkungen des „Internets der Energie“ auf die Rettung der Umwelt durch Reduktion der Treibhausgase, die Einsparung von Energie, die Verbesserung der Versorgungssicherheit und auf die Generierung neuer Märkte, neuer

1 JB 2008, 8.4.3

Marktrollen und neuer Geschäftsmodelle. Es geht um nichts weniger als um die Überführung der größten Maschine der Welt, des alten, störungsanfälligen und den modernen Anforderungen nicht mehr gewachsenen weltweiten Stromnetzes, durch die Konvergenz[2] mit der Informations- und Kommunikationstechnologie in das digitale Zeitalter – wenn man so will, mit der zweitgrößten Maschine der Welt, dem Internet.

Die Verbraucherinnen und Verbraucher sollen ebenfalls von der Intelligenz der Stromnetze profitieren: Sie sollen über ihren täglichen Stromverbrauch informiert werden, möglichst sogar differenziert nach den Strom verbrauchenden Geräten im Haushalt, damit sie entscheiden können, wie und wann sie wie viel Strom verbrauchen, und somit ihr Verbrauchsverhalten besser steuern können. Unterstützt werden sie dabei durch das Angebot zeit- oder lastabhängiger Tarife, wie sie bereits ab 2011 europaweit anzubieten sind. Das Energiewirtschaftsgesetz macht da noch keine genaueren Vorgaben, aber die Planer des Smart Grid gehen soweit, dass vielleicht sogar jedem Haushalt ein Individualtarif angeboten wird, der auf der Grundlage des individuellen Verbrauchsverhaltens optimiert wird.

Es geht aber nicht nur um die flexible oder gar individuelle Steuerung des Verbrauchsverhaltens durch die Ausnutzung günstiger oder Meidung ungünstiger Tarifzeiten. Es geht auch um das intelligente Management des jeweils aktuellen Stromverbrauchs im Verhältnis zur aktuellen Stromerzeugung. Grundsätzlich muss dem Netz der Strom abgenommen werden, der gerade erzeugt wird. Da mit dem Aufkommen erneuerbarer Energiequellen die Stromerzeugung nicht nur von der Steuerung der Kraftwerke, sondern auch vom Wetter (z. B. Wind, Sonnenschein) abhängt, werden auch alle Möglichkeiten zur Speicherung elektrischer Energie bei zu hoher Erzeugung oder zur Zuführung von Energie, etwa durch kleine Blockheizkraftwerke, in Betracht gezogen. Die Speicherung von Energie kann z. B. dadurch geschehen, dass Kühlhäuser, später vielleicht auch Haushaltsgefriergeräte, in Zeiten erhöhten Stromangebots unter Ausnutzung günstigerer Tarife tiefere Temperaturen des Gefrierguts erzeugen, um es dann in Zeiten teureren Stroms bis zum Erreichen der Mindesttemperatur wieder aufwärmen zu lassen und so Kosten zu sparen. Weitere Speicher werden in den Elektrofahrzeugen gesehen, die Strom aus dem Netz zu günstigen

2 JB 2007, 1.1

Zeiten „tanken“ und vom Stromnetz unabhängig verbrauchen. Gedacht wird auch daran, gespeicherte Energie in das öffentliche Stromnetz zurückfließen zu lassen und dadurch den Strompreis zu beeinflussen.

Die Technologie-Förderungsinitiative E-Energy des Bundesministeriums für Wirtschaft und Technologie befasst sich mit diesen Zukunftsthemen[3]. Das Ministerium fördert im Zusammenwirken mit dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit sechs Projekte in Modellregionen:

- In der Modellregion Cuxhaven befasst sich das Projekt eTelligence mit der Zusammenführung von Stromerzeugern, Verbrauchern, Energiedienstleistern und Netzbetreibern auf einem innovativen Energiemarktplatz. Der Stromverbrauch von Industrie, Gewerbe und Privathaushalten soll auf die Stromerzeugung aus dezentralen Quellen, vor allem aus der in Norddeutschland relevanten Windenergie, abgestimmt werden. Das oben beschriebene Kühlhaus-Beispiel gilt für dieses Modellprojekt.
- Das Projekt Meregio (Minimum Emission Regions) befasst sich im Großraum Karlsruhe/Stuttgart mit der Entwicklung eines Zertifikats für solche Regionen und führt beispielhafte Zertifizierungen durch. Gleichzeitig werden die Regionen beraten, wie die Energieeffizienz verbessert werden kann. Das im Rahmen des Projekts konzipierte Modellhaus erzeugt selbst Energie durch Sonnenkollektoren auf dem Dach oder einem Kleinst-Blockheizkraftwerk. Systeme zur Gebäudeautomatisierung kontrollieren die elektrischen Anlagen des Hauses und sorgen für die Gebäudesicherheit. Das in der Garage stehende Elektrofahrzeug nimmt überschüssige Energie auf, wenn die Stromerzeugungssysteme des Hauses mehr Elektrizität erzeugen, als das Netz aufnehmen kann. Die Verbraucherinnen und Verbraucher können über ein Internetportal die Vorgänge im System beobachten und steuern.

- Das Projekt Modellstadt Mannheim zielt auf die Steigerung der Energieeffizienz durch einen virtuellen Markt für Energieerzeuger, -verbraucher und -netzbetreiber. Auf diesem Markt kann jeder Herkunft und Preis seines Stroms erkennen und durch die Steuerung von Energiebezügen und Energieeinspeisungen aus eigenen dezentralen Stromerzeugern direkt da-

3 www.e-energy.de

rauf Einfluss nehmen. Grundlage dafür ist die Entwicklung einer informationstechnischen Vernetzung des Stromnetzes mit Breitband-Powerline[4] für eine Echtzeitkommunikation zwischen Erzeugern sowie Verbraucherinnen und Verbrauchern auf der Grundlage des Internet-Protokolls.

- Das Projekt E-DeMa in der Modellregion Rhein-Ruhr soll neben einem Energiemarktplatz Mechanismen entwickeln, mit denen ein automatisierter Ablauf zwischen Erzeugern sowie Verbraucherinnen und Verbrauchern ermöglicht wird. Diese können damit ihren Verbrauch reduzieren und auf Zeiten verlagern, in denen genug billiger Strom zur Verfügung steht. Die in der Region vorhandene Ausbreitung digitaler Stromzähler ermöglicht die Entwicklung einer Verbrauchssteuerung aufgrund einer zeitnahen Verbrauchsdatenerfassung und -bereitstellung.
- Das Projekt der Regenerativen Modellregion Harz (RegModHarz) befasst sich primär mit der Elektromobilität. Es werden mehrere Fahrzeuge dazu umgerüstet, dass sie Energie sowohl aus dem Netz aufladen als auch umgekehrt wieder einspeisen können. Es wird untersucht, ob die Fahrzeuge auch zum Lastmanagement genutzt werden können, indem sie in Zeiten des günstigen Angebots geladen werden und bei Bedarf Energie wieder in das Netz zurückgegeben werden kann.
- Das Projekt Smart Watts in der Modellregion Aachen verfolgt das Konzept der „intelligenten Kilowattstunde". Die Lieferung der Energie an die Haushalte ist dabei gekoppelt mit Angaben zur Herkunft, zum Weg der Lieferung und zum aktuellen Preis. Dabei wird der Verbrauch zeitbezogen genau erfasst, und durch den Transport von Steuerungsinformationen innerhalb des Stromnetzes wird eine genaue Abrechnung ermöglicht.

Diese Projekte zeigen die Vielfalt der Ideen, die bereits heute im Zusammenhang mit dem Smart Grid in Deutschland verfolgt werden. Sie zeigen aber auch, dass die Projekte zum Teil detaillierte Verbrauchsdaten aus den Haushalten abfragen wollen oder müssen.

4 Powerline = Verwendung des Stromnetzes zur Übertragung von digitalen Daten

### Datenschutz bei Smart Grids

„Wir müssen stark aufpassen, dass der Datenschutz für die Verbraucher nicht in einer Atmosphäre der ungezügelten Begeisterung für die Reform des Elektrizitätswesens geopfert wird.“[5] Diese Aussage von Ann Cavoukian, der Informations- und Datenschutzbeauftragten der kanadischen Provinz Ontario, beschreibt auch die Angst einiger wissenschaftlicher Begleitforscher der deutschen E-Energy-Initiative, die Datenschutzbeauftragten könnten zu Hemmschuhen der Entwicklung werden. Der Datenschutz möge nicht blockieren, er möge den Schritt ins digitale Zeitalter mitmachen, so die Stimmen in einer Arbeitsgruppe der Initiative, die sich mit den rechtlichen Fragen von E-Energy befasst und zu der wir eingeladen waren.

In der Tat bedürfen die Smart Grids intensiver datenschutzrechtlicher Beobachtung. Wenn – wie vorgesehen – der Stromverbrauch in jedem einzelnen Haushalt in kurzen Zeitintervallen, z. B. alle 15 Minuten, erfasst werden soll, um einerseits zum Stromsparen zu animieren und andererseits individuelle Tarife anzubieten, so entstehen detaillierte Verhaltensprofile, die die Gewohnheiten der Bewohnerinnen und Bewohner beim Gebrauch ihrer Wohnung und der in ihnen befindlichen elektrischen Geräte ziemlich genau abbilden können: Wann wird Licht an oder ausgemacht, wird elektrisch geheizt und wie wird das gesteuert, wird elektrisch gekocht, gibt es eine Mikrowelle, wann wird Warmwasser verbraucht, also geduscht oder gebadet, gibt es eine Alarmanlage und wann ist diese ausgeschaltet, wie oft läuft die Waschmaschine oder die Geschirrspülmaschine? Dies sind alles Beispiele für Informationen, deren Nachaußendringen die nach Art. 13 Grundgesetz garantierte Unverletzlichkeit der Wohnung tangiert. Soll das der Preis für die intelligente Steuerung der Stromverteilung und des Stromverbrauchs sein?

Solange es nur darum geht, den Bewohnerinnen und Bewohnern selbst detaillierte Informationen zu ihrem Stromverbrauch zu liefern, könnte man sich Inhouse-Lösungen vorstellen, die die gemessenen Daten für den heimischen Computer aufbereiten und darstellbar machen. Wenn jedoch die zeit- oder

5 „We must take great care not to sacrifice consumer privacy amidst an atmosphere of unbridled enthusiasm for electricity reform”, zitiert aus A. Cavoukian, J. Polonetsky, C. Wolf: SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, November 2009, http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf

lastabhängigen Tarife bis auf Haushaltsebene differenziert ausgestaltet werden sollen, dann werden diese Daten nicht in der Wohnung verbleiben können, sondern zur Tarifgestaltung durch den Stromerzeuger verwendet werden müssen.

Hier stellt sich die Frage, ob eine so hochaufgelöste und differenzierte Erfassung der Verbrauchsdaten für jeden Haushalt für das Erreichen der Energiesparziele überhaupt notwendig ist bzw. welche Abweichung von der Auflösung und Differenziertheit akzeptiert werden muss, um nicht mit elementaren Persönlichkeitsrechten in Konflikt zu kommen. Reicht nicht eine weniger differenzierte Erfassung aus, die keinen Rückschluss auf Einzelhaushalte mehr erlaubt, um die anspruchsvollen Energiesparziele zu erreichen?

Diese Fragen sind auch vor dem Hintergrund zu stellen, dass Daten, die differenzierte Verhaltensprofile von Wohnungsnutzenden ergeben, erhebliche Begehrlichkeiten wecken werden. Mögliche Interessenten sind Kriminelle, aber auch Strafverfolgungsbehörden oder Unternehmen, die solche Informationen gewinnbringend nutzen wollen.

Es geht also nicht darum, technische Entwicklungen zu blockieren, sondern den Prinzipien der strikten Datensparsamkeit und der Datenvermeidung, die im deutschen Datenschutzrecht verankert sind[6], auch bei Smart Grids Geltung zu verschaffen.

### Datenschutz beim Smart Metering

Die eingangs erwähnten Smart Meters, also intelligenten Stromzähler, sind der Einstieg in die Entwicklung der Smart Grids. Während die Smart Grids noch Zukunftsmusik darstellen, für die es allerdings bereits erste Pilotprojekte im Rahmen der E-Energy-Initiative gibt, sind seit Ende 2009 nach § 21 b Energiewirtschaftsgesetz (EnWG) die Messstellenbetreiber verpflichtet, in Neubauten und bei größeren Renovierungen Messstellen einzubauen, die den Nutzerinnen und Nutzern wesentlich differenziertere Verbrauchsdaten anzeigen können, damit sie ihr Verbrauchsverhalten selbst besser steuern können. Soweit sie von der Einbaupflicht betroffen sind, fehlt ihnen dazu die Alternative. Alle anderen können vom Pflichtangebot des Messstellenbetreibers Gebrauch machen, sich ebenfalls solche Zähler einbauen zu lassen.

6 Z. B. § 3 a BDSG, § 5 a BlnDSG

Da die Messstellen, die den Anforderungen des § 21 b EnWG entsprechen, wesentlich mehr Verbrauchsdaten des Haushalts anzeigen, besteht bei ihnen ein höherer datenschutzrechtlicher Schutzbedarf als bei den alten sog. Ferraris-Zählern, die nur den Gesamtverbrauch seit Zählerinbetriebsetzung in digitaler Form und den aktuellen Verbrauch in schwer interpretierbarer analoger Form anzeigen. Aus diesem Grunde müssen technische und organisatorische Maßnahmen nach § 9 BDSG ergriffen werden, um die Kenntnisnahme der angezeigten Daten durch Unbefugte zu verhindern. Sind die Zähler in der Wohnung eingebaut, liegt eine hinreichende Zutrittskontrolle vor, die verhindert, dass Unbefugte sich die Verbrauchsdaten verschaffen. Sind die Zähler jedoch im öffentlich zugänglichen Bereich oder - wie in vielen Wohnanlagen - gesammelt in einem gesonderten Raum untergebracht, zu dem viele Personen Zutritt haben, müssen Maßnahmen der Zugangskontrolle nach Nr. 2 der Anlage zu § 9 Satz 1 BDSG getroffen werden. Es muss also verhindert werden, dass Personen, die den Zählerraum betreten können, die Daten der Zähler unbefugt auslesen können.

Solche Maßnahmen könnten z. B. Klappen vor dem Display des Zählers sein, die mit einem individuellen Schlüssel ausgestattet sind. Auch die Abfrage eines PIN-Codes oder die Verwendung eines maschinenlesbaren Ausweises wären mögliche, allerdings teurere Maßnahmen.

Darüber hinaus sind Maßnahmen zu treffen, die die Datensicherheit bei der Übermittlung der Messergebnisse sicherstellen. Bei allen Übertragungen der Messdaten aus der Wohnung oder in die Wohnung ist entweder die Anonymisierung oder die Pseudonymisierung der Daten erforderlich. Anderenfalls müssen kryptographische Verschlüsselungsverfahren eingesetzt werden.

Weitere datenschutzrechtliche Anforderungen beim Einsatz intelligenter Stromzähler betreffen die Transparenz der Messverfahren und der Datenübermittlungen für den Anschlussinhaber. Die Ablesezeitpunkte und Ableseintervalle sind daher mit den Betroffenen vertraglich zu vereinbaren. Weitere Angebote, die über die gesetzlichen Anforderungen hinaus gehen, müssen gesondert vertraglich geregelt werden. Dies gilt insbesondere dann, wenn Lastprofile bei Messungen mit kurzen Intervallen auf zentrale Rechner übertragen werden sollen, damit die Betroffenen sie über das Internet abrufen können.

## 1.1.2 Aktuelle informationstechnische Trends

Dass die Informations- und Kommunikationstechnik sich permanent weiterentwickelt, ist eine Binsenweisheit. Teilweise überraschend sind die unterschiedlichen Richtungen der Entwicklung. 2008 thematisierten wir erstmals das „Cloud-Computing“[7], ein Geschäftsmodell zur Auftragsdatenverarbeitung in den unendlichen und unbekannten Weiten des grafisch immer als Wolke dargestellten Internets, und deuteten die Konsequenzen an, die solche Dienstangebote für die Kontrollierbarkeit und Beherrschbarkeit, damit für die Sicherheit der Datenverarbeitung haben können. Derzeit gibt es kaum eine Ausgabe der einschlägigen Fachzeitschriften, die ohne ausführliche Erörterungen zum Cloud Computing auskommt.

In diesem Jahr befassten wir uns nicht mit einem neuen Dienstleistungsmodell für die Datenverarbeitung, sondern mit einem relativ isolierten Anwendungsbereich, nämlich der flexiblen Steuerung von Stromnetzen in der Weise, dass Anreize zur Energieeinsparung und permanente Anpassung des Verbrauchs an das Ausmaß der jeweils aktuellen Stromerzeugung geschaffen werden. Der Datenschutz muss sich mit dem scheinbaren Bedarf an permanenter Verfolgung des Energieverbrauchsverhaltens einzelner namentlich identifizierbarer Privathaushalte auseinandersetzen. Auch hier ist ein medialer Hype zu beobachten, nicht zuletzt wegen der partiellen Verpflichtung zum Einbau von Smart Meters. Dass das Interesse jedoch nicht kurzlebig sein dürfte, zeigt das Interesse des US-Unternehmens Google, am Thema Smart Grids mitzuwirken. Mit Google PowerMeter erfolgt gegenwärtig in den USA der Einstieg bei der Visualisierung von Verbrauchsdaten beim Endkunden, sofern dieser bereits einen Smart Meter einsetzt. Mit diesem Dienst sammelt Google sowohl Verbrauchs- als auch Nutzungsdaten (IP-Adressen). Weitere Entwicklungen in den nächsten Jahren zeichnen sich bereits ab:

- Die 2007 als Motor der Entwicklung der Datenverarbeitung behandelte Konvergenz der Informations- und Kommunikationstechnologien[8] erfasst jetzt Mobiltelefone und Computer. Nachdem zunächst mit dem Blackberry die Konvergenz von Mobiltelefonie und E-Mail-Kommunikation erfolg-

7 JB 2008, 1.1.1
8 JB 2007, 1.1

reich durchgeführt wurde, zeigen die **Smartphones**, allen voran das iPhone von Apple, dass es noch weiter geht in Richtung umfassendes Computing.

- Das bereits beschriebene Cloud Computing ist selbst Ausgangspunkt für weitere Konvergenzen: Bekannt ist seit langem, dass weltweit operierende Unternehmen – vor allem der IT-Branche – ihre IT-Kapazitäten dort, wo aktuell dem Tagesgeschäft nachgegangen wird, dadurch optimieren, dass sie ihre IT-Kapazitäten in Rechenzentren der Unternehmen in Regionen mitnutzen, in denen nächtliche „Ruhe" herrscht. Dieses **„Follow-the-Sun-Computing"** verlässt jetzt die Unternehmensgrenzen, indem Firmen Auftragsdatenverarbeitung in weltweit verteilten Data Centers nach dem Follow-the-Sun-Prinzip anbieten. Die Datenverarbeitung hat dann keinen festen Ort, sondern „folgt der Sonne" in der Cloud. Problematisch wird dies vor allem dann, wenn auch die Verantwortung für die Datenverarbeitung verlagert und nationales Datenschutzrecht umgangen wird[9].
- Die Verarbeitung von **Geodaten** dient längst nicht mehr nur der Befriedigung der Neugierde von Google Earth- und Google Street View-Nutzenden, sondern spielt in vielen Wirtschaftsbereichen, bei der Vorhersage von Naturkatastrophen, im Umweltschutz, den Geowissenschaften einschließlich der Meteorologie und der Archäologie und vielen anderen Zusammenhängen eine wesentliche Rolle. Das starke Interesse an der wirtschaftlichen Nutzung der Geodaten entfacht auch die Diskussion um die datenschutzrechtliche Relevanz dieser Daten. So verneinen Geodatenvermarkter das Vorhandensein von Personenbezug[10], um Geodaten ganz aus dem Anwendungsbereich der Datenschutzgesetze herauszunehmen, während von Datenschützern gerade die Möglichkeit des Personenbezugs betont wird[11].

Die Steuerung von Computern wird nicht länger auf die Nutzung von Tastaturen und Mäusen beschränkt sein. Die Eingabe solcher Steuerungssignale wird bald auch mit der Stimme oder mit Gesten erfolgen können. Ob dies datenschutzrechtliche Bedeutung erlangen wird, bleibt abzuwarten. Mit Sicherheit

9 Nur in diesem Fall (etwa bei einer global wandernden Systemadministration) trifft der Begriff „follow the sun" zu. Werden dagegen nur Rechnerkapazitäten an Orten genutzt, wo nicht gearbeitet wird, ist eher die Bezeichnung „follow the moon" zutreffend.

10 M. Herter (infas GEOdaten): Geodaten sind nicht persönlich, http://www.infas-geodaten.de/fileadmin/media/pdf/presse/2008015_PI_Datenschutz_II.pdf

11 M. Karg (ULD Schleswig-Holstein): Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten für die Wirtschaft, https://www.datenschutzzentrum.de/geodaten/datenschutzrechtliche-rahmenbedingungen-bereitstellung-geodaten.pdf

muss das Problem, dass Computer akustische oder optische Signale missverstehen können, gelöst werden. Ob die Spracherkennung zu einem zuverlässigen Mittel der biometrischen Zugriffskontrolle wird, ist noch nicht abzusehen.

## 1.2. Datenverarbeitung in der Berliner Verwaltung

### 1.2.1 IT-Politik

Die Ziele der IT-Politik des Landes Berlin sind weiterhin darauf ausgerichtet, die Berliner Verwaltung fit für das sog. eGovernment zu machen. Den Bürgerinnen und Bürgern sollen über kurz oder lang elektronische Dienstleistungen angeboten werden, die es ihnen ermöglichen, bestimmte Leistungsangebote der Verwaltung vom häuslichen Telefon oder vom heimischen Computer aus über das Internet in Anspruch zu nehmen. Diese Möglichkeit des „Fernzugriffs“ auf die Verwaltung soll nicht nur den Menschen in Berlin das Leben erleichtern, sondern ist auch die technische Voraussetzung für den Zugriff von Bürgerinnen und Bürgern aus der Europäischen Union zur Umsetzung ihrer Rechte nach der Europäischen Dienstleistungsrichtlinie[12].

Es kommt zum einen darauf an, moderne und bürgerfreundliche Kommunikationskanäle über Telefonnetz und Internet zwischen den Menschen und der Verwaltung zu schaffen, und zum anderen die IT-Strukturen des Landes zu modernisieren und soweit wie möglich zu vereinheitlichen. Insbesondere der Zugang über das Internet wird sich vermehrt dem Anspruch zu stellen haben, dass der Austausch von Dokumenten die jeweils erforderliche Verbindlichkeit erreicht. Ohne qualifizierte elektronische Signatur wird dies auf Dauer nicht gehen. Alle Kompromisslösungen unterhalb dieser Qualitätsschwelle werden nicht ausreichen, jedoch schwer zurückholbar sein, wenn sie einmal eingeführt sind.

12 Vgl. 10.9

Ein erster Meilenstein ist der Beginn der Pilotierung der **bundeseinheitlichen Behördenrufnummer 115** (D115) am 24. März 2009, an der neben Berlin diverse deutsche Städte teilnehmen. Für Berlin war dieser Einstieg relativ einfach, weil eine einheitliche Behördenrufnummer 900, das sog. Berlin-Telefon, bereits bestand. Der Leistungskatalog besteht aus der Auskunftserteilung zu einfachen inhaltlichen Fragen, aber auch zur Darstellung des behördlichen Leistungsangebots, zu Gebühren und den benötigten Unterlagen über zuständige Stellen und ihre örtliche und zeitliche Erreichbarkeit (Telefon, Fax, E-Mail), aus dem Versuch der Anrufweiterleitung an zuständige Stellen, aber auch der Aufnahme und Weitergabe von Anliegen. Die wichtigsten Leistungsangebote betreffen nach dem D115-Leistungskatalog: Pass- und Ausweisangelegenheiten, Fahrzeug- und Fahrerlaubnisangelegenheiten, das Personenstandswesen und Angelegenheiten zur Staatsangehörigkeit, Angelegenheiten des Bauwesens, des Gewerbes, der Tierhaltung einschließlich der Hundesteuer, des Straßenverkehrs sowie der sozialen Grundsicherung und Familienförderung.

Zur Rufnummer 115 wird versprochen, dass 75 % der Anrufe innerhalb von 30 Sekunden angenommen werden und 55 % (ab 2010 65 %) davon beim ersten Anruf beantwortet werden sollen. Kann ein Anruf nicht sofort beantwortet werden, erhält der Anrufer innerhalb von 24 Stunden während der Servicezeiten eine Rückmeldung über E-Mail, Fax oder Rückruf.

Rückgrat der Kommunikation innerhalb der Verwaltung waren bisher das Metrolipolitan Area Network (MAN) für die Datenkommunikation und ein optisches synchrones Zeitmultiplex-(SDH-)Kommunikationsnetz für die Telefonie. Mit dem neuen **Berliner Landesnetz der nächsten Generation** (BeLa NG) werden diese beiden Netze zusammengefasst, Daten- und Sprachkommunikation laufen über die gleichen Fasern.

Das BeLa NG wird für die Datenkommunikation stark erweiterte Kapazitäten bereithalten und sie damit beschleunigen. Der wesentliche Aspekt des Generationswechsels liegt jedoch in dem Angebot eines flexiblen Übergangs von der klassischen leitungsgebundenen Telefonie auf das Telefonieren über das Internet-Protokoll (Voice over IP – VoiP). Die Verwaltungen können innerhalb der Verwaltung VoiP nutzen. Sie benötigen dazu keine eigene Telefonanlage

mehr, sondern nutzen ein eigenes VPN[13], das von einem zentralen VoiP-Server im ITDZ gesteuert wird. Verwaltungen, die noch nicht auf das neue Protokoll umsteigen wollen, können ihre bestehenden TK-Anlagen weiter auf dem bestehenden SDH-Netz betreiben. Es ist möglich, zwischen den beiden Netzen zu kommunizieren.

Politisch ist beabsichtigt, auch die bisher vom BeLa getrennt geführten Glasfasernetze der Polizei und der Feuerwehr in das BeLa NG zu integrieren. Dies stieß insbesondere bei der Polizei auf Sicherheitsbedenken. Ob diese politische Absicht daher umgesetzt wird, ist noch offen.

Das sog. **IT-Servicemanagement** (ITSM) soll mit Maßnahmeangeboten und -methoden dazu führen, dass die IT-Organisation die Geschäftsprozesse der Verwaltung optimal unterstützt. Die IT wird im Erfolgsfall mit mehr Kunden- und Serviceorientierung ausgestattet. Sie wird stärker an die Bedürfnisse der Anwender angepasst und sieht die Rückkopplung mit diesen vor, die zu weiteren Anpassungen führen kann.

Für die Umsetzung eines ITSM stehen gesammelte gute Beispielumsetzungen (Best Practices) in einer Reihe von Publikationen zur Verfügung, die in der sog. IT Infrastructure Library (ITIL) zusammengefasst worden sind und damit einen aus positiven Erfahrungen gewonnenen Quasi-Standard bilden. Dort werden die Prozesse, Aufbauorganisation und Werkzeuge für den Betrieb einer IT-Infrastruktur beschrieben.

Im Rahmen des prioritären Projekts ProBetrieb[14] hat sich das IT-Management des Landes zur Einführung eines ITSM nach den Vorgaben des ITIL entschlossen. Zur Umsetzung des ITSM in der Berliner Verwaltung liegen Handlungsvorschläge des ITDZ vor. Zur Harmonisierung der Strukturen und Prozesse von IT-Vorhaben wird die berlinweite Nutzung eines einheitlichen Werkzeugs angestrebt.

13 Virtuelles Privates Netz. Die Virtualität entsteht aus der Nutzung des gleichen physikalischen Netzes mit anderen Nutzenden von VPN. Die Abgrenzung (Privatheit) der Nutzenden voneinander erfolgt durch die kryptographische Verschlüsselung mit unterschiedlichen Schlüsseln.

14 JB 2006, 1.2

### 1.2.2 IT-Sicherheit

Der aktuelle IT-Sicherheitsbericht 2009 des Senats, der nach den IT-Sicherheitsgrundsätzen des Landes Berlin[15] alljährlich auf der Grundlage von strukturierten schriftlichen Umfragen bei den Behörden des Landes erstellt wird und die Situation im Jahre 2008 widerspiegelt, kam zu folgenden Ergebnissen (in Klammern die Ergebnisse des IT-Sicherheitsberichts 2008):

- 68 Behörden, darunter alle Senatsverwaltungen einschließlich der Senatskanzlei und alle Bezirksämter, haben auf die Umfrage geantwortet (71);
- 47 Behörden verfügen über ein schriftliches Sicherheitskonzept (47); 35 behördliche Sicherheitskonzepte sind von der Behördenleitung bestätigt (37); die ordnungsgemäße Umsetzung der übrigen zwölf Konzepte ist also mangels Rückhalt der Leitungen zumindest fraglich;
- 37 behördliche Sicherheitskonzepte sind in dem Sinne vollständig, dass sie alle nach den IT-Grundschutzkatalogen des BSI[16] oder dem darauf aufbauenden Modellsicherheitskonzept der Berliner Verwaltung erforderlichen Komponenten enthalten (38);
- in 21 Behörden wird das Sicherheitskonzept derzeit erarbeitet (24);
- von den 47 Sicherheitskonzepten wurden 38 auf der Grundlage der IT-Grundschutzkataloge erstellt (39), 39 aufgrund des Modellsicherheitskonzepts (38); in vielen Fällen griff man offensichtlich auf beide Methoden zurück;
- regelmäßige Schulungen zur IT-Sicherheit werden in 18 Behörden durchgeführt (27);
- in 37 Behörden wurde ein IT-Sicherheitsmanagement eingeführt (32);
- in 13 Behörden stehen für die IT-Sicherheit keine Ressourcen zur Verfügung (7).

Diese rein quantitativen Angaben, die ungeprüft in den Sicherheitsbericht einfließen, lassen folgende Aussagen zu:

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

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

- Die IT-Sicherheit, insbesondere die Verfügbarkeit von IT-Sicherheitskonzepten, stagniert im Lande, von den Zahlen her mit leicht abfallender Tendenz.
- Die Anzahl der Behörden mit regelmäßigen Schulungen sank um ein Drittel.
- Fast doppelt so viele Behörden wie im Vorjahr stellen der IT-Sicherheit keine Ressourcen zur Verfügung, sodass hier davon auszugehen ist, dass die IT-Sicherheit nicht als anzustrebendes Ziel angesehen wird.
- Aus den letzten beiden Aussagen lässt sich ableiten, dass das durchschnittliche Niveau der IT-Sicherheit im Land künftig abfallen dürfte, weil den eher vorbildlich agierenden Behörden vermehrt andere gegenüberstehen, denen die Sicherheit ihrer Datenverarbeitung gleichgültig ist.

Angaben über Schadensereignisse betreffen hauptsächlich Probleme mit der Verfügbarkeit der Systeme, hervorgerufen durch Störungen im Grenznetz zwischen dem Internet und dem Berliner Landesnetz, durch Kabelschäden, durch Hardwaredefekte sowie Verlust (Diebstahl) von Geräten. Die wichtigsten Risiken, die zu diesen Schadensereignissen führen, liegen in Irrtümern und Nachlässigkeiten der Beschäftigten, im Befall mit Schadsoftware, in Fehlern und Qualitätsmängeln der eingesetzten Software sowie in Hardware-bedingten Fehlern.

Viele Behörden loben die im Grenznetz durchgeführten Maßnahmen zum SPAM-Schutz. Durch den Einsatz eines zentralen SPAM-Filters wurde erreicht, dass die Anzahl der SPAM-Mails, die die Behörden trotzdem erreichen, signifikant zurückgegangen ist. Es wurden im Tagesdurchschnitt fast 10 Millionen an Berliner Behördenaccounts übersandte SPAM-Mails im Grenznetz erkannt und abgewehrt. Demgegenüber lag die Anzahl nicht blockierter E-Mails bei durchschnittlich 52.000 E-Mails pro Tag.

Gegenstand der Umfrage zum IT-Sicherheitsbericht sind die behördlichen Sicherheitskonzepte. Dabei handelt es sich um die IT-Sicherheitsaspekte der behördlichen Infrastruktur. Dazu gehört die Sicherheit der Gebäude und Räumlichkeiten, insbesondere der Spezialräumlichkeiten für den IT-Betrieb, z. B. der Serverräume und Sicherungsarchive, der Verkabelung und ihrer Datenübertragungskomponenten wie Wiring Center, Router, Gateways, der anwendungsunabhängigen Systemprogramme wie etwa Betriebssoftware, der zentra-

len Dienste wie E-Mail, Webzugang, Zeiterfassung, Standard-Büroanwendungen, der Kryptokonzepte, insbesondere für die Nutzung des Berliner Landesnetzes, der Klimatisierung, des Brandschutzes, des Schutzes vor Wassereinbruch, der Absicherung der Stromversorgung und der Datensicherung. Nicht zuletzt sei darauf aufmerksam gemacht, dass auch die personelle Ausstattung, die Qualifikation, Motivation und Zuverlässigkeit der Bediensteten beim behördlichen Sicherheitskonzept eine Rolle spielen.

Die IT-Sicherheitsgrundsätze verlangen zur Ergänzung des behördlichen Sicherheitskonzepts verfahrensspezifische Sicherheitskonzepte, die es um die speziellen Sicherheitsanforderungen der einzelnen Verfahren ergänzen. So gibt es Verfahren, die einen höheren Schutzbedarf aufweisen, als ihn das behördliche Sicherheitskonzept bereits vorgibt. In diesem Fall gehören in ein verfahrensspezifisches Sicherheitskonzept auch Maßnahmen, die die Sicherheit erhöhen, z. B. die Dateiverschlüsselung zum Schutz der Vertraulichkeit gegenüber verfahrensfremden Systemverwaltern. Ferner verlangen viele Anwendungsprogramme differenziertere Rollenkonzepte für die Berechtigungen der Anwender, als die Betriebssysteme schon anbieten.

Ein Sicherheitskonzept, das § 5 Abs. 3 Satz 1 Berliner Datenschutzgesetz genügen soll, muss die Gesamtsicherheit erfassen. Zwar ist das Sicherheitskonzept Voraussetzung für die Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung, also meist einer Anwendung. Ein verfahrensspezifisches Sicherheitskonzept macht jedoch ohne das zugrunde liegende behördenspezifische Sicherheitskonzept keinen Sinn, so gut es auch ausgearbeitet sein mag. Soweit uns professionell erstellte Sicherheitskonzepte im Zusammenhang mit der Einführung neuer Verfahren vorgelegt worden sind, erfassen sie zumindest die für die Anwendung genutzten Teile der Infrastruktur mit oder verweisen (seltener) auf das behördliche Sicherheitskonzept.

In letzter Zeit häufen sich IT-Verfahren, die zunächst für andere Bundesländer entwickelt und entweder von Berlin übernommen wurden oder bei denen auch die zentrale Verarbeitung in einem anderen Bundesland durchgeführt wird.

Zur ersten Kategorie gehört das EOSS-Verfahren („Evolutionär orientierte Steuersoftware“) der Finanzverwaltung[17], das in Bayern entwickelt wurde, ohne dass ein verfahrensspezifisches Sicherheitskonzept dazu erstellt wurde, weil dies in Bayern gesetzlich nicht verlangt wird. Dass dies kein Grund ist, entgegen § 5 Abs. 3 Satz 1 BlnDSG auf ein Sicherheitskonzept zu verzichten, hat die Senatsverwaltung für Finanzen inzwischen eingesehen. Gleichwohl liegt es immer noch nicht vor. Zur gleichen Kategorie gehören die IT-Verfahren des Strafvollzugs wie z. B. BASIS-WEB als wichtigstes Verfahren im Strafvollzug, das von einer nordrhein-westfälischen Firma zunächst für Nordrhein-Westfalen entwickelt wurde und inzwischen in vielen Bundesländern, so auch Berlin, eingesetzt wird. Hier legte uns die Justizverwaltung die für Nordrhein-Westfalen erarbeiteten Sicherheitskonzepte vor, in der Hoffnung, sie würden den Ansprüchen des BlnDSG gerecht werden. Dies traf jedoch nicht zu. Ein für Berlin erstelltes Sicherheitskonzept für BASIS-WEB ist für März 2010 angekündigt.

Zur zweiten Kategorie gehört das IT-Verfahren MESTA[18] der Generalstaatsanwaltschaft Berlin, das als Ersatz für das gescheiterte IT-Verfahren MODESTA in der Berliner Staatsanwaltschaft eingeführt wird. Die zentrale Verarbeitung wird außerhalb Berlins erfolgen. Dies entbindet die Generalstaatsanwaltschaft jedoch nicht von der Pflicht zur Erstellung eines Sicherheitskonzepts für das Verfahren, denn bei der Kommunikation mit dem auswärtigen Rechenzentrum ist zumindest die Sicherheit der dezentralen Komponenten in Berlin und der Datenübertragungswege zu gewährleisten, die für die dezentrale Nutzung von MESTA in Berlin erforderlich sind.

### 1.2.3 Aktuelle IT-Projekte

**MESTA – Mehrländer-Staatsanwaltschaft-Automation**

Im Vorjahr berichteten wir ausführlich über das Projekt MODESTA zur **Mode**rnisierung der **S**taats- und **A**mtsanwaltschaft[19]. Wie uns der Generalstaatsanwalt Ende 2009 mitteilte, hat die Senatsverwaltung für Justiz im Oktober das

17 JB 2007, 1.2
18 Vgl. auch 1.2.3
19 JB 2008, 1.2.3

Projekt abgebrochen. Gründe nannte er dabei nicht. Allerdings hatte die Presse zuvor bereits berichtet, dass der mit der Realisierung von MODESTA beauftragte IT-Dienstleister offensichtlich überfordert war. Das Projekt sei bereits viermal um ein Jahr verschoben worden.

Anstelle einer Eigenentwicklung wird sich Berlin einem Mehrländerverbund anschließen, dem bereits Schleswig-Holstein, Hamburg, Brandenburg, Hessen, Nordrhein-Westfalen und Mecklenburg-Vorpommern angeschlossen sind. Das Verfahren MESTA (**Me**hrländer-**St**aatsanwaltschaft-**A**utomation) wurde von Dataport, einer Anstalt des öffentlichen Rechts mit Sitz in Altenholz bei Kiel, entwickelt und wird von Dataport auch zentral für alle Länder verarbeitet.

Die Teilnahme der Berliner Amts- und Staatsanwaltschaft am MESTA-Verbund bedeutet aber nicht, dass die Berliner Strafverfolgungsbehörden von der datenschutzrechtlichen Verantwortung für die Berliner Teilnahme am Verfahren freigestellt sind. Sie bleiben datenverarbeitende Stellen im Sinne von § 4 Abs. 1 BlnDSG und müssen als Auftraggeber die Berliner Regelungen zur Vergabe von Aufträgen zur Datenverarbeitung nach § 3 BlnDSG beachten. Da auf den schleswig-holsteinischen Auftragnehmer Dataport das BlnDSG keine Anwendung findet, sind auch die speziellen Regelungen von § 3 Abs. 4 BlnDSG zu beachten, wonach Dataport in Bezug auf die Verarbeitung der Berliner Daten verpflichtet werden muss, das BlnDSG anzuwenden und sich der Kontrolle des Datenschutzbeauftragten des Landes zu unterwerfen, in dem die Datenverarbeitung durchgeführt wird.

Hinsichtlich der Sicherheitskonzeption bestehen in Schleswig-Holstein (und in Mecklenburg-Vorpommern) ähnliche Anforderungen wie in Berlin, sodass zunächst davon ausgegangen werden kann, dass die Dataport-Rechenzentren den Anforderungen des § 5 BlnDSG genügen. Allerdings bleiben die Berliner Strafverfolgungsbehörden verpflichtet, für die in der Verantwortung Berlins stehenden Verfahrensteile (Arbeitsplatzrechner als Benutzerschnittstelle, ggf. Server sowie die Datenübertragung und die dazugehörigen Einrichtungen auf Berliner Seite) ein verfahrensspezifisches Sicherheitskonzept zu erstellen und umzusetzen.

### Webbasierte Bewerberdatenbank

Bei dem Projekt der Senatsverwaltung für Inneres und Sport handelt es sich um eine wesentliche Modernisierung und Zusammenführung zweier alter IT-Verfahren: ABIDA zur Verwaltung der Daten der Bewerberinnen und Bewerber um einen Ausbildungsplatz in der Berliner Verwaltung und die Testauswertungsdatenbank für die Verwaltung der Testergebnisse des Eignungsprüfungsverfahrens BETA.

Die Modernisierung wurde mit dem irreparablen Plattencrash des Servers erzwungen. Da die alte Software für neue Server inkompatibel war und für die Software kein Support mehr bestand, weil die Herstellerfirma nicht mehr existierte, musste die Software vollständig ersetzt werden.

Da es sich um die Weiterentwicklung eines seit langem bestehenden und bewährten Verfahrens handelte, führte die rechtliche Überprüfung zu keinen Mangelhinweisen.

Obwohl zugesagt worden war, dass zum Beginn des Echtbetriebs des neuen Verfahrens das dann erforderliche Sicherheitskonzept erstellt und umgesetzt werde, ging das Verfahren ohne diese rechtliche Voraussetzung in Betrieb, was wir im April förmlich beanstandet haben. Zu Beginn des Jahres 2010 erhielten wir das Sicherheitskonzept, über dessen Prüfung wir im nächsten Jahr berichten werden.

### IT-Verfahren „Nexus VeLiS-Kammer“ zur Verwaltung der Habe der Gefangenen in den Justizvollzugsanstalten

Das Verfahren „Nexus VeLiS-Kammer“ dient der Verwaltung der persönlichen Habe und Ausstattung von Gefangenen in den Berliner Justizvollzugsanstalten. Die persönlichen Daten der Gefangenen stammen aus dem JVA-Verwaltungssystem Basis-Web und werden direkt in die Masken von VeLiS eingeblendet, jedoch nicht in die VeLiS-Datenbank kopiert.

Ansonsten werden die Gegenstände benannt und hinsichtlich Beschaffenheit und Zustand beschrieben, der aktuelle Aufbewahrungsort sowie die Bewegungen werden dokumentiert. Darüber hinaus werden Listen und Historien aller

persönlichen Gegenstände und der im Eigentum der JVA stehenden Ausstattungsgegenstände der Gefangenen geführt.

Die Erfassung der persönlichen Habe der Gefangenen einerseits und der Ausstattung mit Gegenständen der JVA beruhen auf unterschiedlichen Rechtsgrundlagen. Wir haben daher die Justizverwaltung darauf hingewiesen, dass diese beiden Datenerhebungen strikt voneinander zu trennen sind. Außerdem bestehen bei manchen Daten, die im Katalog der zu beiden Zwecken zu erhebenden Daten aufgeführt sind, Zweifel an der Erforderlichkeit und damit an der Rechtmäßigkeit. Zweifelhaft ist schließlich, ob alle Personengruppen, die in der Liste der Zugriffsberechtigten aufgeführt waren, zugriffsberechtigt sein müssen. Die Beratungen zu diesem Verfahren sind noch nicht abgeschlossen.

# 2. Schwerpunkte

## 2.1 Auslegungsprobleme beim novellierten Bundesdatenschutzgesetz

„Der Gesetzgeber löst ein Problem und schafft zwei neue." Dieser Satz eines Rechtsprofessors trifft sicher auch auf die drei im Jahr 2009 verabschiedeten Novellen zum Bundesdatenschutzgesetz[20] (BDSG) zu. Auch wenn die Novellierungen insgesamt zu einer Verbesserung des Datenschutzniveaus im nichtöffentlichen Bereich geführt haben, klagen viele Unternehmen zu Recht über die entstandenen Auslegungsprobleme. Die ersten Fragen, die die Wirtschaft uns gestellt hat, werden im Folgenden beantwortet.

In der Praxis gab es bisher häufig Probleme bei Verträgen zur Auftragsdatenverarbeitung. Nun regelt das Gesetz in § 11 Abs. 2 Satz 2 Nr. 1–10 BDSG die Mindestfestlegungen, die der schriftliche Auftrag enthalten muss. Außerdem ist der Auftraggeber nach § 11 Abs. 2 Satz 4 BDSG nun ausdrücklich verpflichtet, regelmäßig die Einhaltung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überwachen. Da § 11 Abs. 2 Satz 2 Nr. 1–10 BDSG nur Mindestanforderungen („insbesondere") festlegt, sollten bei der Auftragsgestaltung zusätzlich die Hinweise der Datenschutzaufsichtsbehörde im Innenministerium Baden-Württemberg[21] beachtet werden.

Eine rechtmäßige Auftragsdatenverarbeitung ist nur möglich, wenn bei der vorgesehenen Datenverarbeitung alle Mindestfestlegungen getroffen werden können und die geforderte regelmäßige Überwachung möglich ist. Bei einigen Internetverfahren (Cloud Computing, Analyseverfahren zur Reichweitenmes-

20 Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009 (BGBl. I, S. 2254); Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I, S. 2814); Art. 5 des Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29. Juli 2009 (BGBl. I, S. 2355).

21 Hinweis zum BDSG Nr. 31, Staatsanz. Nr. 1-2/1993, wiedergegeben bei P. Gola/R. Schomerus: Bundesdatenschutzgesetz. Kommentar, 3. Aufl., Rn. 18 zu § 11.

sung bei Internetangeboten) ist dies zumindest zweifelhaft. Hinzuweisen ist darauf, dass der Auftraggeber die technischen und organisatorischen Maßnahmen nicht selbst überprüfen muss. So muss etwa der einzelne Steuerberater nicht die technischen und organisatorischen Maßnahmen von DATEV überprüfen. Der Kontrolleur sollte aber nicht vom Auftragnehmer beauftragt werden. Er sollte sich im Lager des Auftraggebers befinden. Bei Unterauftragsverhältnissen wird häufig übersehen, dass dem Auftraggeber ein Weisungs- und Kontrollrecht einzuräumen ist.

Bei der Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen gelten bei der Zugriffsmöglichkeit auf personenbezogene Daten nach § 11 Abs. 5 BDSG die Absätze 1 bis 4 entsprechend. Das setzt voraus, dass bei dem schriftlichen Auftrag die Mindestanforderungen des § 11 Abs. 2 Satz 2 BDSG aufgenommen werden, die bei einem Auftrag nach § 11 Abs. 5 BDSG einzuhalten sind.

Das bisherige Bundesdatenschutzgesetz erlaubte bereits in kaum zu rechtfertigender Weise die Verarbeitung bestimmter Daten Betroffener für Zwecke der Werbung und Markt- und Meinungsforschung. Diese Daten waren in § 28 Abs. 3 Satz 1 Nr. 3 BDSG aufgelistet: Die Zugehörigkeit Betroffener zu einer Personengruppe, ihre Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademische Grade, Anschrift und Geburtsjahr (sog. Listenprivileg). Vor der Novellierung des Gesetzes war umstritten, ob diese Vorschrift eine abschließende Regelung für Werbedaten darstellt oder ob über das Listenprivileg hinaus Unternehmen ihre Kunden nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG a. F. bewerben dürfen. Nunmehr ist in § 28 Abs. 3 Satz 3 BDSG insbesondere bei Vertragsdaten ausdrücklich geregelt, dass den Listendaten weitere Daten hinzugefügt werden können. Allerdings ist dies nur zulässig, soweit nicht schutzwürdige Interessen der Betroffenen entgegenstehen (§ 28 Abs. 3 Satz 6 BDSG). Das Hinzufügungsrecht ist also nicht unbegrenzt. Die oder der Betroffene ist beim Vertragsabschluss über den Zweck, die Daten für Werbung zu verwenden, und über sein Widerspruchsrecht dagegen zu informieren. Schutzwürdige Interessen der Betroffenen sind immer dann tangiert, wenn von Kunden Datenprofile gebildet werden. Wenn nach Beendigung des Vertragsverhältnisses die Vertragsdaten der Betroffenen nach § 35 Abs. 2 Satz 2 Nr. 3 bzw. Abs. 3 Nr. 1 BDSG zu löschen bzw. zu sperren sind, sollten sich etwa noch vorhandene Werbedaten auf die Daten des Listenprivilegs beschränken.

In § 28 a Abs. 1 Nr. 1–5 BDSG werden nun abschließend die Fallgruppen aufgezählt, bei denen Gläubiger Forderungen an Auskunfteien melden können. Es gilt aber weiterhin, dass nur Forderungen eingemeldet werden dürfen, deren Nichterfüllung auf Zahlungsunwilligkeit oder Zahlungsunfähigkeit beruht. So darf selbst ein rechtskräftiges Urteil erst dann eingemeldet werden, wenn der Schuldner die Forderung nicht unverzüglich nach Rechtskraft begleicht.

Mit § 28 a Abs. 2 Satz 1 und 2 BDSG trägt der Gesetzgeber dem Umstand Rechnung, dass der „SCHUFA-Einwilligung" die Freiwilligkeit fehlte, da ohne sie kein Girokonto eröffnet wurde. Die Einwilligung hat der Gesetzgeber durch die Schaffung einer Rechtsgrundlage ersetzt, der Betroffene ist vor dem Abschluss des Vertrages über die Datenübermittlung an die SCHUFA zu unterrichten. Banken haben neben dem Bundesdatenschutzgesetz das Bankgeheimnis zu beachten; der Zweck der Norm, Bankkunden nicht mehr zu unfreiwilligen Einwilligungen zu zwingen, gebietet es aber, § 28 a Abs. 2 Satz 1 BDSG als eine das Bankgeheimnis einschränkende Spezialnorm anzusehen.

Spätestens nach der Schaffung des § 28 b BDSG haben die Aufsichtsbehörden die Möglichkeit, bei Scoring-Verfahren die Wissenschaftlichkeit des mathematisch-statistischen Verfahrens zu überprüfen. Die datenschutzrechtlichen Anforderungen an Scoring-Verfahren gelten neben den von der Bundesanstalt für Finanzdienstleistungsaufsicht kontrollierten Vorgaben des Gesetzes über das Kreditwesen. Banken müssen die Vorgaben beider Gesetze beachten. Geodaten dürfen für Scoring-Verfahren zwar verwendet werden. Es bestehen aber verschiedene Einschränkungen. Insbesondere dürfen die Daten nicht ausschließlich für die Berechnung des Wahrscheinlichkeitswerts genutzt werden[22]. Eine Ausschließlichkeit ist auch anzunehmen, wenn neben den Geodaten zwar noch andere Daten verwendet werden, diese aber nicht ins Gewicht fallen.

§ 29 Abs. 6 BDSG regelt, dass Auskunfteien Banken aus anderen Mitgliedstaaten der EU bzw. des EWR genauso zu behandeln haben wie deutsche Banken. Dies gilt selbst dann, wenn inländische Banken in dem Land des ausländischen Darlehensgebers keine Gleichbehandlung erhalten. § 29 Abs. 7 BDSG sieht eine neue Pflicht vor, die Betroffenen bei der Ablehnung des Abschlusses eines Verbraucherdarlehensvertrages oder eines Vertrages über eine entgeltliche Finan-

22 § 28 b Nr. 3 und 4 BDSG

zierungshilfe aufgrund einer ungünstigen Auskunft zu informieren. Schon die Ablehnung eines Kaufs auf Rechnung führt zur Unterrichtungspflicht.

Mit § 30 a BDSG ist eine Rechtsvorschrift geschaffen worden, die eine geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- und Meinungsforschung ermöglicht. Hinzuweisen ist darauf, dass der Gesetzgeber die noch nicht höchstrichterlich entschiedene Frage offen gelassen hat, ob telefonische Marktforschung als Verstoß gegen § 7 Abs. 2 Nr. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) gewertet werden kann.

Da der Gesetzgeber für Beschäftigungsverhältnisse in § 32 BDSG eine Spezialnorm geschaffen hat, ist zu klären, in welchem Umfang neben § 32 BDSG noch § 28 BDSG zur Anwendung kommt. Während § 28 Abs. 1 Satz 1 Nr. 1 BDSG durch § 32 Abs. 1 Satz 1 BDSG verdrängt wird, wird man dem gesetzgeberischen Willen folgend § 28 Abs. 1 Satz 1 Nr. 2 und 3 sowie Abs. 2 Nr. 1 und 2 ebenso weiterhin auf Beschäftigte anwenden wie § 28 Abs. 6 BDSG. Die grundsätzliche Anwendbarkeit des § 28 BDSG darf aber nicht missverstanden werden. Bei der Auslegung des § 28 BDSG ist die Sperrwirkung des § 32 BDSG als Spezialnorm zu beachten. Die Verarbeitung von Beschäftigten- und Bewerberdaten nach § 28 BDSG kommt nur in Betracht, soweit hierdurch keine Festlegungen, die in der Spezialnorm getroffen wurden, zunichte gemacht werden. Eine Google-Recherche über einen Stellenbewerber ist nach § 32 Abs. 1 Satz 1 BDSG in der Regel nicht erforderlich. Hier kann der Arbeitgeber zur Rechtfertigung seiner Recherche nicht auf § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG zurückgreifen. § 32 Abs. 1 Satz 1 BDSG ist enger auszulegen als der bisher im Arbeitsrecht anwendbare § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Für Datenverarbeitungen im Rahmen der Pflicht zum Risiko- bzw. Compliance-Management nach § 31 Abs. 2 Aktiengesetz, § 43 GmbH-Gesetz oder nach den Vorgaben des US-Sarbanes-Oxley-Act (SOX) kommt diese Rechtsnorm nicht als Rechtsgrundlage in Betracht. Datenverarbeitungen zu Präventionszwecken sind aber weiterhin nach § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG möglich. Allerdings ist die Pflicht und das Recht zum Risiko- bzw. Compliance-Management durch die Sperrwirkung des § 32 Abs. 1 Satz 2 BDSG eingeschränkt. Diese Norm stellt für repressive Maßnahmen zur Aufdeckung von Straftaten einschränkende Bedingungen auf, insbesondere das Vorhandensein eines begründeten und zu dokumentierenden Tatverdachts. Da repressive und präventive Maßnahmen sich häufig nicht objektiv unterscheiden, sind auch präventive Maßnahmen nur

gestattet, soweit hierdurch eine Umgehung von § 32 Abs. 1 Satz 2 BDSG ausgeschlossen ist.

Auskunfteien arbeiten häufig mit geschätzten Daten. Es handelt sich dabei um statistische Daten, die in Ermangelung konkret vorhandener Daten einer Auskunft hinzugefügt werden. Bisher haben die Auskunfteien in einer Fußnote zur Auskunft nur den allgemeinen Hinweis gegeben, dass auch Schätzdaten verwendet werden. Nach § 35 Abs. 1 Satz 2 BDSG ist nun jedes einzelne geschätzte Datum als solches zu kennzeichnen.

Bislang haben Auskunfteien ihrer Kundschaft (z. B. Kreditinstituten) mitgeteilt, dass über die Betroffenen gesperrte Daten vorliegen. Dies ist nun nach § 35 Abs. 4a BDSG rechtswidrig. Die Auskunft darf weder die Tatsache der Sperrung noch Hinweise auf eine Sperrung enthalten. Die Befürchtung von Auskunfteien, dass diese Regelung zu Missbräuchen führen kann, ist nicht begründet, da ein Bestreiten nur dann zur Sperrung von Daten führt, wenn das Bestreiten nicht gegen die Grundsätze von Treu und Glauben verstößt.

Neu in das Bundesdatenschutzgesetz aufgenommen ist die Informationspflicht der verantwortlichen Stelle bei unrechtmäßiger Übermittlung oder Kenntniserlangung von bestimmten Daten[23]. Diese Vorschrift ist der in den meisten US-Bundesstaaten geltenden Informationspflicht (security breach notification) nachgebildet. Die Erfüllung der Benachrichtigungspflicht etwa an die Aufsichtsbehörde wird bei betroffenen Unternehmen zu Problemen führen, da die Benachrichtigung einerseits unverzüglich zu erfolgen hat, andererseits aber schon bestimmte Informationen enthalten muss, wie eine Darstellung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen. Sofern eine Informationspflicht tatsächlich bestanden hat, darf die Mitteilung selbst nur mit Zustimmung der oder des Betroffenen im Rahmen eines Straf- oder Ordnungswidrigkeitenverfahrens verwendet werden. Hierdurch soll verhindert werden, dass die Mitteilungspflicht zu einem Zwang zur Selbstbezichtigung führt. Das Gesetz enthält hier aber kein Beweiserhebungsverbot. Der gemeldete Sachverhalt kann daher mit anderen Beweismitteln als der Mitteilung selbst verfolgt werden.

23 § 42 a Satz 1 Nr. 1-4 BDSG

Die 2009 beschlossenen Änderungen des Bundesdatenschutzgesetzes bringen zwar gewisse Verbesserungen für die Betroffenen im Detail, bleiben angesichts des bestehenden Modernisierungsbedarfs jedoch Stückwerk und werfen zudem neue Rechtsfragen auf, zu denen wir erste Antworten geben.

## 2.2 Videoüberwachung an Schulen[24]

### Allgemeine Erwägungen

Die Sozialräume, in denen wir uns alltäglich (im Beruf, im Verkehr, in der Freizeitgestaltung) bewegen, werden zunehmend durch Videoüberwachungstechniken beobachtet und kontrolliert. Diese Kontrolle ist grundsätzlich mit Eingriffen in die Grundrechte der davon erfassten Personen verbunden. Der Einsatz dieser Techniken ist daher generell nur unter sehr eingeschränkten Voraussetzungen zulässig. Erfolgt er in der Schule, steht er darüber hinaus in direktem Widerspruch zu deren Bildungsauftrag. Die Schule hat die ihr anvertrauten Schülerinnen und Schüler zu Persönlichkeiten heranzubilden, die fähig sind, das staatliche und gesellschaftliche Leben auf der Grundlage der Demokratie, des Friedens, der Freiheit und der Menschenwürde zu gestalten (§ 1 SchulG). Eine (objektive oder subjektiv gefühlte) Beobachtung und Kontrolle der Schülerinnen und Schüler in der Schule unter Einsatz von technischen Überwachungsmaßnahmen steht den genannten Werten und damit der Erfüllung des schulischen Auftrags diametral entgegen. Der Einsatz von Videoüberwachungstechnik in und an Schulen ist daher grundsätzlich als problematisch anzusehen.

Die Unterrichtsräume einer Schule dürfen grundsätzlich nicht – insbesondere nicht während des Unterrichts – mit Videokameras überwacht werden. Die damit verbundene Leistungs- und Verhaltenskontrolle der Schülerinnen und Schüler sowie der Lehrkräfte wäre aus datenschutzrechtlichen und aus dienstrechtlichen Gründen unzulässig. Erfolgt eine Videoaufzeichnung im Schulunterricht als methodisches (Hilfs-)Mittel in der schulischen Ausbildung (z. B.

24 Vgl. dazu auch die sehr informative Orientierungshilfe „Ich sehe das, was Du so tust! Videoüberwachung an und in Schulen“ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Aufzeichnung von Rollenspielen, Bewerbungsgesprächen, Theaterproben), so ist sie projektbezogen auf den erforderlichen Umfang und zeitlich eng zu begrenzen. Die Betroffenen (auch die Lehrkräfte) haben zuvor in die Datenverarbeitung einzuwilligen. Sie sind über die Bedeutung der Einwilligung, insbesondere den Verwendungszweck der Videodaten, aufzuklären. Betroffene, deren Einwilligung nicht vorliegt, dürfen nicht gefilmt werden. Eine dauerhafte Beobachtung (z. B. über mehrere Unterrichtsstunden oder -tage) ist mit einem erheblichen Eingriff in die Grundrechte der Betroffenen verbunden. Sie ist – 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. deren Erziehungsberechtigten gestützt werden.

Auch der Eingangsbereich, der Schulhof oder die sonstigen Räumlichkeiten einer Schule (z. B. Kantine) dürfen während des laufenden Schulbetriebes nicht durch Videoanlagen beobachtet werden. Die Schülerinnen, Schüler und Lehrkräfte sind gezwungen, sich in diesen Bereichen (auf dem Weg zum Unterricht oder in den Pausen) aufzuhalten und zu bewegen. Sie könnten sich einer derartigen Überwachung daher nicht entziehen und wären in ihrer selbstbestimmten Bewegungsfreiheit auf dem Schulgelände in erheblicher Weise eingeschränkt. Einem zunehmenden Vandalismus oder körperlichen Auseinandersetzungen, die oftmals als Rechtfertigung für den Einsatz von Videoüberwachung dienen, sollte durch eine gesteigerte Lehrkraftaufsicht und eine verstärkte soziale Kontrolle begegnet werden. Wollte man diese Probleme mit einem erweiterten Technikeinsatz lösen, käme dies einer Bankrotterklärung der Pädagogik gleich.

### Rechtliche Zulässigkeit einer Videoüberwachung in Schulen

Jede Videoüberwachung greift in das „Recht auf informationelle Selbstbestimmung“ und das „Recht am eigenen Bild“ des von der Maßnahme betroffenen Menschen ein. Sind die beobachteten Personen erkennbar, werden durch die Technik personenbezogene Daten der betroffenen Personen verarbeitet. Eine derartige Verarbeitung von personenbezogenen Daten durch eine öffentliche Stelle des Landes Berlin (z. B. den Schulträger und/oder eine Schule) ist nach § 6 Abs. 1 BlnDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin wirksam eingewilligt hat. Weder das Berliner Schul-

gesetz noch die dazu ergangenen Verordnungen enthalten bereichsspezifische Regelungen, die sich mit der Zulässigkeit einer Videoüberwachung in Schulen befassen. Daraus lässt sich ableiten, dass der Gesetzgeber diese Form der Überwachung im Schulbereich grundsätzlich nicht vorgesehen hat.

In § 31 b BlnDSG gibt es – jenseits der bereichsspezifischen Bestimmungen für den Schulbereich – eine allgemeine Regelung für die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen", die für alle öffentlichen Stellen des Landes Berlin gilt. Da es sich bei den Berliner Schulen um öffentliche Stellen des Landes Berlin handelt, kann diese Regelung grundsätzlich auch für diesen Bereich herangezogen werden.

Der Anwendungsbereich des § 31 b BlnDSG stellt nicht darauf ab, dass (Video-) Bilder aufgezeichnet oder gespeichert werden. Die Vorschrift ist schon dann anzuwenden, wenn die tatsächliche Möglichkeit der (Video-)Beobachtung gegeben ist. Die Überwachungsmaßnahme nach § 31 b BlnDSG beginnt daher bereits mit der Installation und Inbetriebnahme einer Kamera, auch wenn das Gerät nur im Bedarfs- oder Alarmfall aufzeichnet oder nur zur bloßen Beobachtung genutzt wird.

§ 31 b BlnDSG bezieht sich nur auf die Überwachung von öffentlich zugänglichen Räumen. In einer Schule und auf dem Schulgelände sind dies alle Bereiche, die frei und ungehindert betreten werden können. Dazu gehören in der Regel der Schulhof, das Schulgebäude als solches, Sporthallen und weitere Außenanlagen. Im Gegensatz dazu sind Bereiche, die nur ganz bestimmten Personenkreisen zugänglich sind (z. B. das Lehrerzimmer, bestimmte Unterrichts-, Selbstlern- und Aufenthaltsräume), als nicht öffentlich zugänglich einzuordnen. Die öffentlich zugänglichen Bereiche einer Schule dürfen nach § 31 b Abs. 1 BlnDSG nur dann videoüberwacht werden, wenn der Einsatz der Videoüberwachung zur Aufgabenerfüllung der Schule oder zur Wahrnehmung des Hausrechts erforderlich ist.

Da der Einsatz von Videoüberwachungsmaßnahmen zur Erfüllung der Aufgaben einer Schule nach dem Schulgesetz nicht erforderlich ist, kann er nur im Rahmen der Wahrnehmung des Hausrechts erfolgen. Die Ausübung des Hausrechts an den Berliner Schulen ist geteilt. Die Schulbehörden in den Bezirken sind nach § 109 Abs. 1 SchulG verpflichtet, die für einen ordnungsgemäßen

Unterricht erforderlichen Schulanlagen, Gebäude, Einrichtungen und Lehrmittel bereitzustellen und zu unterhalten. Für diese sog. äußeren (Schul-)Angelegenheiten steht ihnen das Hausrecht an den Schulen zu. Ist dagegen der Schulbetrieb selbst betroffen, handelt es sich um eine innere (Schul-)Angelegenheit, für die die Leitung der Schule das Hausrecht wahrnimmt[25].

Zur Wahrnehmung des Hausrechts dürfen Maßnahmen ergriffen werden, um Personen, die sich im Schulgebäude aufhalten, vor Gefahren für Leib oder Leben zu schützen sowie erhebliche Eigentumsbeeinträchtigungen zu verhindern. Soll dabei Videotechnik eingesetzt werden, so ist dies nur zulässig, wenn es keine Anhaltspunkte dafür gibt, dass die schutzwürdige Interessen der betroffenen Personen überwiegen (§ 31 b Abs. 1 Satz 1 BlnDSG). Das bedeutet, dass bei jeder Videoüberwachung im Einzelfall das Verhältnismäßigkeitsprinzip gewahrt sein muss. Der Einsatz muss zur Wahrnehmung des Hausrechts geeignet und erforderlich sein, darf die Betroffenen aber nicht unverhältnismäßig belasten. Da hier die Persönlichkeitsrechte der Schülerinnen und Schüler sowie der Lehrkräfte berührt sind, ist eine Abwägung mit deren schutzwürdigen Interessen vorzunehmen. Dabei ist der Erziehungs- und Bildungsauftrag der Schule als vorrangig mit einzubeziehen mit dem Ergebnis, dass eine Videoüberwachung in der Schule grundsätzlich nur außerhalb des Schulbetriebes erfolgen darf. Während des laufenden Schulbetriebs ist sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen dagegen nur in besonderen Ausnahmefällen und in sehr eingeschränktem Umfang zulässig.

Ein derartiger Ausnahmefall kann z. B. gegeben sein, wenn es am Fahrradständer der Schule in der Vergangenheit bereits wiederholt zu Diebstählen und erheblichen Sachbeschädigungen gekommen ist. Zunächst ist auch hier zu prüfen, ob der Einsatz einer Videoüberwachungsanlage überhaupt erforderlich ist und die Fahrräder nicht auf andere Weise wirksam geschützt werden können, z. B. durch Verlegung der Fahrradständer an einen Platz auf dem Schulgelände, der besser beaufsichtigt werden kann. Ist dies nicht der Fall, kann der Einsatz einer Videoüberwachung auch ausnahmsweise während des Schulbetriebs zulässig sein. Bei der Abwägung der Interessen ist zu berücksichtigen, dass die Nutzung der Fahrradständer in der Regel freiwillig erfolgt und sich die Betroffenen nur sehr kurzfristig in dem überwachten Bereich aufhalten müssen.

25 § 69 Abs. 1 Nr. 2 SchulG

Letztlich kommt es bei Beurteilung der Zulässigkeit einer solchen Maßnahme jedoch entscheidend auf die konkreten Umstände des Einzelfalles an.

Die Videoüberwachung außerhalb des laufenden Schulbetriebs (z. B. am Nachmittag, in der Nacht oder am Wochenende) muss ebenfalls die gesetzlichen Vorgaben des § 31 b Abs. 1 BlnDSG erfüllen. Vor dem Einsatz der (Video-)Überwachung ist daher zu prüfen, ob es andere Maßnahmen gibt (wie die Einzäunung des Geländes und Sicherung der Tore, Bewegungsmelder mit Scheinwerfern, Alarmanlagen), die für die Persönlichkeitsrechte Dritter weniger belastend sind, aber dennoch wirksamen Schutz bieten. Dritte können hier Personen wie Teilnehmer von Veranstaltungen, Mitglieder von Sportvereinen sein, die sich außerhalb des eigentlichen Schulbetriebes zulässigerweise in den Gebäuden oder auf dem Gelände der Schule aufhalten. Dürfen diese Bereiche auch außerhalb der Schulzeiten von Schülerinnen, Schülern und von Dritten zu deren Freizeitgestaltung genutzt werden, ist das Interesse von solchen Personen, sich dort unbeobachtet zu bewegen, grundsätzlich höher zu bewerten als das Hausrecht der Schulbehörde.

Im Verhältnis zur bloßen (Video-)Beobachtung ist die Videoaufzeichnung als der schwerwiegendere Eingriff in das Persönlichkeitsrecht der Betroffenen anzusehen. Er ist nach § 31 b Abs. 3 BlnDSG nur zulässig, wenn der mit der Videoüberwachung verfolgte Zweck eine Aufzeichnung erfordert. Diese sollte grundsätzlich nur anlass- und bereichsbezogen erfolgen. Eine permanente Aufzeichnung ist nur dann zulässig, wenn die anlassbezogene Aufzeichnung nicht durchführbar oder unzureichend ist. In jedem Fall sind dann als Ausgleich besondere Sicherheitsmaßnahmen zu treffen. Aufzeichnungen, die nicht mehr benötigt werden (das dürfte grundsätzlich nach 48 Stunden der Fall sein), sind unverzüglich zu löschen bzw. automatisiert in einem Black-Box-Verfahren zu überschreiben. Die Zugriffsrechte auf das Videomaterial sollten auf die Schulleitung begrenzt sein.

Die Videoüberwachung von nicht öffentlich zugänglichen Räumen in einer Schule (z. B. das Lehrerzimmer, der PC-Selbstlernraum) ist weder im SchulG noch im BlnDSG geregelt. Sie ist daher ohne die Einwilligung der Betroffenen in der Regel unzulässig. Einige Schulen stellen den Schülerinnen und Schülern bestimmte Räumlichkeiten, die nicht öffentlich zugänglich sind (z. B. Musiksaal, PC-Raum), auch außerhalb des Unterrichts als Selbstlerneinrich-

tung zur Verfügung. Eine Videoüberwachung dieser Bereiche zum Schutz der Instrumente und Geräte ist nur dann zulässig, wenn die freiwillige Nutzung der Räumlichkeiten auch eine Einwilligung der Betroffenen in die Videoüberwachung mit umfasst. Die Voraussetzungen für eine wirksame Einwilligung sind in § 6 Abs. 3-6 BlnDSG geregelt. Die Einwilligungsfähigkeit von minderjährigen Schülerinnen und Schülern ist davon abhängig, ob sie die Bedeutung der Einwilligung und deren rechtlicher Folgen erfassen können. Bei Schülerinnen und Schülern in der Oberstufe ist davon grundsätzlich auszugehen. Bei jüngeren Schülerinnen und Schülern ist bei der Beurteilung der Einsichtsfähigkeit auf den Einzelfall abzustellen.

Bevor die Installation auf die Einwilligung der Betroffenen gestützt wird, sollte jedoch geprüft werden, ob die Geräte und die Einrichtung nicht durch alternative (z. B. bauliche) Maßnahmen geschützt werden können, die weniger intensiv in die Rechte der Betroffenen eingreifen.

Angesichts des erheblichen Eingriffs in die Grundrechte der Betroffenen sollte grundsätzlich von einer Videoüberwachung in Schulen abgesehen werden.

## 2.3 Auch Kranke brauchen Datenschutz – Zugriffsregelungen in Krankenhausinformationssystemen

Krankenhausinformationssysteme (KIS) sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Versuchung für Klinikbeschäftigte, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, ist groß. Bekannt gewordene Missbrauchsfälle – auch in Berlin – belegen dies.

Zusätzliche Gefährdungen entstehen durch die Anbindung der Informationssysteme der Krankenhäuser an Systeme Dritter, etwa ausgegründete Medi-

zinische Versorgungszentren, zuweisende Ärzte, Labore, externe Dienstleister. Beispielhaft findet sich weiter unten Näheres zur Nutzung von sog. Zuweiserportalen[26].

Erste Prüfungen in vier großen Berliner Krankenhäusern offenbarten erhebliche Gefahren bei der Nutzung von KIS: In einem Krankenhaus bestand die inakzeptable Situation, dass dem gesamten ärztlichen und pflegerischen Personal die Einsicht in die Daten aller Personen möglich war, die seit Einführung des KIS in dem Krankenhaus behandelt wurden. Die Mehrheit der Häuser folgt dem Prinzip, dass der Zugriff auf Patientendaten pauschal allen Ärztinnen und Ärzten, Pflege- und Funktionskräften eingeräumt wird, die in Zukunft wahrscheinlich oder möglicherweise mit der Behandlung der Patientin oder des Patienten zu tun haben könnten (Prinzip des „weißen Kittels").

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten dagegen, dass ein Zugriff auf Patientendaten grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Patientinnen und Patienten behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die vorgefundenen Zugriffsmöglichkeiten gehen jedoch deutlich über den erforderlichen Umfang hinaus und sind als datenschutzrechtlich unzulässig abzulehnen.

Die Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten durch die Krankenhäuser hat sich an der konkreten Behandlungssituation der einzelnen Patientinnen und Patienten und nicht an der administrativen und funktionalen Gliederung des Krankenhauses zu orientieren:

- Der Zugriff auf die Daten ist nach der Erforderlichkeit für die Aufgabenerfüllung der zugreifenden Person zu differenzieren. Dabei ist nach Behandlungsrolle, -ort und -zeit zu unterscheiden.
- Patientinnen und Patienten sind zu jedem Zeitpunkt ihrer Behandlung sowohl fachlich als auch räumlich einer Ärztin oder einem Arzt bzw. einer Gruppe von Ärzten zugeordnet. Nach dieser Zuordnung bestimmen sich die Schranken für den lesenden wie schreibenden Zugriff auf die Patientendaten. Diese Schranken schließen den Bereitschaftsdienst ein.

26 Vgl. 7.2.3

- Für das pflegerische Personal bedeutet die Orientierung am Behandlungszusammenhang, dass es grundsätzlich nur die Daten der Patientinnen und Patienten der Station einsehen kann, auf der es eingesetzt ist.
- Ein Notfallzugriff von Ärztinnen und Ärzten auf die Daten aller Patientinnen und Patienten, mit denen sie potenziell in Berührung kommen können, ist zu gewährleisten. Er unterliegt jedoch besonderen Kontrollerfordernissen.
- Der Zugriff auf die Akten entlassener Patientinnen und Patienten ist nach Ablauf eines angemessenen Zeitraums nach Abschluss einer Fallbehandlung nur einem eingeschränkten Personenkreis und nur für bestimmte, gesetzlich zulässige Zwecke oder mit Einverständnis der Patientinnen und Patienten z. B. für die klinische Forschung gestattet.

Darüber hinaus muss die Patientin oder der Patient nachvollziehen können, wer auf ihre oder seine Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat[27]. Weiterhin ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Zur Erreichung dieser Zwecke hat regelmäßig eine Protokollierung sowohl schreibender als auch lesender Zugriffe auf Patientendaten zu erfolgen.

Diese bei der Ausgestaltung von Zugriffskonzepten zu beachtenden Grundsätze haben wir den von uns bereits geprüften Krankenhäusern mitgeteilt. Wir haben empfohlen, als ersten Schritt die Notwendigkeiten des Zugriffs auf Patientendaten aus fachlich-medizinischer Sicht zu bestimmen. Es ist eine primär ärztliche Entscheidung, wer in den Kreis der Behandelnden einer Patientin oder eines Patienten aufgenommen werden muss. Ausdrücklich wird diese Entscheidung bei der Übergabe der Behandlung an eine Kollegin oder einen Kollegen oder deren konsiliarischer Hinzuziehung getroffen. Implizit ist sie in der Zuweisung von Patientinnen und Patienten zu Funktionseinheiten des Krankenhauses und in der Anordnung von diagnostischen und therapeutischen Leistungen enthalten. Und auch bei der Erbringung von ärztlichen Leistungen im Bereitschaftsdienst oder in Notsituationen ergibt sie sich aus dem Handeln der Ärztin oder

27 Urteil vom 17. Juli 2008 – no. 20511/03, I. versus Finland

des Arztes. Stehen die Notwendigkeiten des Zugriffs fest, besteht der nächste Schritt darin, sie in den technischen Systemen abzubilden. Die Möglichkeiten, welche hierzu von den eingeführten Krankenhausinformationssystemen angeboten werden, variieren ebenso stark wie die Handhabbarkeit der Einschränkung und Kontrolle der Zugriffe. Ein Krankenhausbetrieb lässt sich jedoch nur mit hierzu geeigneter Software datenschutzfreundlich führen.

Die Software-Hersteller sind daher in der Pflicht, in ihren Systemen die Abbildung einer behandlungs- bzw. patientenbezogenen Zugriffslogik sowie eine durchgängige Zugriffsprotokollierung zu ermöglichen und durch die Ergonomie ihrer Produkte gelebten Datenschutz zu unterstützen. Nur datenschutzfreundliche Systeme werden sich in diesem sensitiven Bereich langfristig am Markt durchsetzen. Nicht zuletzt sind Politik und Selbstverwaltung aufgerufen, im Rahmen des Systems der gesetzlichen Krankenversicherung die finanziellen Voraussetzungen für eine datenschutzgerechte Gestaltung der Krankenhausabläufe und der sie unterstützenden technischen Systeme zu schaffen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf die bestehenden Defizite hingewiesen[28] und eine Arbeitsgruppe unter unserem Vorsitz ins Leben gerufen, welche sich vertieft mit dem Thema auseinandersetzen wird. Ziel ist es, die datenschutzrechtlichen Vorgaben für den Krankenhausbetrieb zu konkretisieren und einen Anforderungskatalog für Krankenhausinformationssysteme zu formulieren. Hierbei werden wir auf externe Expertise aus Wissenschaft, Fachgesellschaften und Anwendergruppen zurückgreifen. Die Ergebnisse werden wir den Krankenhausträgern zur Verfügung stellen, damit sie diese bei künftigen Neubeschaffungen und Weiterentwicklungen bestehender Systeme anwenden. Parallel zu der Arbeit in der Arbeitsgruppe werden wir unsere Prüfungen in Berlin fortsetzen und auf weitere Krankenhäuser ausweiten.

28 Vgl. Entschließung vom 8./9. Oktober 2009: Krankenhausinformationssysteme datenschutzgerecht gestalten!; Dokumentenband 2009, S. 17

Unsere Prüfungen haben ergeben, dass in Berliner Krankenhäusern teilweise weit über das für die medizinische Behandlung erforderliche Maß hinaus Zugriffe auf elektronische Patientenakten möglich sind. Dies ist mit datenschutzrechtlichen Vorgaben und der ärztlichen Schweigepflicht unvereinbar. Wir werden mit Nachdruck darauf hinwirken, dass Krankenhausinformationssysteme datenschutzgerecht gestaltet und betrieben werden.

## 2.4 Datenerhebung für den Europäischen Sozialfonds

Über den Europäischen Sozialfonds (ESF) werden Weiterbildungsmaßnahmen finanziert, die der Berufsorientierung für Schülerinnen und Schüler sowie der Integration von Arbeitslosen in den Arbeitsmarkt dienen. Diese Maßnahmen werden aus Mitteln des ESF, des Landes Berlin und den Agenturen für Arbeit finanziert. Nach den Förderbedingungen der Europäischen Union müssen alle ESF-finanzierten Maßnahmen geprüft werden. Dazu werden Daten über Teilnehmerinnen und Teilnehmer gesammelt, die über die Struktur, den Durchführungsstand und den Erfolg der Maßnahmen und damit den erfolgreichen Einsatz von ESF-Mitteln informieren. Zu den damit verbundenen Datenflüssen, mit denen wir uns bereits früher[29] auseinandergesetzt haben, erreichen uns immer wieder kritische Fragen. Die Träger der Qualifizierungsmaßnahmen (Maßnahmeträger) erheben u. a. Namen und Vornamen, Adresse, Geschlecht, Staatsangehörigkeit, Geburtsdatum, Muttersprache, Spätaussiedler, Vorliegen von Behinderungen, Angaben zur Jahrgangsstufe, Eintritts- und Austrittsdatum und Anzahl der absolvierten Teilnehmerstunden. Eine Weiterleitung dieser Daten erfolgte bislang personenbezogen an die das Programm umsetzenden Institutionen, die sog. Service- und Treuhandgesellschaften, und über diese an die Technische Hilfe des ESF in Berlin, die ECG GmbH.

Die jeweilige Service-/Treuhandgesellschaft ist dabei im Rahmen der Umsetzung z. B. des Programms „Berliner Programm Vertiefte Berufsorientierung (BVBO)“ in zweierlei Funktionen tätig: Zum einen handelt sie als beliehenes Unternehmen, soweit es um die Verwaltung und Ausreichung der Mittel an nachgeordnete Maßnahmeträger geht. Zum anderen ist sie Antragstellerin und

29 JB 1997, 4.4.1

Zuwendungsempfängerin im Zusammenhang mit der Beantragung der Mittel des ESF. Zuwendungsempfänger haben nach den zu § 44 Abs. 1 Landeshaushaltsordnung erlassenen Ausführungsvorschriften, die Bestandteil des Zuwendungsbescheides sind, einen Verwendungsnachweis zu führen. Nach den in den Zuwendungsbescheid einbezogenen Förderbedingungen des ESF hat der Maßnahmeträger zu gewährleisten, dass die Teilnehmerinnen und Teilnehmer ihren Wohnsitz im für das beantragte Ziel förderfähigen Gebiet des Landes Berlin haben. Er hat zum Zweck des Nachweises der tatsächlichen Qualifizierungsstunden Teilnehmerlisten zu führen. Zudem muss der Träger zum Zweck der Erfolgskontrolle sechs Monate nach Projektende über den Verbleib der Teilnehmenden berichten.

Die Service-/Treuhandgesellschaften beriefen sich bei der Datenerhebung gegenüber dem jeweiligen Maßnahmeträger auf eine Vorgabe der für die Steuerung und Finanzierung von BVBO-Maßnahmen zuständigen Senatsverwaltung und führten insbesondere aus, in den Förderbedingungen sei geregelt, dass für die Berichterstattung die dafür zur Verfügung gestellten „EDV-gestützten Unterlagen (TRS)“ zu verwenden seien. Die Angaben in diesem System seien obligatorisch. Nur bei Vollständigkeit der Daten und nur im Hinblick auf nachgewiesene Teilnehmerstunden könnten auch Projektkosten abgerechnet werden. Insoweit sei die jeweilige Service-/Treuhandgesellschaft berichts- und nachweispflichtig und könne diese Aufgabe nur bei Erhalt personenbezogener Daten der Teilnehmerinnen und Teilnehmer erfüllen.

Hinter der Abkürzung TRS verbirgt sich ein sog. Teilnehmer-Registrierungssystem, das bei der Technischen Hilfe des Landes Berlin, der ECG GmbH, geführt wird. Sowohl für die Gestaltung als auch für die Durchführung ist die Senatsverwaltung für Wirtschaft, Technologie und Frauen verantwortlich. Diese begründete die personenbezogene Datenerhebung damit, dass jedes Jahr ein Bericht für die EU-Kommission zu fertigen sei, der Nachweise über den Ablaufprozess der Fondsverwaltungen geben soll und für Prüfzwecke daher personenbezogene Daten der Teilnehmenden enthalten oder zumindest eine Rückverfolgung zur Personenbeziehbarkeit ermöglichen müsse.

Sowohl nach § 3 a BDSG als auch nach § 5 a Berliner Datenschutzgesetz (BlnDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an

dem Ziel der Datensparsamkeit auszurichten. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen unverhältnismäßigen Aufwand erfordert.

Wir haben der Senatsverwaltung für Wirtschaft, Technologie und Frauen daher empfohlen, dass zunächst nur die jeweiligen Bildungs(maßnahme)träger die erforderlichen Daten erheben, speichern und nutzen und anschließend diese Daten in pseudonymisierter Form (jeder Teilnehmer erhält eine Kennziffer) an die Service-/Treuhandgesellschaften weitergeben. Sollte es bei einer Prüfung zu Unklarheiten oder Zweifeln kommen, könnte die Service-/Treuhandgesellschaft sich an den jeweiligen Bildungsträger wenden und die personenbezogenen Daten der Teilnehmerin oder des Teilnehmers zu Prüfzwecken verlangen.

Die Senatsverwaltung teilte uns mit, dass Bedenken gegen eine derartige Pseudonymisierung nicht bestünden, solange im Rahmen von Vor-Ort-Prüfungen eine individuelle Zuordnung eines Schlüssels (Zusammenführung von Kennziffer und personenbeziehbaren Daten) möglich ist und ansonsten die für die Evaluierung erforderlichen statistischen Aggregate verfügbar sind.

Derzeit laufen die Entwicklungsarbeiten am neuen IT-Begleitsystem, in dem auch das Verfahren der Pseudonymisierung programmiert wird. Die Pseudonymisierung personenbezogener Daten von Teilnehmenden an ESF-Maßnahmen erfolgt dann im Teilnehmer-Registratursystem (TRS) des IT-Begleitsystems. Das TRS, in das sowohl die Servicegesellschaften als auch die Senatsverwaltung für Wirtschaft, Technologie und Frauen als Verwaltungsbehörde für den ESF zu Zwecken der Programmsteuerung, Berichterstattung und Evaluation Einblick haben, weist Anschrift und Geburtsdatum jeder Teilnehmerin und jedes Teilnehmers aus, nicht jedoch Vor- und Zunamen, welche ausschließlich dem Maßnahmeträger bekannt sind. Die Pseudonymisierung wird also künftig bereits beim Bildungs- bzw. Maßnahmeträger erfolgen. Eine Weitergabe oder Übermittlung der Daten der Teilnehmenden findet nicht mehr statt.

Dagegen ist die Datenerhebung, -verarbeitung und -nutzung der eingangs genannten personenbezogenen Daten der Teilnehmenden durch den jeweiligen Maßnahmeträger zulässig. Für den Europäischen Sozialfonds sind Informationen über die Teilnehmenden der Fördermaßnahmen die grundlegende Basis

der finanziellen und inhaltlichen Begleitung und Bewertung. Rechtsgrundlagen hierfür sind die Verordnung (EG) Nr. 1083/2006 des Rates[30] und die Verordnung (EG) Nr. 1828/2006 der Kommission[31]. Diese sehen auf europäischer Ebene aber nur die Erhebung von zahlenmäßigen und aufgeschlüsselten Angaben zu den Teilnehmenden an ESF-Vorhaben vor[32].

Um diese Angaben auf einer einheitlichen Datenbasis zusammenstellen zu können, dürfen die Maßnahmeträger personenbezogene Daten erheben, aber nicht pauschal an andere Stellen übermitteln. Die Datenerhebung dient folgenden Zwecken:

- Der Name und Vorname der teilnehmenden Person, die als Endbegünstigte von dem Einsatz der EU-Mittel profitieren soll, werden erhoben, um überprüfen zu können, wer gefördert worden ist.
- Die Adresse der teilnehmenden Person wird erhoben, um die geforderte Evaluierung nach dem Einsatz der ESF-Mittel für diese Person vornehmen zu können (Teilnehmerbefragung) und um die Zugehörigkeit zur vorgesehenen Zielgruppe zu prüfen.
- Das Geburtsdatum der teilnehmenden Person wird erhoben, um die für den Nachweis der Altersstruktur erforderlichen Daten liefern zu können.
- Das Eintritts- und Austrittsdatum von Individuen in die Maßnahme wird erhoben, um die durchgeführten Qualifizierungs- oder Beratungsstunden der Projektlaufzeit zuordnen zu können.

Im Ergebnis ist festzustellen, dass die Erhebung, Verarbeitung und Nutzung der eingangs genannten personenbezogenen Daten der Teilnehmenden nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG durch den Maßnahmeträger erforderlich und damit zulässig sind. Überwiegende schutzwürdige Belange der Betroffenen stehen nicht entgegen. Die Datenübermittlung an Servicegesellschaften und die ECG GmbH (Technische Hilfe des ESF in Berlin) erfolgt pseudonymisiert nach § 3 Abs. 6a BDSG und ist datenschutzrechtlich nicht zu beanstanden.

30 ABl. L 210 vom 31. Juli 2006, S. 25

31 ABl. L 371 vom 27. Dezember 2006, S. 1

32 Vgl. Anhang XXIII zur VO Nr. 1828/2006

Wir haben die Senatsverwaltung für Wissenschaft, Technik und Frauen gebeten, aufgrund der Vielzahl von Bürgereingaben die erreichten Änderungen im Verfahren auch bei den Treuhandgesellschaften sowie insbesondere bei den Bildungsträgern zu kommunizieren, damit die Teilnehmenden über den Zweck und das Verfahren der Datenerhebung ausreichend informiert werden. Die Senatsverwaltung teilte uns mit, das „Handbuch für die Umsetzung des OP ESF Berlin 2007“ werde aktualisiert. Die Verwaltungen sollen Projektträger in Zuwendungsbescheiden dazu verpflichten, Teilnehmende entsprechend zu unterrichten.

Die Daten von Personen, die an Förderprojekten im Rahmen des Europäischen Sozialfonds (ESF) teilnehmen, dürfen von den Maßnahmeträgern verarbeitet werden, soweit dies für eine Evaluation der Förderung erforderlich ist. An die Servicegesellschaften und die Technische Hilfe des ESF in Berlin sind diese Daten nur pseudonymisiert zu übermitteln. Dies wird künftig informationstechnisch unterstützt.

## 2.5 Private Meldedatenpools zur Adressermittlung

Versandhäuser, Versicherungen, Inkasso- und andere Unternehmen nehmen oft zur Ermittlung der Adressen von Bestellern, Schädigern oder Schuldnern die Dienstleistung eines erwerbsmäßigen Adressmittlers in Anspruch. Dieser holt im Auftrag des Unternehmens bei der zuständigen Meldebehörde eine Melderegisterauskunft ein und gibt das Ergebnis an den Auftraggeber weiter. Mittlerweile gibt es erwerbsmäßige Adressmittler, die darüber hinaus die Ergebnisse der Melderegisterauskünfte in einer eigenen Datenbank speichern, um ihren Kunden eine schnellere und oftmals billigere Auskunft zu erteilen. Dieses Sammeln von Daten wird auch als „Pooling“ bezeichnet. Das Geschäftsmodell des „Pooling“ hat unter den Datenschutzbeauftragten des Bundes und der Länder eine Diskussion ausgelöst, ob dieses rechtlich zulässig ist. Das haben wir zum Anlass genommen, ein in Berlin ansässiges Unternehmen einer Kontrolle nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) zu unterziehen. Schwerpunkte der Kontrolle waren die drei Bereiche Geschäftsmodell, förmliche Anforderungen des Datenschutzes und technisch-organisatorische Maßnahmen nach § 9 BDSG.

**Geschäftsmodell**

Das geprüfte Unternehmen bietet zunächst die Dienstleistung an, eine einfache Melderegisterauskunft bei der zuständigen Meldebehörde einzuholen. Dazu muss die Kundschaft die gesuchte Person durch Angabe mehrerer Merkmale hinreichend bestimmen und folgende Daten anliefern: Eindeutiges Aktenzeichen, Vor- und Nachnamen, letzte bekannte Anschrift mit Straße, Hausnummer, Postleitzahl und Ort und – wenn vorhanden oder bekannt – Titel, Geschlecht, Namenszusätze und Geburtsdatum. Mit diesen Angaben wird die einfache Melderegisterauskunft bei der zuständigen Meldebehörde eingeholt. Das Ergebnis wird dann einerseits der Kundschaft mitgeteilt und andererseits in einer Datenbank (Datenpool) im Unternehmen für einen Zeitraum von sechs Monaten gespeichert. Das Unternehmen bietet eine weitere Dienstleistung zur Adressmittlung über diesen Datenpool an. Die Angaben der Kundin oder des Kunden über die gesuchte Person sind identisch mit denen, die bei der Einholung der einfachen Melderegisterauskunft bei den Meldebehörden notwendig sind. Die Angabe der Adresse der gesuchten Person ist bei der Adressmittlung über den Datenpool zwingend erforderlich. Wird die gesuchte Person im Datenpool mit der angegebenen Adresse gefunden, wird diese bestätigt. Wird die gesuchte Person im Datenpool gefunden, ist dort jedoch mit einer anderen Adresse verzeichnet, wird automatisch eine einfache Melderegisterauskunft bei der zuständigen Meldebehörde veranlasst. Der Kundschaft wird das Ergebnis der Melderegisterauskunft mitgeteilt und nicht die Daten aus dem Datenpool. Es geht also stets nur um die Frage, ob die oder der Betroffene noch an der angegebenen Adresse gemeldet ist oder nicht.

Hinsichtlich der Speicherung der Daten im Datenpool stellt sich die Frage, ob sie rechtmäßig ist. Nach § 29 Abs. 1 Satz 1 Nr. 2 BDSG ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

Zunächst ist zu klären, ob das Melderegister, soweit es Daten enthält, die in einer einfachen Melderegisterauskunft mitgeteilt werden, eine allgemein zugängliche Quelle ist. Diese Frage ist zu bejahen, denn nur bei der erweiterten Melderegisterauskunft ist ein berechtigtes Interesse der Anfragenden erfor-

derlich. Die Tatsache, dass der Meldebehörde ein Ermessen zusteht, das jedenfalls bei einfachen Melderegisterauskünften in der Regel auf Null reduziert ist, spricht nicht gegen den Charakter als öffentlich zugängliche Quelle.

Aus melderechtlicher Sicht stellt sich darüber hinaus die Frage, ob schutzwürdige Belange der Meldepflichtigen beeinträchtigt werden. Das wäre möglich, wenn das Unternehmen durch die Datenerhebung oder den weiteren Umgang mit den beauskunfteten Daten, insbesondere durch die Bildung eines Datenpools, datenschutzrechtliche Sicherungen im Meldegesetz gefährden, z. B. die Rechte der Betroffenen vereiteln oder ihre Ausübung erschweren würde. Hierzu zählt die Auskunftssperre nach § 28 Abs. 5 Berliner Meldegesetz, die einzutragen ist, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass einer Person durch die Melderegisterauskunft Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann.

Bei einer Auskunftssperre nach einem Umzug, und dies ist der Regelfall, ergibt sich keine Schlechterstellung der Betroffenen, da bei einer Melderegisterauskunft die Auskunftssperre greifen würde und keine solche Auskunft erteilt wird. Daten, die mit einer Auskunftssperre versehen sind, werden nicht im Datenpool des Unternehmens gespeichert. In den seltenen Fällen einer Auskunftssperre ohne Umzug ergibt sich ebenfalls keine Schlechterstellung der Betroffenen, weil die anfragende Kundschaft die Adresse bereits kennt, denn sie ist als Pflichtangabe zur Adressmittlung aus dem Datenpool zwingend erforderlich.

Da das Melderegister hinsichtlich der einfachen Melderegisterauskunft eine allgemein zugängliche Quelle ist und schutzwürdige Belange der Betroffenen nicht offensichtlich überwiegen, kann das Geschäftsmodell einschließlich der Anlage eines Adresspools auf § 29 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden.

Allerdings ist die Übermittlung der gepoolten Daten an Dritte nur zulässig, wenn der Dritte ein berechtigtes Interesse glaubhaft dargelegt hat[33]. Die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung sind vom Adressmittler aufzuzeichnen[34]. Ein Verstoß gegen diese Vorschrift ist eine Ordnungswidrigkeit.

33 § 29 Abs. 2 Satz 1 Nr. 1 BDSG
34 § 29 Abs. 2 Satz 3 BDSG

### Organisation des Datenschutzes

Im Rahmen der Kontrolle haben wir auch die Umsetzung der gesetzlichen Anforderungen zur inneren Organisation des Datenschutzes geprüft. Dazu gehören der betriebliche Datenschutzbeauftragte, die Meldepflicht zum Verfahrensverzeichnis, die Verpflichtung zum Datengeheimnis und die Gewährleistung der Rechte der Betroffenen.

Zum Zeitpunkt der Prüfung war der Leiter der Datenverarbeitung und Systemverwaltung betrieblicher Datenschutzbeauftragter des Adressmittlers. Er verfügt über ausgezeichnete Kenntnisse des technischen Datenschutzes und der IT-Sicherheit. In rechtlichen Fragen beschränkt er sich auf die Kenntnis des Bundesdatenschutzgesetzes. Allerdings wird das Unternehmen von einer Rechtsanwaltskanzlei unterstützt, die auf IT-Recht und damit auch Datenschutzrecht spezialisiert ist. Als Leiter der Datenverarbeitung und Systemverwaltung ist der Datenschutzbeauftragte jedoch Interessenkonflikten ausgesetzt, die ihn für dieses Amt ungeeignet machen. Das ist ein Mangel nach § 4 Abs. 2 BDSG, der allerdings inzwischen durch Bestellung eines anderen betrieblichen Datenschutzbeauftragten behoben wurde. Da der Mangel schon vor unserer Kontrolle erkannt und inzwischen auch behoben ist, haben wir von der Verfolgung als Ordnungswidrigkeit abgesehen.

Da die beim Adressmittler gepoolten Daten zum Zwecke der Übermittlung ohne Kenntnis der Betroffenen gespeichert sind, sind sie nach § 33 Abs. 1 Satz 2 BDSG von der erstmaligen Übermittlung zu benachrichtigen. Diese gesetzliche Anforderung befolgt das Unternehmen bisher nicht. Hierin liegt eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 8 BDSG. Eine Verfolgung dieser Ordnungswidrigkeit wird von uns davon abhängig gemacht, ob das Unternehmen in Zukunft der Benachrichtigungspflicht nachkommt.

### Technisch-organisatorische Maßnahmen nach § 9 BDSG

Das Ergebnis der technisch-organisatorischen Kontrolle ausnahmsweise mal vorweg: Dabei wurden keine datenschutzrechtlichen Mängel festgestellt. Die Datenverarbeitung erfolgt auf einem sehr hohen Sicherheitsniveau.

Die eingesetzte Hard- und Software teilt sich auf die Räume des erwerbsmäßigen Adressmittlers und einen externen Dienstleister auf. Die Server stehen bei einem auf Server Hosting spezialisierten Dienstleister, der die höchste Sicher-

heitsstufe garantiert. Alle personenbezogenen Daten, die im Rahmen der Auskunftsdienste des Adressmittlers verarbeitet werden, werden ausschließlich auf den Servern des externen Dienstleisters verschlüsselt gespeichert. Der Zugriff auf die Daten erfolgt sowohl für den Adressmittler als auch den Kunden webbasiert und ist verschlüsselt. Beim Adressmittler kommen im Produktionsbetrieb ausschließlich Thin Clients zum Einsatz, die nicht über Laufwerke verfügen. Ein Anschluss externer Speichermedien ist nicht möglich. Ein eventuelles Kopieren und Abspeichern personenbezogener Daten wird damit verhindert. Die Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 BDSG ist gewährleistet.

Die Server beim externen Dienstleister befinden sich in einem Sicherheitsbereich. Der Zutritt ist durch biometrische Schlüssel, Alarmanlage, Sicherheitspersonal und ein Zugangskartenkontrollsystem gesichert. Der Zutritt wird protokolliert. Beim Adressmittler wird der Zutritt durch eine in verschiedene Sicherheitsbereiche eingeteilte Schließanlage gesichert. Alle Büroräume verfügen über eine Alarmanlage. Die Zutrittskontrolle nach Nr. 1 der Anlage zu § 9 BDSG ist sichergestellt. Die Arbeitsplätze beim Adressmittler sind passwortgeschützt, und es gibt strenge Vorgaben zur Passwortgestaltung. Weiterhin kommen passwortgeschützte Bildschirmschoner zum Einsatz. Um Zugriffe aus dem Internet heraus zu verhindern, werden Virenschutzprogramme und gestaffelte Firewalls eingesetzt. Die Zugangskontrolle nach Nr. 2 der Anlage zu § 9 BDSG ist gewährleistet. Zur Umsetzung der Zugriffskontrolle existiert ein detailliertes Berechtigungskonzept. Es steuert den Zugriff auf alle Komponenten des Produktionssystems. Zur Sicherstellung der Eingabekontrolle erfolgt eine Protokollierung der Dateneingaben, Datenänderungen und Datenlöschung. Um eine hohe Verfügbarkeit zu gewährleisten, ist der Produktionsserver gespiegelt. Es erfolgt eine tägliche Datensicherung.

Die Kontrolle eines Berliner Adressmittlers ergab, dass das Speichern von Melderegisterauskünften in einem Datenpool zum Zwecke einer späteren Übermittlung für einen begrenzten Zeitraum zulässig ist, wenn die Betroffenen von der erstmaligen Übermittlung und der Art der übermittelten Daten benachrichtigt werden. Die ergriffenen technisch-organisatorischen Maßnahmen sind vorbildlich, das Sicherheitsniveau damit sehr gut.

## 2.6 Datenschutz und Virtualisierung

Kaum ein technischer Begriff ist so facettenreich wie der der Virtualisierung. So besteht schon jetzt die Möglichkeit, ein zusätzliches „virtuelles Leben“ am Computer zu führen. Viele Bereiche der Informationstechnologie werden „virtualisiert“. Es gibt bereits seit mehr als 30 Jahren das Konzept der „virtuellen Speicherung“. Sehr aktuell, mittlerweile weit verbreitet und von großer Bedeutung für die Sicherheit der Datenverarbeitung ist das Konzept der Rechnervirtualisierung. Dabei können mehrere virtuelle Rechner, auch mit unterschiedlichen Betriebssystemen, parallel auf einer gemeinsamen physikalischen Rechnerplattform betrieben werden.

Virtualisierungstechniken werden bereits seit geraumer Zeit sowohl in professionellen Umgebungen als auch von Privatanwendern genutzt. Diverse kommerzielle Anbieter, aber auch die Open-Source-Gemeinde, bieten den Einstieg in die Welt der Virtualisierung kostenfrei an. Die Einsatzmöglichkeiten sind vielfältig. Sie reichen von der Möglichkeit, ein neues Betriebssystem zu erproben, bis hin zum Aufbau einer „virtuellen Surfstation“, die die Risiken der Nutzung des World Wide Web minimieren kann. Angesichts der Vielfalt von Anbietern gibt es auch Unterschiede bei den Verfahren, die eine Virtualisierung ermöglichen.

Bei der Paravirtualisierung wird zwischen der Hardware und dem Betriebssystem, das im Normalfall direkt mit der Hardware kommuniziert, eine Zwischenschicht (Virtualisierungsschicht) eingerichtet. Damit die Kommunikation zwischen Betriebssystem und Virtualisierungsschicht reibungslos funktioniert, ist eine Anpassung des Betriebssystemkerns erforderlich. Diese Anpassung ist gerade bei proprietären Betriebssystemen problematisch, deren Quellen nicht offenliegen (z. B. Windows). Die Anpassung kann in einem solchen Fall nur durch den Hersteller erfolgen. Der Vorteil dieser Technik liegt im relativ geringen Anteil der für die Virtualisierung benötigten Rechnerleistung.

Die Betriebssystem-Virtualisierung verfolgt einen anderen Ansatz. Bei dieser Technik ist das Wirts-Betriebssystem auch Verwalter der Rechnerressourcen, die von den Gast-Betriebssystemen über die Programmbibliotheken des Wirtes mitgenutzt werden. Diese Technik verbietet den Einsatz unterschiedlicher Gast-Betriebssysteme. Der Umstand, dass Wirts- und Gastbetriebssystem gleich

sein müssen, ist zugleich ein wesentlicher Nachteil. Vorteilhaft ist der geringe Anspruch an Systemkapazitäten durch ein Gastbetriebssystem, was eine verhältnismäßig hohe Zahl von virtuellen Instanzen ermöglicht.

Die Komplettvirtualisierung wird auch als „Systemvirtualisierung mittels Virtual Machine Monitor (VMM)“ bezeichnet. Virtuell wird jedem Gast-Betriebssystem unabhängig voneinander eine gleichartige Hardware zur Verfügung gestellt. Diese Virtualisierungsschicht fängt direkte Betriebssystemsaufrufe zur Hardware ab und verarbeitet diese durch Umsetzung in Aufrufe des Wirts-Betriebssystems. Im Unterschied zur Paravirtualisierung ist eine Anpassung des Gast-Betriebssystems nicht notwendig. Bei dieser Form der Virtualisierung ist es möglich, unterschiedliche Betriebssysteme (z. B. Windows und Linux) parallel auf einer Hardwareplattform zu betreiben. Die Emulation der Hardware hat aber ihren Preis in Form des relativ hohen Bedarfs an Ressourcen beim Wirts-Betriebssystem von bis zu 20 Prozent. Dieser Nachteil gegenüber den oben beschriebenen Virtualisierungskonzepten wird durch die höhere Flexibilität und den Verzicht auf Betriebssystemanpassungen bei den Gast-Betriebssystemen mehr als ausgeglichen, sodass die Komplettvirtualisierung das am meisten verbreitete Konzept ist.

### Vorteile der Virtualisierungstechnik aus Sicht des Datenschutzes

Besonders gut geeignet sind Virtualisierungslösungen für den Einsatz als Testumgebung. Es handelt sich dabei nicht um kritische Dienste, sodass die Ausfallsicherheit eine untergeordnete Rolle spielt. Geschwindigkeit ist hier nicht das oberste Bewertungskriterium, das Teilen von Ressourcen ist unproblematisch. Vielmehr bietet der virtuelle Betrieb die Möglichkeit, Systeme schnell wiederherzustellen. Es ermöglicht schnelles Umkonfigurieren, Wiederaufsetzen und Neustarten der eingesetzten Komponenten. Auch das Patch-Management[35] lässt sich mit einfachen Mechanismen besser steuern.

Die Möglichkeit der schnellen (Wieder-)Herstellung definierter Umgebungen eröffnet ein weiteres Anwendungsfeld. Insbesondere Privatanwender reizt bei der Virtualisierung vor allem die Möglichkeit, ohne Risiko im Web zu surfen und gefahrlos Software testen zu können. Das Betriebssystem, auf dem

35 Verfahren zur zentralisiert verwalteten Einspielung von Software-Updates zur Fehlerbeseitigung

die Virtualisierungs-Software aufsetzt, kann dabei grundsätzlich keinen Schaden nehmen. Der virtuelle PC läuft in einer Art abgeschotteter Umgebung, die als „Sandbox“ (Sandkasten) bezeichnet wird. Mittlerweile werden Softwareprodukte angeboten, die ausgewählte Applikationen, beispielsweise einen Browser, in einer „Sandbox“ ablaufen lassen, ohne dass hierfür ein komplettes Betriebssystem installiert werden müsste. Wird der Browser durch Viren oder Trojaner kompromittiert, lassen sich diese ohne größeren Aufwand restlos vom PC entfernen.

Generell liegen die Stärken von virtuellen Umgebungen in der deutlich höheren Verfügbarkeit von Systemen. Neben den bereits angeführten Gründen sind eine einfachere und schnellere Notfallwiederherstellung[36] sowie das Entfallen der Ausfallzeiten während einer Hardwarewartung oder eines Hardwarewechsels die wohl maßgeblichen Vorteile im Bereich Datensicherheit und Datenschutz. Sie liegen im Wesentlichen darin, dass durch die Loslösung des Betriebssystems von der Hardware diese problemlos ausgetauscht werden kann.

### Probleme beim Einsatz von Virtualisierungsszenarien

Schwachstellen gibt es in so gut wie allen Systemen und Anwendungen, selbst in den allgemein als sicher geltenden virtuellen Umgebungen. Bereits 2006 wurden drei Techniken[37] präsentiert, die die Schutzmechanismen virtueller Technologien effektiv aushebelten. Bis heute sind diese Techniken weiterentwickelt und zum Teil komplett überarbeitet worden. Im Ergebnis könnten moderne Schädlinge ein laufendes Windows-Betriebssystem unbemerkt in eine virtuelle Umgebung verschieben, ohne dass es vom Anwender bemerkt würde. Die praktische Umsetzung dieser Studien ist bis heute umstritten. Sie weisen auf einen neuen Typus von Schadsoftware hin, der „virtualisierten Malware“. Er nutzt die Hypervisortechnologie[38], um sich selbst oberhalb des infizierten Betriebssystems zu verstecken, und ist somit in einem infizierten System schwer nachweisbar. Die Bedrohung durch virtualisierte Malware ist real.

36 Englischer Fachbegriff: Disaster Recovery

37 Bei den Techniken handelte es sich um Proof-of-Concept-Rootkits: das Virtual-Machine-Rootkit Subvirt (PDF), das Intel-VT-x/Vanderpool-Rootkit Vitriol (PDF) und das Virtualisierungs-Rootkit Blue Pill.

38 Der Hypervisor ist die eigentliche Virtualisierungssoftware.

Auch wenn der Einsatz von Virtualisierungstechniken, insbesondere im Bereich der „Sandbox“, als hinreichend sicher bezeichnet wird, gelten für Virtualisierungsprodukte die gleichen Gesetzmäßigkeiten wie für jede Software. Software kann immer Fehler enthalten, die Ansatzpunkte für Angriffe sein können. Virtualisierung bietet zudem völlig neue Angriffspunkte und erlaubt den Zugang zu einer weit größeren Zahl von Anwendungen als herkömmliche Server. Es ist daher notwendig, dass alle Schritte eingeleitet werden, um einen gleichwertigen Grad an Sicherheit zu erreichen, den eine physikalische Umgebung bietet. Im Kern besteht das Problem darin, dass virtuelle Infrastrukturen ständigen Veränderungen unterliegen. Es verbietet sich daher, mit den gleichen Sicherheitslösungen zu agieren wie bei herkömmlichen Infrastrukturen.

Virtualisierungstechniken bieten neue Möglichkeiten, die Verfügbarkeit von Rechnersystemen signifikant zu erhöhen. Im Gegenzug sind diese neuen Möglichkeiten, insbesondere wenn sie in produktiven Systemen zum Einsatz gelangen, im Rahmen einer Sicherheitskonzeption zusätzlich zu bewerten. Verfahren, die die Sicherheit physikalischer Rechner erhöhen, funktionieren nur bedingt in einer virtuellen Umgebung. Zusätzliche Maßnahmen sind in der Regel erforderlich.

# 3. Öffentliche Sicherheit

## 3.1 Kfz-Kennzeichenscanning



Der Studie des ADAC zum Kennzeichenscanning – Umsetzung und Vorgaben des Bundesverfassungsgerichts[39] – war zu entnehmen, dass die Berliner Polizei 2008 zwei Geräte für die automatisierte Erfassung und Auswertung von Kfz-Kennzeichen angeschafft hat, die allerdings bis Mai 2009 nicht zum Einsatz gekommen sind.

In der Einsatzanordnung für das Automatische Kennzeichen-Lese-System macht der Polizeipräsident deutlich, dass die Erfassung und Speicherung von Kennzeichendaten einen Eingriff darstellt, der einer konkreten gesetzlichen Ermächtigung bedarf. Es ist danach insbesondere nicht zulässig, solche Daten zur allgemeinen Gefahrenvorsorge oder zur Erstellung von Bewegungsbildern zu erheben. Das umfasst auch ein Verbot des dauerhaften Abgleichs mit dem Sachfahndungsbestand. Diese Auffassung teilen wir in vollem Umfang.

Der Polizeipräsident und die Senatsverwaltung für Inneres und Sport vertreten jedoch weiter den Standpunkt, dass in Ausnahmefällen der verdeckte Einsatz dieser technischen Mittel geboten und zulässig sein kann, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat von erheblicher Bedeutung begangen werden soll. Das begründen sie damit, dass die möglichen technischen Mittel im Gesetz[40] nicht abschließend aufgezählt sind und somit auch ein spezielles videografisches Gerät darunterfällt.

Dem können wir uns nicht anschließen. Die gesetzliche Regelung ist zum einen zu unbestimmt, weil sie nicht präzise genug regelt, welche Daten außer Kfz-Kennzeichen erhoben werden dürfen, und weil sie weder die spezifischen Anlässe zum heimlichen Einsatz des Kontrollmittels noch den Zweck der Erhebung festlegt. Weiterhin fehlen Regelungen zu Schutzvorkehrungen und zur

39 A. Roßnagel: Rechtsgutachten – Verfassungsrechtliche Bewertung der automatisierten Erfassung von Kraftfahrzeugkennzeichen nach dem Urteil des Bundesverfassungsgerichts vom 11. März 2008, ADAC-Studie zur Mobilität, März 2009

40 § 25 Abs. 1 Nr. 2 ASOG

automatisierten sofortigen Löschung der Daten Unbeteiligter. Insgesamt rechtfertigt das Allgemeine Sicherheits- und Ordnungsgesetz nicht den heimlichen Einsatz von Kfz-Kennzeichenscannern, weil es insoweit nicht den Anforderungen genügt, die das Bundesverfassungsgericht formuliert hat[41].

Die Befugnisse zur Datenerhebung durch den verdeckten Einsatz technischer Mittel müssen hinreichend bestimmt und verhältnismäßig sein. Für den Einsatz von Geräten zur automatisierten Erfassung von Kfz-Kennzeichen zu Zwecken der Gefahrenabwehr fehlt in Berlin eine verfassungskonforme Rechtsgrundlage.

## 3.2 Datei „Gewalttäter Sport"

Aus der Praxis

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat seit Jahren in Bezug auf INPOL-Verbunddateien das Fehlen einer Rechtsverordnung nach § 7 Abs. 6 Gesetz über das Bundeskriminalamt (BKAG) moniert. Nach dieser Vorschrift bestimmt das Bundesministerium des Innern (BMI) mit Zustimmung des Bundesrates durch Rechtsverordnung das Nähere über die Art der Daten, die nach §§ 8, 9 BKAG gespeichert werden. Dem hat das BMI entgegengehalten, dass die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, sondern im Hinblick auf die übrigen Regelungen des BKAG nur deklaratorische Bedeutung habe.

Auch das Niedersächsische Oberverwaltungsgericht[42] hat festgestellt, dass es zurzeit für die Erhebung und Speicherung von Daten in der Verbunddatei „Gewalttäter Sport" an der notwendigen Rechtsverordnung fehlt[43]. Die Auffassung des BMI wird nach den Ausführungen des Gerichts weder durch den Wortlaut der einschlägigen Regelungen noch durch die Gesetzesmaterialien zum BKAG gestützt.

41 Urteil vom 11. März 2008, BVerfGE 120, 378

42 Entscheidung vom 16. Dezember 2008 – 11 LC 229/08

43 Vgl. auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009: Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage, Dokumentenband 2009, S. 13.

Das BMI hält auch nach der Entscheidung des OVG Niedersachsen an seiner Auffassung fest. Mit Blick auf das anhängige Verfahren beim Bundesverwaltungsgericht wird allerdings vorsorglich am Entwurf einer Verordnung gearbeitet.

**Wenn keine Rechtsvorschrift die Datenverarbeitung erlaubt, ist sie ohne Einwilligung der Betroffenen unzulässig. Das gilt auch für die Dateien im INPOL-Verbund.**

## 3.3 Leichtathletik-Weltmeisterschaft

Im Vorfeld der Leichtathletik-Weltmeisterschaft sind die freiwilligen Helferinnen und Helfer und sonstige Personen wie Journalisten, Beschäftigte privater Sicherheitsdienste oder Caterer, die zum sicherheitsempfindlichen Bereich Zugang erhalten wollten, vom Landeskriminalamt auf ihre Zuverlässigkeit überprüft worden. Diese Überprüfungen haben zu heftigen Diskussionen geführt, nachdem Journalisten der „tageszeitung“ ihr Einverständnis dazu verweigert hatten. Anders als zur Fußball-Weltmeisterschaft 2006 wurden diesmal die Beschäftigten der Feuerwehr nicht einbezogen. Offensichtlich wurde zumindest in diesem Punkt unsere Kritik aufgegriffen[44]. Sportlerinnen und Sportler, Funktionäre, Betreuungspersonal und Zuschauerinnen und Zuschauer sind nicht überprüft worden.

Das Akkreditierungsverfahren entsprach dem vor der Fußball-Weltmeisterschaft 2006 durchgeführten Verfahren[45]. Mangels gesetzlicher Regelung basierte es auf der Einwilligung der Bewerberinnen und Bewerber, die ein entsprechendes Formular ausfüllen mussten. Das LKA hat nach einem selbst erarbeiteten Kriterienkatalog die Datenverarbeitungssysteme nach Erkenntnissen über die Bewerberinnen und Bewerber überprüft. Als Ergebnis wurde dem Veranstalter mitgeteilt, dass Erkenntnisse bzw. keine Erkenntnisse im Sinne des Kriterienkataloges vorlagen, auf deren Grundlage der Veranstalter über die Akkreditie-

44 JB 2006, 2.2
45 JB 2006, 2.2

rung entschieden hat. Sofern Erkenntnisse vorlagen, hat die sich bewerbende Person zeitgleich mit der Mitteilung an den Veranstalter eine Benachrichtigung darüber erhalten, dass Erkenntnisse im Sinne des Kriterienkataloges vorliegen und sie bei der Polizei eine Selbstauskunft[46] einholen kann.

Kriterien für Mitteilungen an den Veranstalter waren rechtskräftige Verurteilungen wegen Verbrechen oder Vergehen, die im Einzelfall nach Art oder Schwere geeignet sind, den Rechtsfrieden zu stören, soweit sie sich gegen das Leben, die Gesundheit oder die Freiheit einer oder mehrerer Personen oder bedeutende fremde Sach- oder Vermögenswerte richten. Straftaten im Bereich des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung, Staatsschutzdelikte oder gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangene Delikte führten ebenso zu Mitteilungen wie mehrfache Verurteilungen wegen anderer als solcher Straftaten von erheblicher Bedeutung oder Eintragungen in die Datei „Gewalttäter Sport“. Ferner konnte das der Fall sein bei sonstigen Erkenntnissen über laufende oder eingestellte Verfahren, oder wenn Staatsschutz-, Rauschgift- oder Erkenntnisse aus dem Deliktsbereich „Organisierte Kriminalität“ vorhanden waren, die darauf schließen lassen, dass die Person künftig solche Taten begehen wird. Die Verfassungsschutzbehörden und Nachrichtendienste waren in die Akkreditierungsverfahren einbezogen.

In der Sache halten wir an unserer Auffassung fest, dass Zuverlässigkeitsüberprüfungen nicht auf die Einwilligung der Betroffenen gestützt werden können[47]. Das Abgeordnetenhaus hat den Senat aufgefordert, bei der nächsten Senatsvorlage zur Änderung des ASOG eine klarstellende Regelung für Zuverlässigkeitsüberprüfungen und Akkreditierungsverfahren bei Großereignissen oder von Personen, die als Lieferanten oder Dienstleister Zutritt zu sicherheitsempfindlichen Einrichtungen benötigen, vorzusehen[48]. Die Umsetzung dieses Beschlusses wurde beim 8. ASOG-Änderungsgesetz allerdings versäumt.

Auch bekräftigen wir unsere Auffassung, dass die Beteiligung des Verfassungsschutzes und des Bundesnachrichtendienstes an dem Akkreditierungsverfah-

46 § 50 ASOG
47 JB 2007, 3.1.7
48 Vgl. Anhang 1

ren unzulässig ist. Die Zuverlässigkeitsüberprüfung ist eine Aufgabe der Gefahrenabwehr, die weder dem Verfassungsschutz noch dem Bundesnachrichtendienst obliegt. Die fehlende gesetzliche Aufgabenzuweisung für den Verfassungsschutz und den Bundesnachrichtendienst kann nicht durch die Einwilligung der Betroffenen ersetzt werden.

Insgesamt wurden bei der Leichtathletik-Weltmeisterschaft rund 15.200 Personen überprüft, davon etwa 3.400 Journalistinnen und Journalisten. Dabei lagen bei etwa 100 Personen Erkenntnisse im Sinne des Kriterienkataloges vor. Diese Fälle haben wir stichprobenartig überprüft. Zu einigen Fällen haben wir uns die Entscheidungen nochmals erläutern lassen. Sie haben sich am Kriterienkatalog orientiert. Unter den abgelehnten Bewerbungen waren Personen, die wegen Schwerstverbrechen zu langjährigen Haftstraften verurteilt waren. Alle im Zusammenhang mit der Zuverlässigkeitsüberprüfung angefallenen Daten sind inzwischen sowohl bei der Polizei als auch beim Veranstalter gelöscht worden.

Zuverlässigkeitsüberprüfungen können nicht auf die Einwilligung der Betroffenen gestützt werden. Daher ist eine gesetzliche Grundlage zu schaffen.

## 3.4 Abhören des Bürgertelefons

Ein Petent beschwerte sich darüber, dass sein Anruf über die Rufnummer des Bürgertelefons der Polizei (4664 4664) auf die Notrufleitung 110 weitergeleitet und das Gespräch dort aufgezeichnet worden war.

Der Polizeipräsident hat uns mitgeteilt, dass der den Anruf annehmende Beamte am Bürgertelefon während des Gesprächs mit dem Petenten keinen Konsens erzielen konnte, sodass der Hauptsachbearbeiter „Lage“ in die Gesprächsführung eintrat. Dieser war irrtümlich der Meinung, bei dem Gespräch handele es sich um einen 110-Notruf. Auf Nachfrage teilte er dem Beschwerdeführer mit, dass das Telefongespräch aufgezeichnet würde. Nachdem der Beamte seinen Irrtum bemerkt hatte, korrigierte er die Aussage unverzüglich und teilte dem Petenten mit, dass Gespräche mit dem Bürgertelefon der Polizei nicht aufgezeichnet werden.

Was den Beamten allerdings nicht bekannt war, ist die Tatsache, dass die über das Bürgertelefon geführten Gespräche zum fraglichen Zeitpunkt aufgrund eines Systemfehlers bei der Umstellung der Notrufabfrageeinrichtung (NrAbE) auf ein neues, digital-technisches System tatsächlich aufgezeichnet wurden.

Die Beschäftigten der Funkbetriebszentrale konnten nach Abschluss der Testphase und nach Übergang in den erweiterten Testbetrieb unter Realbedingungen davon ausgehen, dass die beauftragte Trennung zwischen den eingehenden Notrufen, die aufgezeichnet werden dürfen[49], und anderen Gesprächen (also auch die des Bürgertelefons), bei denen dies nicht erfolgen darf, gewährleistet war. Erst durch die Beschwerde des Petenten wurde der Systemfehler im Dezember 2008 bekannt. Daraufhin wurden die eingehenden Anrufe des Bürgertelefons technisch von der NrAbE getrennt und auf einer separaten Leitung auf zwei hierfür bereitgestellten Telefonapparaten geführt. Diese verfügen über keinerlei Applikationen zu einer Sprachdokumentation. Die Aufzeichnung eines Gespräches mit dem Bürgertelefon ist weder unmittelbar noch mittelbar im Wege der Weiterleitung auf einen anderen Aufnahmeplatz technisch möglich.

Die in dem fraglichen Zeitraum rechtswidrig aufgezeichneten Gespräche am Bürgertelefon wurden nach Ablauf von 42 Tagen automatisch gelöscht. Die Löschung der letztmalig am 12. Dezember 2008 aufgezeichneten Gespräche war am 23. Januar 2009 abgeschlossen.

Wir haben den Verstoß gegen § 46 a ASOG gegenüber der Senatsverwaltung für Inneres und Sport beanstandet. Nach dieser Vorschrift können die Polizei und die Ordnungsbehörden Anrufe über Notrufeinrichtungen auf Tonträger aufzeichnen. Eine Aufzeichnung von Anrufen im Übrigen ist nur zulässig, soweit die Aufzeichnung im Einzelfall zur Erfüllung der Aufgaben erforderlich ist. Die Aufzeichnungen sind spätestens nach drei Monaten zu löschen, es sei denn, sie werden zur Verfolgung von Straftaten benötigt oder die Tatsachen rechtfertigen die Annahme, dass die anrufenden Personen Straftaten begehen werden und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung ist.

49 § 46 a ASOG

Beim Bürgertelefon handelt es sich nicht um eine Notrufeinrichtung. Der Polizeipräsident hat dies in seiner Stellungnahme eingeräumt. Ferner handelte es sich nicht um einen Einzelfall, sondern um einen grundlegenden Systemfehler, der nunmehr beseitigt ist.

**Bei der Einführung von neuer Technik ist eine umfassende Qualitätsprüfung erforderlich.**

## 3.5 Videoüberwachung von Demonstrationen



Eine Bürgerin hat uns vorgetragen, in einem Gerichtsverfahren gegen sie sei bekannt geworden, dass ein verdeckt ermittelnder Beamter des Landeskriminalamts sie mit einer Digitalkamera bei einer Demonstration in Dresden gefilmt habe. Dabei soll er insbesondere die Teilnahme der Petentin dokumentiert haben. Bei dieser Demonstration sollen sich weitere verdeckt ermittelnde Beamte des Landeskriminalamts aufgehalten und ohne Vorliegen einer unmittelbaren Gefahr für die öffentliche Sicherheit digitale Filmaufnahmen von einzelnen Demonstrierenden angefertigt haben.

Tatsächlich wurden Berliner Polizisten zur Unterstützung der Dresdner Polizei bei dieser Demonstration eingesetzt. Sie haben die Bildaufnahmen bei bzw. am Rande der Demonstration offen – also nicht mit einer versteckten Digitalkamera – angefertigt. Die Beamten trugen Zivilkleidung.

Verdeckte Bildaufnahmen durch die Polizei bedürfen sowohl aus datenschutz- als auch aus verfassungsrechtlichen Gründen einer hinreichend bestimmten Rechtsgrundlage. Nach dem Versammlungsgesetz[50] darf die Polizei Aufnahmen von Teilnehmenden anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Eine Speicherung ist zur Verfolgung von Straftaten der Teilnehmenden oder im Einzelfall zur Gefahrenabwehr zulässig. Die Vorschrift regelt lediglich Bild- und Tonaufnahmen von Teilnehmern im Zusammenhang

50 § 12 a Abs. 1

mit öffentlichen Versammlungen, aber keine Voraussetzungen für die Zulässigkeit verdeckter Videoaufnahmen.

Staatliches Handeln bei der Grundrechtsausübung hat grundsätzlich transparent zu erfolgen. Verdeckte Bildaufnahmen bei Versammlungen dürfen jedenfalls nur die Ausnahme sein. Heimliche bzw. verdeckte Maßnahmen der Datenerhebung stellen einen tiefer gehenden Grundrechtseingriff dar als offen erfolgende Maßnahmen. Dies ergibt sich insbesondere daraus, dass sich Betroffene schlechter vor derartigen Eingriffen schützen und erst im Falle einer späteren Benachrichtigung Rechtsschutz erlangen können, da sie von der Maßnahme keine Kenntnis haben. Vor diesem Hintergrund bedürfen heimliche Maßnahmen der Datenerhebung einer besonderen Rechtfertigung und Kontrolle, weshalb beispielsweise derartige strafprozessuale Eingriffsbefugnisse regelmäßig einen Richtervorbehalt vorsehen. Das Versammlungsgesetz[51] sieht indes weder eine besonders hohe Eingriffsschwelle noch eine besondere Kontrolle bei der Inanspruchnahme dieser Befugnisse vor. Das spricht dafür, dass nur eine offene Datenerhebung zugelassen werden sollte. In die gleiche Richtung weist eine Auslegung unter Berücksichtigung des vom Bundesverfassungsgericht entwickelten Grundsatzes, dass wesentliche Bedingungen für Grundrechtseingriffe vom Gesetzgeber normenklar und möglichst präzise festgelegt werden müssen. Danach wäre eine Befugnis zur verdeckten Datenerhebung ausdrücklich zu regeln. Deshalb gehen wir davon aus, dass das Versammlungsgesetz nur eine offene Datenerhebung zulässt.

Verdeckt ist eine Maßnahme, wenn sie nicht als polizeiliche erkennbar ist. Dementsprechend müssen offene Eingriffe als polizeiliche Maßnahmen zu erkennen sein. Angesichts dessen erfolgt eine Bildaufnahme nach dem Versammlungsgesetz nicht nur dann verdeckt, wenn sie mit einer versteckten Kamera durchgeführt wird; es reicht vielmehr bereits aus, wenn die filmenden Polizeibediensteten nicht als solche zu erkennen sind, weil sie beispielsweise in Zivil agieren. Offen ist eine Maßnahme nach dem Versammlungsgesetz demnach nur, wenn ein als solcher erkennbarer Polizeibediensteter erkennbar filmt. In diesem Sinne hat auch der Bayerische Verwaltungsgerichtshof entschieden[52].

51 § 12 Abs. 1

52 Urteil vom 15. Juli 2008 – 10 BV 07.2143

Ferner darf die Wahl des Ortes nicht dazu führen, dass die Bildaufnahme von einer offenen zu einer verdeckten Maßnahme wird. Als problematisch erweist sich insoweit auch das Filmen aus Häusern heraus, aber auch das Filmen innerhalb von Versammlungen, da die Teilnehmer dort eine solche Maßnahme eher nicht erwarten werden.

Darüber hinaus ist zu berücksichtigen, dass das Bundesverfassungsgericht in seinem Brokdorf-Beschluss[53] die Bedeutung der Deeskalation betont hat und die Polizei grundsätzlich auf Distanz zu Versammlungen bleiben sollte, um deren unreglementierten, staatsfreien Charakter nicht zu gefährden. Zudem hat das Gericht wiederholt betont, dass Menschen durch eine staatliche Registrierung ihres Verhaltens davon abgehalten werden, von ihren Grundrechten (z. B. der Versammlungsfreiheit) Gebrauch zu machen. Vor diesem Hintergrund können Bildaufnahmen aus dem Versammlungsgeschehen heraus ebenfalls nur ausnahmsweise in Betracht kommen, z. B. wenn ihr Zweck von einem anderen Standort aus nicht erreichbar ist. Dies wird angesichts des heutigen Standes der Technik kaum einmal der Fall sein. Jedenfalls dürfen sie nicht dazu führen, dass das Filmen nicht mehr hinreichend als polizeiliche Maßnahme erkennbar ist.

Der Gesetzgeber war zwar ausweislich der Gesetzesmaterialien bei der Schaffung des § 12 a Versammlungsgesetz der Auffassung, dass Übersichtsaufnahmen zur Einsatzdokumentation sowie zu Ausbildungszwecken nicht unter diese Norm fallen würden, da das Ziel nicht die Identifizierung von Teilnehmenden sei. Außerdem griffen derartige Aufnahmen nicht in Grundrechte ein. Das ist angesichts des heutigen Standes der Technik nicht mehr vertretbar, da sich bei Verwendung digitaler Technik in aller Regel auch aus Übersichtsaufnahmen heraus einzelne Personen identifizieren lassen. Darüber hinaus liegt eine Übersichtsaufnahme schon begrifflich nicht vor, wenn einzelne Teilnehmende der Versammlung identifiziert werden können oder sollen.

Im Ergebnis halten wir daran fest, dass es nicht nur für verdeckte Bildaufnahmen Einzelner, sondern auch für Übersichtsaufnahmen bei Versammlungen einer gesetzlichen Grundlage bedarf, die das Grundrecht auf Versammlungsfreiheit nicht unverhältnismäßig einschränkt. Solange der (nach der Föderalismusreform zuständige) Landesgesetzgeber eine solche Regelung nicht geschaf-

53 vom 14. Mai 1985, BVerfGE 69, 315, 346

fen hat, sind solche Aufnahmen rechtswidrig. Insofern teilen wir auch nicht die Auffassung des Polizeipräsidenten, dass die Anfertigung von Übersichtsaufnahmen bis zur Schaffung einer Rechtsgrundlage zulässig ist. Er teilte mit, dass zwischen der Polizei und der Innenverwaltung ein Gedankenaustausch stattfindet, über dessen Ergebnis wir später unterrichtet werden.

**Bildaufnahmen, die Polizeibeamte in Zivil bei Demonstrationen machen, sind unzulässig.**

## 3.6 Datennutzung nach rechtswidriger Hausdurchsuchung

Aus der Praxis

Ein Petent wollte eine Tätigkeit als Dolmetscher bei der Staatsschutzkammer eines Gerichts in Sachsen-Anhalt übernehmen. Das dortige Landeskriminalamt hat in Berlin nachgefragt, ob dagegen Bedenken bestünden. Dazu hat die Berliner Polizei mitgeteilt, dass sie eine Wohnungsdurchsuchung beim Petenten durchgeführt habe.

Tatsächlich wurde die Wohnung des Petenten aufgrund eines Beschlusses des Verwaltungsgerichts Berlin durchsucht. Allerdings hat das Oberverwaltungsgericht Berlin-Brandenburg fast vier Monate vor der Datenübermittlung an das Landeskriminalamt Sachsen-Anhalt festgestellt, dass die Durchsuchungs- und Beschlagnahmeanordnung des Verwaltungsgerichts Berlin rechtswidrig war.

Die Polizei hat uns dazu mitgeteilt, dass ihr zum Zeitpunkt der Datenübermittlung die Entscheidung des Oberverwaltungsgerichts nicht bekannt gewesen sei. Sie hat erst durch uns von dieser Entscheidung Kenntnis erhalten. Daraufhin wurde geprüft, ob die Daten des Petenten für eine ordnungsgemäße Aufgabenerfüllung benötigt werden[54] mit dem Ergebnis, dass dessen Daten insgesamt gelöscht worden sind.

Die das Land Berlin in dem Verfahren vertretende Senatsverwaltung für Inneres und Sport hat keine Notwendigkeit gesehen, den Polizeipräsidenten über die

54 § 48 Abs. 2 ASOG

Entscheidung des Oberverwaltungsgerichts zu informieren. Der Polizeipräsident war nur auf Bitten der Senatsverwaltung in Amtshilfe tätig geworden.

Diese Auffassung teilen wir nicht, weil die Polizei nach § 42 Abs. 1 ASOG nur rechtmäßig erhobene personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen kann, soweit das zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Die Entscheidung des Oberverwaltungsgerichts hätte die Senatsverwaltung für Inneres und Sport zur Prüfung veranlassen müssen, ob eine weitere Speicherung der Daten erforderlich ist und ob unrichtige oder zu löschende Daten übermittelt worden sind. In diesen Fällen ist der empfangenden Stelle die Berichtigung, Sperrung oder Löschung mitzuteilen[55].

Mit der Feststellung des Oberverwaltungsgerichts, dass die Durchsuchung rechtswidrig war, waren die ursprünglich übermittelten Daten (der Hinweis im polizeilichen Informationssystem auf die Durchsuchung) zu löschen. Zwar kann die Mitteilung unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass dadurch schutzwürdige Belange der betroffenen Person beeinträchtigt werden[56]. Diese Voraussetzungen lagen aber nicht vor. Deshalb hätte eine Nachmeldung an die Polizei erfolgen müssen. Die Senatsverwaltung für Inneres und Sport wird die Rechtslage künftig beachten und den Polizeipräsidenten über gerichtliche Entscheidungen unterrichten.

Ordnungsbehörden und die Polizei haben nach erfolgter Datenübermittlung eine Nachberichtspflicht, wenn unrichtige, zu löschende oder zu sperrende Daten übermittelt wurden.

55 § 48 Abs. 5 ASOG
56 § 48 Abs. 5 Satz 2 ASOG

## 3.7 Der Polizeieinsatz in „Bild“



Einer Boulevard-Zeitung war zu entnehmen, dass die Polizei eine Razzia am Kottbusser Tor durchgeführt hat. Dabei wurden – offensichtlich im Beisein von Reportern – verschiedene Personen durchsucht. In zumindest einem Fall wurde vor Dritten auch der Intimbereich durchsucht und davon Fotos angefertigt.

Die Polizei teilte uns mit, dass bei diesem Einsatz im Bereich des Kottbusser Tors die Polizeibeamten von Reportern der Zeitung begleitet wurden. Bei dem Einsatz sind viele Personen der örtlichen Drogenszene überprüft worden. Für die erforderlichen Durchsuchungsmaßnahmen wurde ein für die Öffentlichkeit nicht zugänglicher und nicht einsehbarer Raum genutzt. In dem konkreten Fall wurde ein in der Vergangenheit bereits einschlägig als Drogendealer in Erscheinung getretener junger Mann überprüft. Er kannte aus einer Vielzahl vergleichbarer polizeilicher Maßnahmen das bevorstehende Prozedere. Da er nach Darstellung des verantwortlichen Polizeibeamten vor der Durchsuchungshandlung sein Einverständnis sowohl zur Anwesenheit der Journalisten als auch zur fotografischen Dokumentation äußerte, wurde den Journalisten die Anwesenheit und das Fotografieren im Durchsuchungsraum gestattet.

Der Polizeipräsident räumt ein, dass dies nicht hätte erfolgen dürfen. Auf die Zustimmung des Betroffenen kommt es hier nicht an. Voraussetzung für die journalistische Begleitung von polizeilichen Einsätzen ist die Unterzeichnung einer Vereinbarung, mit der sich der Vertragspartner verpflichtet, den Anweisungen der Polizei Folge zu leisten, insbesondere wenn diese der Anfertigung bestimmter Aufnahmen widersprechen. Die Einhaltung des vereinbarten Verfahrens wird dadurch sichergestellt, dass die Journalisten durch Beschäftigte der Pressestelle begleitet werden.

Der Polizeipräsident hat den Vorgang zum Anlass genommen, die Grenzen der journalistischen Begleitung polizeilicher Einsätze in den schon sehr restriktiven Regelungen der Behörde noch deutlicher aufzuzeigen und die genaue Beachtung in der Praxis durch Bedienstete der Pressestelle zu gewährleisten.

Auch bei polizeilichen Maßnahmen sind die Rechte der Betroffenen, insbesondere das Recht auf Achtung ihrer Würde, jederzeit zu wahren.

# 4. Melde-, Personenstands- und Ausländerwesen

## 4.1 Internetauskunftsserver für Privatpersonen (IASP)



Wir hatten darüber berichtet, dass das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) die Möglichkeit der Melderegisterauskünfte an Private über das Internet mittels des IASP realisiert hat[57]. Bei der Überprüfung des Verfahrens haben wir die Speicherung von Daten im Melderegister bemängelt, für die nach dem Meldegesetz keine Speicherungsbefugnis besteht.

Über den Katalog der Einzeldaten in § 2 Meldegesetz hinaus werden das früher gespeicherte Geburtsdatum, Hinweise zur letzten Eheschließung oder Begründung der letzten Lebenspartnerschaft bzw. deren Beendigung sowie des früheren Familienstandes gespeichert. Das ist ohne Einwilligung der Betroffenen unzulässig.

Auf unseren Vorschlag hat der Unterausschuss „Datenschutz und Informationsfreiheit“ und später das Abgeordnetenhaus den Senat aufgefordert, dafür zu sorgen, dass die Daten, für die keine gesetzliche Speicherungsbefugnis besteht, unverzüglich gelöscht werden, und dem Unterausschuss über die Umsetzung zu berichten[58]. Das alles hat das LABO keineswegs beeindruckt. Erst nachdem wir den Vorgang gegenüber der Senatsverwaltung für Inneres und Sport beanstandet und empfohlen haben, den Beschluss des Abgeordnetenhauses umgehend umzusetzen, wurde das LABO angewiesen, die Daten zu löschen. Bisher steht eine Mitteilung über den Vollzug noch aus.

Ohne Einwilligung der Betroffenen dürfen nur die im Meldegesetz ausdrücklich zugelassenen Daten im Melderegister gespeichert werden.

57 JB 2007, 4.1.3
58 Vgl. Anhang 1

## 4.2 DVO-Meldegesetz

Aus der Praxis

Seit Jahren fordern wir eine Änderung der Durchführungsverordnung zum Meldegesetz (DVO-Meldegesetz)[59]. Danach dürfen die jeweils zuständigen Stellen der Bezirksämter abschließend festgelegte Daten abrufen, soweit im Einzelfall die Kenntnis zur Erfüllung der dem Bezirksamt durch Rechtsvorschrift obliegenden Aufgaben erforderlich ist. Diese Regelung ist allerdings zu unbestimmt. Der Verordnungsgeber hat explizit festzulegen, welche Stelle des Bezirksamtes vor dem Hintergrund des funktionalen Behördenbegriffs[60] gemeint ist. Bei der Novellierung der DVO-Meldegesetz 2003 wurde diese Forderung aus Zeitgründen nicht mehr berücksichtigt. Es bestand aber mit der Senatsverwaltung für Inneres und Sport Einvernehmen darüber, dass das Problem in einer „zweiten Welle" angegangen wird.

Sechs Jahre später hat uns die Senatsverwaltung für Inneres und Sport einen Entwurf vorgelegt. Der zentrale Punkt dieser Änderungsverordnung ist die Schaffung einer generellen Zugriffsmöglichkeit aller Behörden und sonstigen öffentlichen Stellen auf die Grunddaten Familienname, Vorname, Doktorgrad, gegenwärtige Anschriften und ggf. die Tatsache, dass die Einwohnerin oder der Einwohner verstorben ist. Dagegen bestehen keine grundlegenden Einwände. Damit wird im Wesentlichen das Institut der einfachen Melderegisterauskunft an Private für den öffentlichen Bereich nachgebildet.

Private erhalten allerdings keine Auskunft, wenn eine melderechtliche Auskunftssperre[61] vorliegt. Daneben gibt es auch noch die Widerspruchsmöglichkeit der oder des Meldepflichtigen gegen Datenweitergaben an bestimmte Empfänger (wie an politische Parteien zum Zwecke der Wahlwerbung). Dieses Regulativ zwischen den Interessen der bei der Meldebehörde Anfragenden und den schutzwürdigen Belangen der Betroffenen wirkt nicht bei Datenübermittlungen innerhalb des öffentlichen Bereichs. Der Gesetzgeber ist davon ausgegangen, dass ein GefährdungsPotenzial für die Meldepflichtigen nur von Privaten – nicht aber von einer Behörde – ausgehen kann. Ein vergleichbares

59 JB 2003, 4.2.1; JB 2004, 4.2.1
60 § 4 Abs. 3 Nr. 1 BlnDSG
61 § 28 Abs. 5 MeldeG

Regulativ für die neu geschaffene Abrufmöglichkeit sämtlicher Behörden und sonstiger öffentlichen Stellen ist jedoch geboten, weil nur so die schutzwürdigen Belange der Betroffenen gewahrt werden können.

Ferner soll vielen Stellen der Zugriff auf über den Grunddatenbestand hinausgehende Datenfelder eröffnet werden. Die Einrichtung automatisierter Abrufverfahren ist eine Abweichung vom Grundprinzip der Datenerhebung bei Betroffenen. Das ist beim Zugriff auf die Grunddaten vertretbar, um Betroffene überhaupt erreichen zu können. Eine Erforderlichkeit[62] für die Schaffung dieser erweiterten Zugriffsmöglichkeiten wurde dagegen nicht plausibel dargelegt. Solange sie nicht überzeugend begründet wird, sollten diese Stellen – wie die übrigen Behörden und sonstigen öffentlichen Stellen – nur den Zugriff auf die Grunddaten erhalten.

Weiterhin gehen wir davon aus, dass technisch sichergestellt ist, dass nur nach bestimmten Personen gesucht werden kann, also Anfragen zu ganzen Häusern nicht möglich sind. Auch dürfen keine Phonetikprogramme eingesetzt werden, die zu einer Übermittlung von Daten zu ähnlich klingenden Namen führen. Die Erfahrungen mit solchen „Schrotschuss"-Programmen bei privaten Auskunfteien haben gezeigt, dass dabei häufig zu Unrecht Auskünfte über Dritte („zur Auswahl") erteilt werden.

Bei der Schaffung von über den Grunddatenbestand hinausgehenden Zugriffsmöglichkeiten auf das Melderegister sind die Empfänger und die Einzeldaten präzise festzulegen. Die Erforderlichkeit ist in jedem Einzelfall darzulegen. Der Grundsatz der Datenerhebung beim Betroffenen ist auch bei der Auskunftserteilung aus dem Melderegister zu beachten.

62 § 26 Abs. 3 MeldeG

## 4.3 Postsendungen nach Totgeburt

Aus der Praxis

Eine Frau hat uns in einem bewegenden Brief mitgeteilt, dass sie nach der Totgeburt ihres Kindes Schreiben der verschiedensten Einrichtungen erhalten hat (regelmäßig verbunden mit Glückwünschen zur Geburt des Kindes), wie z. B. vom Arbeitskreis Neue Erziehung den Elternbrief, vom Bundeszentralamt für Steuern die Mitteilung der Steueridentifikationsnummer für das Kind, von der Deutschen Rentenversicherung Informationen über die Rentenversicherungspflicht wegen Kindererziehung und vom Jugendamt.

Bei der Überprüfung haben wir festgestellt, dass das Standesamt der Meldebehörde die Tatsache der Geburt automatisiert übermittelt hat. Aufgrund einer nicht mehr nachvollziehbaren Fehlermeldung musste die Geburt – der Datensatz enthielt keinen Hinweis auf die Totgeburt – manuell in das Melderegister eingegeben werden. Wegen eines Programmfehlers war zu dieser Zeit in dem Verfahren AUTISTA[63] nicht erkennbar, wenn es sich bei einer Geburt um eine stille gehandelt hatte. Dieser Fehler ist inzwischen behoben worden. Aufgrund des Programmfehlers ist für das Kind ein Datensatz im Melderegister angelegt worden, der nicht hätte angelegt werden dürfen. Unmittelbar nach Bekanntwerden dieser Tatsache wurde der Datensatz des Kindes gelöscht. In der Zeit zwischen Anlage des Datensatzes und der Löschung sind die in den einschlägigen Rechtsverordnungen vorgesehenen regelmäßigen Datenübermittlungen durchgeführt worden.

So erhält das Gesundheitsamt des Bezirks für die Durchführung des Gesundheitsdienst-Gesetzes Kenntnis von Neugeborenen[64]. Die Meldebehörden übermitteln dem Bundeszentralamt für Steuern zum Zwecke der erstmaligen Zuteilung der Identifikationsnummer für jeden in ihrem Zuständigkeitsbereich registrierten Einwohner abschließend festgelegte Daten[65]. Der Steuerpflichtige ist über die Zuteilung eines Identifikationsmerkmals unverzüglich zu unterrichten[66]. Ferner übermitteln die Meldebehörden nach Speicherung einer Geburt

63 Automatisiertes Standesamt

64 Nr. 2 der Anlage 4 zu § 3 Nr. 1 DVO-Meldegesetz

65 § 139 b Abs. 6 Abgabenordnung (AO)

66 § 139 b AO

oder einer erstmaligen Erfassung eines Einwohners dem Träger der Rentenversicherung zur Erfüllung verschiedener Zwecke einen abschließenden Katalog von Daten in automatisierter Form (Rentenversicherungsmitteilung)[67]. Die Senatsverwaltung für Bildung, Wissenschaft und Forschung erhält nach der Registrierung von Neugeburten Daten des Kindes und der Mutter zum Versand der Elternbriefe des Arbeitskreises Neue Erziehung als pädagogisches Informationsmaterial für junge Eltern[68]. Das Anlegen eines Datensatzes für ein Neugeborenes löst automatisch diese Meldepflichten aus, die regelmäßig zu Handlungen der empfangenden Stelle führen.

Die Datenübermittlungen können unter datenschutzrechtlichen Aspekten nicht beanstandet werden, denn sie erfolgten aufgrund von Rechtsvorschriften. Ausgelöst wurde alles durch den inzwischen behobenen Programmfehler bei den Standesämtern. Das kann und wird der Frau nicht über den schmerzlichen Verlust ihrer Tochter hinweghelfen. Mit unserem Tätigwerden wollten wir lediglich versuchen, ihr die Zusammenhänge nahezubringen.

Der Fall zeigt zweierlei: Fehler in der Datenverarbeitung können schmerzliche und inakzeptable Folgen für die Betroffenen haben. Jede Geburt löst eine Vielzahl von Datenübermittlungen der Meldebehörde aus, die den wenigsten bekannt ist.

## 4.4 Auskunft über Weggezogene

Die Meldebehörde erteilt über aus Berlin weggezogene Einwohnerinnen und Einwohner Auskunft aus dem Melderegister auch zu der im Rückmeldeverfahren bekannt gewordenen neuen Anschrift.

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) hat das Verfahren mit Hinweis auf das nicht anwendbare Melderechtsrahmengesetz (MRRG) und den Referentenentwurf eines Bundesmeldegesetzes begründet. Danach darf die Meldebehörde Privaten Auskunft über Vor- und Famili-

67 § 5 der 2. Bundesmeldedatenübermittlungsverordnung
68 Nr. 12 der Anlage 4 zu § 3 Nr. 1 DVO-Meldegesetz

ennamen, Doktorgrad und Anschrift bestimmter Einwohner übermitteln[69]. Fast alle Landesmeldegesetze enthalten vergleichbare Regelungen. In den Ländern Berlin, Brandenburg und Sachsen dürfen jedoch bei einfachen Melderegisterauskünften nur die „gegenwärtigen Anschriften" mitgeteilt werden.

Im Ergebnis verkennen wir nicht das Dilemma, in dem die Berliner Meldebehörde steckt. Melderegisterauskünfte werden regelmäßig erst dann eingeholt, wenn die Einwohnerin oder der Einwohner nicht mehr unter der letzten bekannten Berliner Wohnanschrift erreicht werden kann. Das dürfte häufig auf einen Wegzug zurückzuführen sein. Bei dem klaren Wortlaut des Berliner Meldegesetzes darf die Meldebehörde im Rahmen einfacher Melderegisterauskünfte nur die gegenwärtigen Anschriften mitteilen. Das kann sie allerdings nicht gewährleisten, weil ihr nicht bekannt ist, ob die oder der Meldepflichtige nach der erfolgten Rückmeldung nochmals umgezogen ist. Nach einem erneuten Wegzug ist die im Rahmen der Rückmeldung in Berlin bekannt gewordene Wohnanschrift eine frühere Anschrift. Darüber darf aber nur bei Vorliegen eines berechtigten Interesses Auskunft erteilt werden[70]. Seit Juli warten wir auf eine sachgerechte Stellungnahme der Senatsverwaltung für Inneres, die sich mit der Berliner Rechtslage auseinandersetzt und eine akzeptable Lösung aufzeigt.

Vom Melderechtsrahmengesetz und anderen Landesmeldegesetzen abweichende Regelungen in Berlin erfordern von der Berliner Meldebehörde ein vom Verwaltungshandeln anderer Landesmeldebehörden abweichendes Verfahren.

69 § 21 Abs. 1 MRRG
70 § 28 Abs. 2 MeldeG

## 4.5 Scheinanmeldungen verhindern durch Vorlage des Mietvertrages?



Zehn Berliner Bezirke haben angekündigt, in ihrer Funktion als Meldebehörde bei An- und Ummeldungen von den Meldepflichtigen die Vorlage des Mietvertrages zu verlangen. Damit soll dem Problem der hohen Zahl von Scheinanmeldungen in Berlin begegnet werden. Zwei Bezirke haben sich dem aus rechtlichen Gründen nicht angeschlossen.

Eine Verpflichtung der Meldepflichtigen zur Vorlage kompletter Mietverträge ist dem Meldegesetz nicht zu entnehmen. Auch eine pauschale Verpflichtung zur Vorlage auszugsweiser Mietverträge ist mit dem Grundsatz der Erforderlichkeit[71] nicht vereinbar. Ferner bestehen erhebliche Zweifel an der Geeignetheit, mit der generellen Vorlagepflicht Scheinanmeldungen zu verhindern. Das ist schon mit der früher bestehenden Nebenmeldepflicht der Vermieter nicht gelungen, die bei der Novellierung des Meldegesetzes u. a. mit der Begründung abgeschafft wurde, so bürokratische Hemmnisse abzubauen.

Das Problem der Scheinanmeldung und mögliche Strategien zu ihrer Bekämpfung waren in den letzten Jahren wiederholt Gegenstand von Erörterungen auf Bund-Länder-Ebene. Der Bund und die überwiegende Zahl der Bundesländer haben sich dabei dezidiert gegen eine Wiedereinführung der Vermieternebenmeldepflicht ausgesprochen. Belastbares Zahlenmaterial, das eine deutliche Zunahme von Scheinanmeldungen belegt, liegt nicht vor. Es scheint sich im Übrigen offensichtlich um eine Berliner Besonderheit zu handeln[72]. Unbenommen bleibt es der Meldebehörde, in begründeten Einzelfällen – immer dann, wenn sie begründete Zweifel an der Richtigkeit der Angaben hat – eine Überprüfung vorzunehmen. Geeignete Mittel dazu sind die Überprüfungen vor Ort. Denkbar ist aber auch die Vorlage einer Bescheinigung des Vermieters über den tatsächlichen Einzug in die Wohnung[73]. Die Pflicht zur Vorlage eines Mietvertrages kann auf diese Vorschrift allerdings nicht gestützt werden. Ein Mietvertrag enthält etliche Daten, deren Kenntnisnahme durch die

71 § 9 BlnDSG

72 Antwort des Staatssekretärs Hahlen auf eine Anfrage des Abgeordneten Carsten Müller, BT-Drs. 16/7572

73 § 14 MeldeG

Meldebehörde für die Anmeldung nicht erforderlich ist. Die Vorlage eines Mietvertrages ist allenfalls dann akzeptabel, wenn das die oder der Meldepflichtige freiwillig statt der Vorlage einer schriftlichen Bestätigung der Vermieterin oder des Vermieters über den Wohnungsbezug anbietet.

Im Übrigen bestehen erhebliche Zweifel, ob eine generelle Vorlagepflicht von Mietverträgen ein geeignetes Mittel zur Verhinderung von Scheinanmeldungen wäre. Auch Mietverträge können in der Praxis mit Leichtigkeit fingiert werden, ohne dass die Meldebehörde über entsprechende Mittel verfügt, dies im Einzelfall überprüfen und feststellen zu können. Der Abschluss eines Mietvertrages beweist lediglich das Vorliegen eines mietrechtlichen Schuldverhältnisses zwischen Vermieter und Mieter. Das mag zwar ein Indiz dafür sein, dass der Mieter die Mieträume auch bezogen hat, ist jedoch nicht zwingend. Der melderechtlich relevante Vorgang ist das tatsächliche Beziehen der Wohnung, der die Meldepflicht auslöst, und nicht der Abschluss eines Mietvertrages.

**Auch mit Einwilligung der Betroffenen dürfen nur die für die ordnungsgemäße Aufgabenerfüllung erforderlichen Daten erhoben werden.**

## 4.6 Wahlvorschläge im Internet

Aus der Praxis

Ein Mitglied des Abgeordnetenhauses hat bei der Suche nach der Quelle für die an die Privatanschrift geschickte Werbepost festgestellt, dass der Landeswahlleiter auf seiner Internetseite neben den Namen und Vornamen auch die Privatanschriften der Kandidatinnen und Kandidaten veröffentlicht.

Das Landeswahlgesetz[74] schreibt vor, dass jeder Wahlvorschlag nur eine Person benennen darf und ihren Familiennamen, Vornamen, Geburtstag und -ort, Beruf und Anschrift angeben muss. Die Landeswahlleiterin oder der Landeswahlleiter hat nach der Landeswahlordnung[75] spätestens drei Wochen vor dem Wahltag die zugelassenen Wahlvorschläge in der vom Landeswahlausschuss fest-

74 § 10 Abs. 4
75 § 40

gelegten Reihenfolge mit der Angabe von Doktorgrad, Familiennamen, Vornamen, Geburtsjahr und -ort, Beruf sowie Anschrift für jede Bewerberin und jeden Bewerber im Amtsblatt für Berlin bekanntzumachen.

Sowohl der Gesetz- als auch der Verordnungsgeber haben das Verfahren und den Umfang der zu veröffentlichen Daten präzise geregelt. Zwar weicht der Landeswahlleiter mit der Veröffentlichung im Internet von dem vorgeschriebenen Medium ab; das halten wir aus zwei Gründen aber noch für vertretbar: Zum einen hat der Landeswahlleiter technisch sichergestellt, dass bei einer schlichten Namenssuche im Internet die Veröffentlichung auf seiner Seite nicht angezeigt wird. Zum anderen stellt der Kulturbuchverlag seinerseits das Amtsblatt für Berlin in das Internet ein. Bei einer Namenssuche wird auch diese Veröffentlichung nicht angezeigt.

Mit der Veröffentlichung wird dem Transparenzgebot Rechnung getragen. Die Wahlberechtigten sollen sich über die Kandidatinnen und Kandidaten informieren können. Dazu gehört auch, ob sie aus einem anderen Bezirk oder aus der näheren Umgebung kommen und man daher erwarten kann, dass sie sich mit den Besonderheiten des Wahlkreises auskennen. Für diesen Zweck würde zwar bereits die Postleitzahl ausreichen, also die vollständige Anschrift nicht erforderlich sein. Voraussetzung für eine Reduzierung des Kataloges der Daten, die der Landeswahlleiter zu veröffentlichen hat, ist allerdings eine Änderung der Landeswahlordnung.

Die Senatsverwaltung für Inneres und Sport sieht keinen Anlass für eine solche Änderung. Unsere Anregung, statt der Anschrift nur die Postleitzahl zu veröffentlichen, trage dem wahlrechtlichen Sinn und Zweck der Regelung über die Veröffentlichung der Anschrift nicht ausreichend Rechnung. Die Veröffentlichung der Anschrift soll den Wahlberechtigten die Möglichkeit eröffnen, sich vor der Wahl postalisch oder auf anderem Wege an die Bewerberinnen und Bewerber wenden zu können, um sie zu ihrer Bewerbung befragen zu können. Die Bewerberinnen und Bewerber können nur in Ausnahmefällen die Veröffentlichung durch eine Auskunftssperre im Melderegister verhindern. Soweit im Melderegister eine Auskunftssperre besteht, wird anstelle der Anschrift eine Erreichbarkeitsanschrift verwendet. Die Angabe eines Postfaches genügt nicht.

Kandidatinnen und Kandidaten für das Abgeordnetenhaus müssen grundsätzlich eine Veröffentlichung ihrer Privatanschrift im Internet hinnehmen. Dies können sie nur vermeiden, wenn sie zuvor nach den allgemein geltenden melderechtlichen Vorschriften eine Auskunftssperre im Melderegister haben eintragen lassen.

## 4.7 Praktische Erfahrungen mit dem neuen Personenstandsrecht

Aus der Praxis

Kurz vor Inkrafttreten des neuen Personenstandsgesetzes (PStG)[76] hat sich ein Petent darüber beschwert, dass er vom Standesamt keine Personenstandsurkunden bzw. Auskunft aus den Personenstandsbüchern über einen entfernten Verwandten erhalten hat. Das Bezirksamt Steglitz-Zehlendorf hatte den Antrag im Dezember 2008 nach der geltenden Rechtslage richtigerweise abgelehnt. Der Bescheid enthielt allerdings keinen Hinweis auf die ab 1. Januar 2009 geltende neue Rechtslage.

Das Bezirksamt erklärt den unterlassenen Hinweis auf die zum Jahresbeginn mögliche Nutzung des Archivgutes damit, dass noch keine konkreten Aussagen zur Nutzung des Archivs im Standesamt hätten gemacht werden können und damit nur weitere Fragen entstanden wären. Das Bezirksamt hat ferner mitgeteilt, dass die Standesämter seit dem 1. Januar 2009 „sonstige öffentliche Archive“[77] sind. Das hat zur Folge, dass gegenwärtig zwölf verschiedene Archivbehörden auf Standesamtsebene die zum Archivgut gewordenen früheren Personenstandseinträge zu verwalten haben. Eine Ausführungsverordnung zum PStG wurde von der Senatsverwaltung für Inneres und Sport bereits im Dezember 2008 angekündigt. Ferner hat das Bezirksamt unter Hinweis auf einen umfangreichen Katalog von ungeklärten Verfahrensfragen erklärt, dass die Urkundenstellen der Standesämter im Interesse einer einheitlichen Verfahrensweise und Vermeidung von Ungleichbehandlungen der Nutzenden einen

76 JB 2008, 4.3

77 § 7 Abs. 3 PStG i.V. m. § 10 Archivgesetz Berlin

Konsens dahingehend erzielt haben, dass vor Klärung der wichtigsten dieser noch offenen Fragen keine Archivnutzungen erfolgen sollten.

Weiterhin hat das Bezirksamt mitgeteilt, dass die umfangreichen Änderungen im gesamten Personenstandsrecht in Verbindung mit lang anhaltenden Personalminderausstattungen dazu führen, dass – zur Aufrechterhaltung eines ordnungsgemäßen Beurkundungswesens – Prioritäten bei der Umsetzung der reformierten personenstandsrechtlichen Regelungen zu setzen sind. Der Bearbeitung von Archivnutzungsanträgen könne kein besonderer Vorrang eingeräumt werden.

Das alles ist nur schwer zu verstehen. Das Gesetz der Neuregelung des Personenstandsrechts ist im Bundesgesetzblatt im Februar 2007 veröffentlicht worden. Bis zum Inkrafttreten am 1. Januar 2009 hatten die Standesämter fast zwei Jahre Zeit, diese Fragen zu klären. Diese Versäumnisse führen dazu, dass die Antragstellenden verzögert beschieden wurden.

Die um Stellungnahme gebetene Senatsverwaltung für Inneres und Sport hat nach Ablauf von dreieinhalb Monaten mitgeteilt, dass sämtliche Standesämter Auskunft aus dem bei ihnen vorhandenen Archivgut erteilen werden, nachdem sie sich auf eine einheitliche Verfahrensweise geeinigt haben. Im Übrigen wurde angekündigt, uns hinsichtlich der Ausführungsverordnung zum PStG zu beteiligen. Das ist bisher nicht geschehen. Wenigstens dem Petenten ist die gewünschte Auskunft erteilt worden – allerdings erst nach erneutem Antrag.

**Die Verwaltung ist gehalten, offene Verfahrensfragen vor Inkrafttreten neuer gesetzlicher Bestimmungen zu klären und Antragstellende auch auf Rechtsänderungen zu ihren Gunsten hinzuweisen.**

## 4.8 Der EuGH zum Ausländerzentralregister

Aus der Praxis

Der Europäische Gerichtshof (EuGH) hat festgestellt, dass die Speicherung und Verarbeitung personenbezogener Daten von Unionsbürgern zu statistischen Zwecken nicht dem Erforderlichkeitsgebot im Sinne der Europäischen Richtlinie zum Schutz personenbezogener Daten entspricht und die Nutzung der im Ausländerzentralregister enthaltenen Daten zur Bekämpfung der Kriminalität gegen das gemeinschaftsrechtliche Diskriminierungsverbot verstößt, weil die Verfolgung von Verbrechen und Vergehen unabhängig von der Nationalität notwendig sei, das Ausländerzentralregister aber keine Daten Deutscher enthalte[78].

Die grundsätzlich zulässige Speicherung von Daten ausländischer Unionsbürgerinnen und -bürger unterliegt einer doppelten Einschränkung. Zum einen darf das Register nur die für die Anwendung der ausländerrechtlichen Vorschriften erforderlichen Daten enthalten. Zum anderen muss sein zentralisierter Charakter eine effizientere Anwendung der Vorschriften erlauben.

Von dem Kläger, einem österreichischen Staatsbürger, der sich 1996 in Deutschland niedergelassen hat, sind personenbezogene Daten nur im zulässigen Umfang gespeichert. Der zentralisierte Charakter des Ausländerzentralregisters ermöglicht die effizientere Anwendung aufenthaltsrechtlicher Vorschriften als der (alternative) Rückgriff auf die dezentralisierten Melderegister der Länder. Ferner hat der Kläger aufgrund der Einschränkung zulässiger Nutzungszwecke keinen Anspruch auf eine Löschung der Daten. Die Datenspeicherung dient dem Anliegen, die mit der Anwendung ausländerrechtlicher Vorschriften betrauten Behörden zu unterstützen. Die Unterbindung einer Datennutzung durch sonstige Behörden zu anderen als ausländerrechtlichen Zwecken ist nicht durch eine Löschung, sondern durch ein Verbot der zweckfremden Weiterverarbeitung zu erreichen. Das ist durch eine Dienstanweisung des Bundesministeriums des Innern (BMI) sichergestellt. Danach dürfen die Daten des Klägers zu statistischen Zwecken nur anonymisiert verarbeitet werden, und ein Zugriff auf sie zum Zwecke der Kriminalitätsbekämpfung unterbleibt. Die Maßgaben der EuGH-Entscheidung bei der Behandlung der gespeicherten Daten von

78 EuGH vom 16. Dezember 2008 – C-524/06, H. gegen Deutschland

Unionsbürgerinnen und -bürgern sollen im Rahmen des Einzelabrufs berücksichtigt werden. Ferner plant das BMI zur Umsetzung eine Änderung des Ausländerzentralregistergesetzes. Das Ergebnis bleibt abzuwarten.

Diese Vorgaben sind allerdings für den Bereich des automatisierten Auskunftsverfahrens aus dem Register[79] nicht zuletzt wegen der Kosten und der noch nicht vollzogenen Gesetzesänderung bisher noch nicht umgesetzt. Das hält der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ebenso wie wir für nicht akzeptabel.

Grundsätzlich dürfen die Daten von Unionsbürgerinnen und -bürgern in einem zentralen Register gespeichert werden. Der Umfang der zu speichernden Daten und die Zwecke, für die diese Daten verwendet werden dürfen, sind jedoch eingeschränkt. Dies muss bereits jetzt auch im automatisierten Auskunftsverfahren berücksichtigt werden.

## 4.9 Datenaustausch zwischen Ausländerbehörde und Krankenkasse

Ein mit einer Ausländerin verheirateter Deutscher hat sich darüber beschwert, dass die Ausländerbehörde und seine Krankenkasse, die AOK Berlin, untereinander seine Einkommensdaten ausgetauscht haben.

Die Ehefrau des Petenten hat ein Kind aus einer vorherigen Ehe. Zur Beschleunigung der Einreise im Wege des Familiennachzuges zu ihrem deutschen Mann wurde das Einreiseverfahren des Kindes von dem der schwangeren Mutter abgetrennt. Die Ausländerbehörde stimmte daher zunächst nur der Einreise der Ehefrau zu. Bei der Prüfung des Einreiseantrages für das Kind sollte der Petent belegen, dass er in der Lage ist, den Lebensunterhalt der gesamten Familie zu sichern.

Die vorgelegte Bestätigung der AOK war hinsichtlich des zugrunde gelegten Einkommens mit den Angaben des Petenten gegenüber der Ausländerbehörde

79 § 22 AZRG

nicht vereinbar. Das wurde zum Anlass genommen, bei der AOK um Auskunft darüber zu bitten, ob bekannt ist, über welches Einkommen er tatsächlich verfügt, und ob somit die Berechnung der Krankenkassenbeiträge ordnungsgemäß erfolgt ist. Ferner wollte die Ausländerbehörde wissen, welches Einkommen genau als Berechnungsgrundlage gedient hat und ob der vereinbarte Krankenversicherungsschutz dem der gesetzlichen Krankenkasse entspricht. Die AOK hat die gewünschten Auskünfte auch erteilt.

Diese wechselseitigen Datenübermittlungen waren unzulässig. Die Ausländerbehörde hat eingeräumt, dass sie hier unzutreffend davon ausgegangen ist, sie die personenbezogenen Daten im Rahmen des § 90 Aufenthaltsgesetz an die AOK übermitteln dürfe und diese um Auskunft im Rahmen der besonderen Pflichten- und Mitteilungsbefugnisse der Sozialleistungsträger nach § 71 SGB X ersuchen. Die Mitarbeiterin hat übersehen, dass hier allein Daten eines deutschen Staatsangehörigen in Rede standen. Alle Beschäftigten im Einreisesachgebiet sind in einer Dienstbesprechung nochmals ausführlich über die Sach- und Rechtslage informiert worden. Dieses Vorgehen haben wir auch der AOK dringend angeraten.

**Die Ausländerbehörde kann Datenübermittlungen über deutsche Familienangehörige nicht auf § 90 Aufenthaltsgesetz stützen.**

# 5. Justiz

## 5.1 Den Datensündern auf der Spur – Entwicklung der Bußgeldpraxis



Viele Bürgerinnen und Bürger haben sich bei uns darüber beschwert, dass sie unaufgefordert Werbeschreiben erhalten. Wir wurden gebeten, die Nutzung der Daten durch die Unternehmen zu diesem Zweck zu überprüfen.

Bei der Prüfung der Eingaben haben wir festgestellt, dass viele Unternehmen in den Werbematerialien nicht darauf hinweisen, dass der Nutzung oder Verarbeitung der personenbezogenen Daten zu Werbezwecken widersprochen werden kann. Diese unterlassene Belehrung über das Widerspruchsrecht kann mit einem Bußgeld bis zu 50.000 € geahndet werden (§ 43 Abs. 1 Nr. 3 BDSG). Es handelt sich daher nicht um eine Bagatelle, denn nur informierte Bürgerinnen und Bürger können eine weitere Nutzung und Verwendung ihrer Daten verhindern. Die von uns dazu eingeleiteten Bußgeldverfahren zeigten meist schon nach der Anhörung der Verantwortlichen Wirkung. Sie räumten ein, die Belehrungspflicht über das Widerspruchsrecht nach dem BDSG nicht zu kennen, sicherten aber zu, die gesetzlichen Vorschriften zukünftig zu beachten.

Zum Jahresbeginn haben wir unsere bußgeldrechtliche Ahndungspraxis grundsätzlich umgestellt. Aufgrund der zunehmenden Anzahl bekannt gewordener massiver Datenschutzverstöße haben wir die in den letzten Jahren eher restriktive Handhabung von Bußgeldverfahren als letztes Mittel aufgegeben. Vielmehr haben wir in zahlreichen Fällen Bußgeldverfahren eingeleitet, in denen es um mehr ging als um den unterlassenen Hinweis auf das Recht, der Werbung zu widersprechen[80]. Die Einleitung von Bußgeldverfahren steht im pflichtgemäßen Ermessen der Verwaltungsbehörde, denn im Ordnungswidrigkeitenrecht[81] gilt – anders als im Strafprozessrecht – das Opportunitätsprinzip. Kriterien für die Einleitung eines Bußgeldverfahrens sind u. a.die Anzahl der Geschädig-

80 Zum Bußgeldverfahren gegen die Deutsche Bahn AG vgl. 10.1

81 § 47 Abs. 1 OWiG

ten, die Folgen einer unrechtmäßigen Datenerhebung und -verarbeitung oder generalpräventive Gründe. Insbesondere kann es nicht länger hingenommen werden, dass verantwortliche Stellen Datenschutzverstöße als Teil des unternehmerischen Risikos einkalkulieren oder zwingend in Kauf nehmen.

Nach den Datenskandalen bei Unternehmen hat auch der Gesetzgeber reagiert und mit den im Sommer erfolgten Novellierungen des Bundesdatenschutzgesetzes (BDSG)[82] nicht nur den Bußgeldrahmen für datenschutzrechtliche Verstöße im BDSG weiter angehoben, sondern auch zwölf neue Bußgeldtatbestände geschaffen. Zudem sind die Unternehmen jetzt verpflichtet, schon bei Vertragsabschluss auf das Recht zum Widerspruch gegen Werbung hinzuweisen. Die Anzahl der Bußgeldverfahren wird daher voraussichtlich weiter zunehmen, zumal zukünftig die nicht ordnungsgemäße Erfüllung des Auskunftsanspruchs von Bürgerinnen und Bürgern nach § 34 BDSG mit einem Bußgeld sanktioniert werden kann. Die durch die Novellierung erfolgte sanktionsrechtliche Verschärfung spiegelt insgesamt die wachsende wirtschaftliche Bedeutung beim Umgang mit personenbezogenen Daten und das damit einhergehende gesteigerte Missbrauchspotenzial wider.

In den parlamentarischen Beratungen zu den BDSG-Novellierungen haben die Abgeordneten die bisherige Bußgeldfestsetzung durch die Aufsichtsbehörden und Gerichte kritisiert. Diese Kritik haben wir aufgegriffen und uns mit einem Schreiben an die Senatorin für Justiz sowie den Präsidenten des Amtsgerichts Tiergarten gewandt. Wir haben angeregt, für eine verstärkte Fortbildung der Richterinnen und Richter zu sorgen und eine besondere Zuständigkeit bei den Amtsgerichten im Bereich datenschutzrechtlicher Ordnungswidrigkeiten einzurichten, um der Kritik des Gesetzgebers gerecht zu werden und Datenschutzverstöße als besondere Form der Wirtschaftskriminalität besser zu sanktionieren.

**Das Bußgeldverfahren ist ein Instrument zum Schutz der informationellen Selbstbestimmung. Wir werden dieses Instrument zukünftig stärker nutzen.**

82 Vgl. 2.1

## 5.2 Umgang mit Gefangenendaten in der Justizpressestelle



Vor fünf Jahren wurde der damals 19-jährige S. zu einer neunjährigen Haftstrafe wegen dreifachen Totschlags verurteilt. Nachdem er einen Teil seiner Strafe zunächst in einer Jugendstrafanstalt verbüßt hatte, wurde er im Jahr 2008 in die Justizvollzugsanstalt (JVA) Tegel verlegt. Als Grund für die Verlegung gab die Regionalpresse unter Berufung auf die Pressestelle der Senatsverwaltung für Justiz an, dass sich S. den Angeboten in der Jugendstrafanstalt komplett verweigern würde und er nunmehr in der sozialtherapeutischen Teilanstalt der JVA Tegel therapiert werden solle, sofern dies möglich sei. Nach derzeitiger Prognose sei jedoch eine nachträgliche Sicherheitsverwahrung wahrscheinlich. Diese Presseberichte lasen auch die Eltern von S., die uns um Prüfung baten, ob die Justizpressestelle unrechtmäßig Informationen über ihren Sohn an die Medien weitergegeben hat.

Die Senatsverwaltung für Justiz teilte uns mit, dass die Justizpressestelle einer Journalistin auf Anfrage telefonisch die Haftfortdauer und -verlegung von S. bestätigt habe. Als Gründe für die Haftverlegung seien auf Nachfrage der Journalistin die besseren Therapiemöglichkeiten für S. angegeben worden. Weitere Angaben zu einer etwaigen Verweigerungshaltung von S., zu einer Sozialprognose oder zu einer möglichen Haftentlassung seien nicht gemacht worden. Die Sicherungsverwahrung bei Jugendlichen sei lediglich allgemein und losgelöst vom konkreten Einzelfall dargestellt worden.

Die Auskunft der Justizpressestelle zur Haftfortdauer ist mit Blick auf § 180 Abs. 5 Nr. 2 Strafvollzugsgesetz datenschutzrechtlich nicht zu beanstanden. Jedoch war die Senatsverwaltung für Justiz nicht berechtigt, weitere Auskünfte zur Verlegung von S. aus der Jugendstrafanstalt in die JVA Tegel unter Angabe der Gründe für diese Verlegung (Unterbringung in einer sozialtherapeutischen Anstalt mit besseren Therapiemöglichkeiten) zu geben. Deshalb haben wir einen datenschutzrechtlichen Mangel nach § 26 Abs. 2 BlnDSG festgestellt.

Ungeklärt blieb, wie es zu den Angaben zu einer möglichen Sicherungsverwahrung unter Berufung auf die Pressestelle der Senatsverwaltung für Justiz

kam. Zur Nachweisbarkeit gesetzeskonformer Auskunftserteilung auf Presseanfragen, die zu bestimmten Personen erfolgen und deren Beantwortung für diese Personen erhebliche nachteilige Wirkungen haben können, haben wir der Senatsverwaltung für Justiz empfohlen, künftig im Anschluss Gesprächsvermerke anzufertigen, aus denen sich der Umfang der erteilten Auskünfte ergibt. Die Senatsverwaltung für Justiz bewertete das Vorgehen ihrer Mitarbeiterin als datenschutzrechtlich zulässig und sah sich aufgrund der erheblichen Arbeitsbelastung der Pressestelle sowie der besonderen Eilbedürftigkeit bei der Beantwortung von Presseanfragen nicht in der Lage, unserer Dokumentationsempfehlung zu folgen.

Es ist erforderlich und zumutbar, zumindest risikoträchtige Auskünfte in der Pressestelle der Senatsverwaltung für Justiz zu dokumentieren, um sie justiziabel zu machen und so die Umsetzung datenschutzrechtlicher Vorschriften im Bereich des Strafvollzugs zu gewährleisten.

## 5.3 Psychologische Gutachten in der Gefangenenpersonalakte

Aus der Praxis

Im Rahmen der Prüfung der Eingabe eines Gefangenen fiel uns bei Durchsicht seiner Gefangenenpersonalakte in der JVA Tegel auf, dass darin für jeden Nutzenden frei zugänglich Stellungnahmen des Psychologischen Dienstes abgelegt worden waren. Bei den Stellungnahmen handelt es sich um fachdienstliche Gutachten, die der Prüfung der Eignung des Gefangenen für den offenen Vollzug dienen.

Wir teilten der JVA Tegel mit, dass wir den unbeschränkten Zugang zu Detailinformationen über die psychische Verfassung von Gefangenen für datenschutzrechtlich bedenklich halten, und schlugen vor, psychologische Begutachtungen von Gefangenen zu Prognosezwecken in einem geschlossenen Umschlag als Anhang zur Gefangenenpersonalakte aufzubewahren. In diesem Zusammenhang verwiesen wir auf ein Urteil des Bundesarbeitsgerichts[83], wonach der Arbeitgeber aus Rücksicht auf das allgemeine Persönlichkeitsrecht

83 vom 12. September 2006 – 9 AZR 271/06

des Arbeitnehmers verpflichtet ist, dessen Gesundheitsdaten vor unbefugter zufälliger Kenntnisnahme durch Einschränkung des Kreises der Informationsberechtigten zu schützen. Nach unserer Ansicht ist der Grundgedanke der Entscheidung, einen geeigneten Schutz für sensible Daten zu schaffen, auf den vorliegenden Sachverhalt übertragbar.

Die Senatsverwaltung für Justiz wies demgegenüber darauf hin, dass die Gutachten des Psychologischen Dienstes nach Prüfung der Eignung für den offenen Vollzug Bestandteil der Vollzugsplanung der Inhaftierten und somit Basis jeder Betreuung seien. Sie seien daher jedem an der Behandlung beteiligten Bediensteten zugänglich zu machen. Zudem unterlägen die Beschäftigten des Psychologischen Dienstes nach §§ 203 Strafgesetzbuch, 182 Abs. 2 StVollzG der Schweigepflicht nur in ihrer Funktion als Therapeuten, nicht jedoch in ihrer Funktion als prognostizierende Gutachter. Der Zugriff von unbefugten Dritten auf die psychologische Begutachtung sei in der Praxis auch ausgeschlossen, da die jeweilige Gefangenenpersonalakte nur für die an der Behandlung konkret beteiligten Bediensteten zugänglich sei.

Wir halten diese Rechtsansicht für vertretbar und haben daher keinen Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt. Problematisch ist jedoch, dass § 183 Abs. 2 Satz 2 StVollzG ausdrücklich nur die getrennte Führung von Gesundheitsakten und Krankenblättern regelt. Für sonstige Unterlagen, die Gesundheitsdaten enthalten, hat der Gesetzgeber keine Regelung getroffen, sodass in Bezug auf die vergleichbare Sensitivität der Daten eine entsprechende Anwendung auf fachdienstliche Stellungnahmen des Psychologischen Dienstes zu befürchten ist. Zumindest sollte aus Gründen der Überprüfbarkeit schriftlich festgelegt werden, welche Bediensteten konkret an der Behandlung beteiligt sind und somit Zugang zu fachpsychologischen Gutachten in einer Gefangenenpersonalakte haben.

**Wir halten die Praxis der Ausgestaltung der Gefangenenpersonalakte im Hinblick auf fachpsychologische Gutachten angesichts der momentanen Gesetzeslage weiterhin für datenschutzrechtlich sehr problematisch und haben deshalb für das derzeit in der Planung befindliche Berliner Justizvollzugsdatenschutzgesetz eine entsprechende Änderung angeregt.**

# 6. Finanzen

## 6.1 Beitreibung von Zahlungsrückständen durch Inkassobüros?



Die Senatsverwaltung für Finanzen bat uns zu prüfen, ob es datenschutzrechtlich zulässig sei, dass Zahlungsrückstände im Zusammenhang mit Ansprüchen, die nach § 7 Unterhaltsvorschussgesetz (UhVorschG) auf das Land Berlin übergegangen sind, durch private Inkassounternehmen eingezogen werden können.

Ein Inkasso durch private Dritte würde voraussetzen, dass das Land Berlin dem Inkassounternehmen die Daten, die den Anspruch begründen, zur Verfügung stellt. Handelt es sich bei der Schuldnerin oder dem Schuldner um eine natürliche Person, würden somit zwangsläufig deren personenbezogene Daten an einen privaten Dritten übermittelt. Für die Frage, ob diese Weitergabe von personenbezogenen Schuldnerdaten zulässig ist, kommt es entscheidend darauf an, ob die Daten im Auftrag des Landes Berlin verarbeitet[84] oder zur Erledigung eigener Aufgaben an das Inkassounternehmen übermittelt[85] werden.

Eine Datenverarbeitung im Auftrag setzt voraus, dass der Auftragnehmer die damit verbundenen Aufgaben im Rahmen einer engen, weisungsgebundenen Abhängigkeit vom Auftraggeber erledigt. Bei der Übertragung von Inkassoaufgaben an Dritte ist aber davon auszugehen, dass diese das Verfahren zur Beitreibung der Zahlungsrückstände umfassend erledigen sollen. Dazu sind dem Inkassounternehmen eigene Entscheidungsbefugnisse einzuräumen (z. B. bei der Überwachung des Zahlungsverkehrs, Bearbeitung von Widersprüchen und Stundungen, der Durchsetzung von Forderungen). Die Datenverarbeitung dient diesem Zweck und erfolgt damit unter eigener datenschutzrechtlicher Verantwortung des privaten Inkassounternehmens. Eine Datenverarbeitung im Auftrag des Landes Berlin ist deshalb bei der Übertragung von Inkassoaufgaben an private Dritte grundsätzlich ausgeschlossen.

84 § 3 Abs. 1 BlnDSG
85 § 4 Abs. 2 Nr. 4 BlnDSG

Sofern dem privaten Inkassounternehmen personenbezogene Daten von Schuldnern nach UhVorschG übermittelt werden sollen, handelt es sich um Sozialdaten[86]. Außerhalb einer Datenverarbeitung im Auftrag, die in diesem Bereich noch strengeren Regeln[87] unterliegt, ist eine derartige Datenübermittlung nach § 67 d SGB X nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im SGB vorliegt. Eine solche Rechtsgrundlage, auf die die Datenübermittlung durch die Finanzbehörden an private Dritte gestützt werden könnte, ist nicht vorhanden.

Hoheitlich handelnde Verwaltungen dürfen ihre Aufgaben nicht ohne gesetzliche Grundlage an private Dritte übertragen. Da es sich bei der Beitreibung von Zahlungsrückständen nach § 7 UhVorschG um eine hoheitliche Aufgabe handelt, scheidet ihre Übertragung an private Dritte aus. Ungeachtet dessen darf die Verwaltung keine Schuldnerdaten an private Inkassounternehmen übermitteln.

## 6.2 Das Finanzamt als verlängerter Arm der GEZ

Eine Petentin beschwerte sich darüber, dass die Gebühreneinzugszentrale (GEZ) dem Finanzamt Daten im Zusammenhang mit einer Gebührenforderung gegen sie übermittelt habe. Das Finanzamt habe diese Daten verwendet, um im Auftrag der GEZ eine Kontopfändung bei ihr durchzuführen.

Nach dem Rundfunkgebührenstaatsvertrag hat grundsätzlich jede oder jeder Rundfunkteilnehmende für jedes zum Empfang bereitgehaltene Rundfunkempfangsgerät eine Grundgebühr und für das Bereithalten jedes Fernsehgerätes jeweils zusätzlich eine Fernsehgebühr zu entrichten. Diese Gebühren werden von der GEZ im Auftrag der Landesrundfunkanstalten eingezogen. Werden die Gebühren nicht entrichtet, ergeht ein Bescheid über rückständige Rundfunk-

86 Das Unterhaltsvorschussgesetz ist nach § 68 Nr. 14 SGB I ein besonderer Teil des Sozialgesetzbuchs.

87 § 80 SGB X

gebühren, der im Verwaltungszwangsverfahren vollstreckt wird[88]. Für das Vollstreckungsverfahren in Berlin gilt das Verwaltungsvollstreckungsgesetz des Bundes[89]. Danach erfolgt die Vollstreckung von Geldforderungen grundsätzlich durch die Vollstreckungsbehörden der Finanzverwaltung[90], das Verfahren und der Vollstreckungsschutz richten sich nach den Vorschriften der Abgabenordnung[91]. Dort ist in § 249 Abs. 1 geregelt, dass die Vollstreckung der Geldforderung durch die Finanzbehörden selbst erfolgt. Die Übermittlung der Daten von der GEZ an das Finanzamt war für die Vollstreckung des Gebührenbescheides erforderlich und damit zulässig.

**Die Übermittlung von personenbezogenen Daten durch die GEZ an das Finanzamt zur Vollstreckung rückständiger Rundfunkgebühren ist grundsätzlich rechtmäßig.**

88 Art. 4 § 7 Abs. 5 Nr. 1 des Rundfunkgebührenstaatsvertrages
89 § 5 Abs. 2 VwVG Bln
90 § 4 Abs. 1 b VwVG
91 § 5 Abs. 1 VwVG

# 7. Sozialordnung

## 7.1 Sozial- und Jugendverwaltung

### 7.1.1 Neues von den Jobcentern

Zur Intensivierung der Zusammenarbeit und um ein einheitliches Datenschutzniveau in allen Berliner Jobcentern zu erreichen, haben wir eine Gesprächsrunde mit den Ansprechpartnerinnen und -partnern für Datenschutz der Jobcenter ins Leben gerufen. Dieses Jahr hat das Treffen zweimal stattgefunden. Dabei wurden sowohl allgemeine datenschutzrechtliche Fragen als auch spezielle Einzelfragen besprochen.

**Hausbesuche durch Außendienst – was Leistungsempfangende wissen sollten**

Als Kernthema haben wir die zwar nicht neue, jedoch immer wieder aktuelle datenschutzrechtliche Problematik der Durchführung von Hausbesuchen durch die Außendienstteams der Jobcenter aufgegriffen. Wie wir bereits früher betont haben[92], wird durch einen Hausbesuch in erheblichem Maße in das Grundrecht auf Unverletzlichkeit der Wohnung eingegriffen. Solange es hinsichtlich der Zulässigkeit von Hausbesuchen keine eindeutige Rechtsprechung gibt und auch der Gesetzgeber das Problem durch die Aufnahme einer entsprechenden Regelung im SGB II nicht gelöst hat, bedarf es zumindest einer einheitlichen und datenschutzkonformen Praxis. Es muss klar festgelegt sein, unter welchen Voraussetzungen und Bedingungen Hausbesuche durch die Jobcenter angeordnet und durchgeführt werden können.

Um diesbezüglich eine größtmögliche Transparenz für die Betroffenen zu schaffen, haben wir zusammen mit den Jobcentern Hinweise entwickelt, die bereits bei der Antragstellung an die Leistungsempfängerinnen und -empfänger ausgegeben werden sollen. Über folgende Punkte werden sie zukünftig informiert:

92 JB 2005, 3.2; JB 2007, 7.2.1

Zur Bedarfsfeststellung oder zur Aufklärung von Leistungsfragen kann es in begründeten Einzelfällen zur Durchführung eines angekündigten Hausbesuches von Außendienstmitarbeiterinnen und -mitarbeitern des Jobcenters kommen. Bei begründetem Verdacht eines Leistungsmissbrauchs, der im Einzelfall zu dokumentieren ist, kann der Hausbesuch auch unangekündigt erfolgen. Dabei ist jedoch zu beachten, dass die Duldung eines Hausbesuchs freiwillig ist und nicht unter die Mitwirkungspflicht nach § 60 SGB I fällt. Die Betroffenen haben das Recht, den Zutritt zu ihrer Wohnung zu verweigern. Der jeweilige Grund des Hausbesuchs muss ihnen vorab mitgeteilt werden. Die Betroffenen haben die Möglichkeit, einen bestehenden Bedarf auch anderweitig nachzuweisen. Der Leistungsantrag darf grundsätzlich nicht allein aufgrund des verweigerten Hausbesuchs abgelehnt werden. Ist ein geltend gemachter Bedarf jedoch ausschließlich anhand eines Hausbesuchs feststellbar, kann die Weigerung im Einzelfall zur Ablehnung der beantragten Leistung führen.

Durch die Aufklärung der Leistungsempfangenden darüber, unter welchen Voraussetzungen und Bedingungen es im Einzelfall zur Durchführung eines Hausbesuchs kommen kann, wird das Handeln der Jobcenter transparenter, und es ist den Betroffenen möglich, sich hierauf einzustellen.

### Wann müssen Jobcenter der Polizei Auskunft geben?

Ein weiteres hervorzuhebendes Thema der gemeinsamen Gesprächsrunde mit den Jobcentern ist der Umgang mit Polizeianfragen. Auslöser war die Praxis der Polizei, von den Jobcentern Informationen zu bestimmten, ins Visier der Polizei geratenen Leistungsempfängerinnen und -empfängern abzufragen. Es bestand bei den Jobcentern eine große Ungewissheit, ob Daten überhaupt, und falls ja, in welchem Ausmaß an die Polizeibehörden übermittelt werden dürfen. Hierzu haben wir anhand der gesetzlichen Regelungen Leitlinien entwickelt, die wir in Form eines Informationsblattes den Jobcentern zur Verfügung gestellt haben.

Eine wesentliche Maßnahme zum Umgang mit Auskunftsersuchen der Polizei ist die Benennung einer oder eines Verantwortlichen. Sie oder er prüft die Anfragen der Polizeibehörden, soweit die Leitung des Jobcenters sich nicht die Beantwortung solcher Anfragen vorbehält. Andere Mitarbeiterinnen und Mitarbeiter sind gegenüber der Polizei weder zur Auskunft verpflichtet noch

berechtigt. Die Auskunftsersuchen sollen an die oder den Verantwortlichen weitergeleitet werden. Insbesondere ist bei der Übermittlung von Sozialdaten an Polizeibehörden in jedem Einzelfall zu prüfen, inwieweit eine gesetzliche Erlaubnisnorm zur Datenübermittlung besteht. Auskunftsersuchen sind nur in begründeten Einzelfällen unter der Benennung der jeweiligen Rechtsgrundlage zulässig. Um die Zulässigkeit des Auskunftsersuchens prüfen zu können, muss die Anfrage der Polizei im Regelfall schriftlich erfolgen. Die auskunftsersuchenden Beamten sind auf den Schriftweg zu verweisen.

Die Datenübermittlung kann durch die §§ 68, 73 und 69 Abs. 1 Nr. 2 SGB X gerechtfertigt sein. Im Rahmen des § 68 SGB X dürfen ausschließlich folgende Daten übermittelt werden: Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift der oder des Betroffenen, derzeitiger oder zukünftiger Aufenthalt (darunter fallen allerdings auch zukünftige Vorsprache-Termine beim Jobcenter) sowie Namen und Anschriften der derzeitigen Arbeitgeber. Weitere Sozialdaten dürfen gemäß § 73 SGB X ausschließlich aufgrund einer richterlichen Anordnung weitergegeben werden. Datenübermittlungen nach § 69 Abs. 1 Nr. 2 SGB X bilden die Ausnahme und sind daher besonders zu prüfen.

Die Beachtung der Hinweise zum Umgang mit Polizeianfragen bei den Jobcentern gewährleistet, dass die datenschutzrechtlichen Voraussetzungen eingehalten werden und der Sozialdatenschutz der Betroffenen gewahrt wird.

### Vermittlung trotz Schulbesuch?

Der Vater einer minderjährigen Tochter, die bis zum Erreichen des angestrebten Schulabschlusses noch mehrere Schuljahre vor sich hatte, wurde vom Jobcenter aufgefordert, einen siebenseitigen Vordruck („Arbeitspaket“) mit Fragen zu den beruflichen Kenntnissen und Fertigkeiten der Tochter auszufüllen und das aktuelle Schulzeugnis des Kindes beizufügen. Das Jobcenter begründete das damit, es wolle die Tochter anhand der Informationen bei der Ausbildungsplatz- oder Arbeitsstellensuche gezielt unterstützen.

Eine pauschale Anforderung des Arbeitspaketes sowie von Schulzeugnissen der erwerbsfähigen Schülerinnen und Schüler, die in einer Bedarfsgemeinschaft

leben, ist weder erforderlich noch gesetzlich begründet. Grundlage für die Verpflichtung der Hilfebedürftigen, Zeugnisse vorzulegen, kann nur eine zwischen dem Jobcenter und der oder dem Hilfebedürftigen abgeschlossene Eingliederungsvereinbarung sein.

Zum Zeitpunkt des laufenden Schulbesuches ist jedoch noch nicht absehbar, wann und ob diese Daten überhaupt erforderlich werden, wenn sich zum Beispiel unmittelbar nach der Schule eine Ausbildung oder ein Studium anschließt. Eine Erhebung dieser Datenmenge ist zu diesem Zeitpunkt nicht erforderlich. Zunächst muss geprüft werden, ob mit den jeweiligen Mitgliedern der Bedarfsgemeinschaft überhaupt eine Eingliederungsvereinbarung geschlossen werden soll oder ob darauf wegen des noch länger andauernden Schulbesuches verzichtet werden kann. Dafür reicht neben den Stammdaten und der Vorlage einer Schulbescheinigung die Angabe aus, ob die Schule auch in Zukunft noch länger besucht wird. Alle weiteren Angaben, insbesondere die Schulzeugnisse, sind zu diesem Zeitpunkt nicht erforderlich.

Die Anforderung von Schulzeugnissen im begründeten Einzelfall ist dagegen zulässig. Allerdings haben die Beschäftigten des Jobcenters gegenüber den Leistungsempfängerinnen und -empfängern die Anforderung der Zeugnisse im Einzelfall zu begründen.

Mittlerweile hat sich das Jobcenter unserer Rechtsauffassung angeschlossen. Zukünftig wird es nur in begründeten Einzelfällen die Schulzeugnisse bzw. relevanten Daten im Rahmen einer Eingliederungsvereinbarung anfordern, soweit es für die weitere Integrationsarbeit erforderlich ist. Von einer pauschalen Anforderung von Schulzeugnissen der erwerbsfähigen Schülerinnen und Schüler wird das Jobcenter absehen.

Soweit ein minderjähriges Mitglied einer Bedarfsgemeinschaft noch die Schule besucht, sind zunächst eine Erklärung, dass das Kind die Schule auch in der Zukunft noch weiter besuchen wird, sowie die Vorlage einer aktuellen Schulbescheinigung ausreichend. Lediglich in begründeten Einzelfällen kann auch die Anforderung von Schulzeugnissen erforderlich sein. Dies ist gegenüber den Betroffenen zu begründen und in einer Eingliederungsvereinbarung festzulegen.

## 7.1.2 Berliner Kinderschutzgesetz datenschutzrechtlich tragbar

Das Berliner Gesetz zum Schutz und Wohl des Kindes (Berliner Kinderschutzgesetz) ist am 10. Dezember 2009 vom Abgeordnetenhaus verabschiedet worden und am 31. Dezember 2009 in Kraft getreten[93]. Ziel ist, Kindern und Jugendlichen eine gesunde Entwicklung zu ermöglichen und sie vor Gefährdungen für ihr Wohl zu schützen. Dazu wird u. a. ein verbindliches Einladungswesen und Rückmeldeverfahren geschaffen, mit dem die Erhöhung der Teilnahmequoten an den vom Gemeinsamen Bundesausschuss in den „Kinder-Richtlinien“[94] vorgesehenen Früherkennungsuntersuchungen für Kinder angestrebt wird.

Wir haben im Gesetzgebungsverfahren auf die verfassungsrechtlichen Bedenken hingewiesen, die gegen das Verfahren bestehen[95]. Es ist zu bezweifeln, dass die Kontrolle der Teilnahme an den Früherkennungsuntersuchungen und die weitergehenden Mitteilungspflichten tatsächlich geeignet sind, Gefährdungen des Kindeswohls aufzudecken, und dass die vollständige Erfassung aller Berliner Kinder bei der an der Charité angesiedelten Zentralen Stelle ein angemessenes Mittel zur Erreichung des gesetzlichen Ziels ist. Da auf politischer Ebene Konsens darüber bestand, die Früherkennungsuntersuchungen in einem Berliner Gesetz verbindlicher auszugestalten, haben wir uns jedoch unabhängig von unseren grundsätzlichen Bedenken in konstruktiven Gesprächen mit der federführenden Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz, der Charité sowie einzelnen Abgeordneten an einer datenschutzgerechten Umsetzung des politischen Ziels beteiligt. Unsere Forderungen wurden dabei im Wesentlichen berücksichtigt. Begrüßenswert ist, dass die mit dem Einladungswesen und Rückmeldeverfahren verbundene Datenverarbeitung ausdrücklich im Gesetz geregelt ist und nicht der Regelung durch Rechtsverordnung überlassen wurde. In das Gesetz wurden zudem Vorschriften über Löschungsfristen aufgenommen. Unserer Forderung nach einer gesetzlichen Regelung der wesentlichen Datenverarbeitungsbefugnisse wurde damit entsprochen.

93 GVBl. 2009, S. 875

94 Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des 6. Lebensjahres

95 JB 2008, 8.1.1.

Ein wichtiger Kritikpunkt war für uns die im ursprünglichen Gesetzentwurf[96] vorgesehene Verknüpfung der Datenbestände der Charité aus dem **freiwilligen** Verfahren des Neugeborenen-Screenings mit denen des **verpflichtenden** Einladungswesens und Rückmeldeverfahrens durch die Zentrale Stelle. Es war vorgesehen, die für das Neugeborenen-Screening verwendete Screening-Identitätsnummer (Screening-ID), mit der der Personenbezug zu den Kindern wiederhergestellt werden kann, auch für das neue Einladungswesen und Rückmeldeverfahren zu verwenden. Ziel war es, das Verfahren durch einfachere Zuordnung effizienter auszugestalten und so die Rücklaufquoten zu erhöhen. Allerdings verzichtete der Gesetzentwurf auf eine Regelung zur notwendigen Abschottung der Datenbestände voneinander. Unsere Bedenken gegen die unzulässige Verknüpfung der beiden zu gänzlich unterschiedlichen Zwecken aufgebauten Datenbestände konnten durch die Einrichtung einer sog. Vertrauensstelle ausgeräumt werden. Die als räumlich, organisatorisch und personell getrennte Einheit bei der Zentralen Stelle angesiedelte Vertrauensstelle hat die Aufgabe, allein die Verwendung der im Neugeborenen- und Hörscreening vergebenen Screening-ID auch für das Einladungswesen und Rückmeldeverfahren zu ermöglichen. Im Übrigen erfolgt keine Verknüpfung der Datenbestände der beiden Verfahren.

Die Zentrale Stelle ermittelt durch einen Datenabgleich diejenigen Kinder, für die keine Untersuchungsbescheinigungen eingegangen sind. Das Gesundheitsamt soll daraufhin einen Hausbesuch durchführen. Zwar benannte der ursprüngliche Gesetzentwurf Fallgruppen, bei deren Vorliegen ein Hausbesuch nicht erfolgen sollte. Jedoch war hierfür Voraussetzung, dass die freiwillige Früherkennungsuntersuchung nachgeholt und ein entsprechender Nachweis gegenüber dem Gesundheitsamt erbracht wurde. Die Früherkennungsuntersuchungen wurden damit quasi verpflichtend gemacht, eine „echte" Abwendungsmöglichkeit bestand nicht. Da die Teilnahme an den Früherkennungsuntersuchungen nach der Konzeption des Gesetzes aus verfassungsrechtlichen Gründen aber nicht verpflichtend ist, stellte sich ein Hausbesuch in diesen Fällen als unverhältnismäßig dar. Eine tatsächliche Freiwilligkeit war weder hinsichtlich der Hausbesuche noch hinsichtlich der Früherkennungsuntersuchungen gewährleistet. Da das Gesundheitsamt vor dem Hintergrund des Grundrechts der Unverletzlichkeit der Wohnung kein Recht zum Betreten

96 Abghs.-Drs. 16/2154

einer Wohnung hat, sieht das Kinderschutzgesetz nunmehr entsprechend unserem Vorschlag vor, dass das Gesundheitsamt den Personensorgeberechtigten den Hausbesuch vorher schriftlich ankündigt und diese ausdrücklich auf die Freiwilligkeit des Hausbesuchs hinweist.

Das Gesetz enthält auch keine Verpflichtung mehr zur Nachholung der jeweiligen Früherkennungsuntersuchung. Den Personensorgeberechtigten wird die Entscheidung überlassen, die unter dem Gesichtspunkt der Früherkennung von Krankheiten bei Kindern unstreitig sehr wichtigen, aber dennoch weiterhin freiwilligen Früherkennungsuntersuchungen von einer Kinderärztin oder einem -arzt durchführen zu lassen. Im Ergebnis ist damit eine Wahrung der Grundrechte der Betroffenen gewährleistet. Lehnen Personensorgeberechtigte den Hausbesuch und die Nachholung der Früherkennungsuntersuchung weiterhin ab, ist dies vor dem Hintergrund der Freiwilligkeit hinzunehmen.

Auch unsere Empfehlung, eine Vorschrift über die Evaluation in das Gesetz aufzunehmen, wurde umgesetzt. § 7 Berliner Kinderschutzgesetz sieht vor, dass zwei Jahre nach Beginn der Arbeit der Zentralen Stelle durch einen Dritten eine Evaluation durchzuführen ist. Wir gehen davon aus, dass sich im Rahmen der Evaluation zeigen wird, ob das mit dem Einladungswesen verfolgte Ziel, Kindeswohlgefährdungen zu verhindern, tatsächlich erreicht wird. Sollte dies nicht der Fall sein, ist das gesamte Verfahren unter dem Gesichtspunkt der Verhältnismäßigkeit erneut zu beleuchten.

In Anlehnung an den in der vergangenen Legislaturperiode nicht mehr verabschiedeten Entwurf eines Gesetzes zur Verbesserung des Kinderschutzes[97] auf Bundesebene enthält das Berliner Kinderschutzgesetz in § 11 eine Regelung über die „Beratung und Weitergabe von Informationen bei Gefährdung des Wohls eines Kindes oder eines Jugendlichen". Wir haben uns für eine Streichung dieser Vorschrift ausgesprochen und auf die Vorteile einer einheitlichen bundesgesetzlichen Regelung hingewiesen. Zumindest konnten wir erreichen, dass das Gesetz für die zur Einschätzung der Gefährdung des Wohls eines Kindes vorgesehene – fachlich sehr sinnvolle – Heranziehung einer insoweit erfahrenen Fachkraft lediglich die Übermittlung anonymisierter oder pseud-

97 BR-Drs. 59/09

onymisierter Daten vorsieht, die datenschutzrechtlich unbedenklich ist. Wir haben uns dafür eingesetzt, auf eine Übermittlungsbefugnis gegenüber den Jugendämtern allein zum Zwecke der Gefährdungseinschätzung zu verzichten. Wir sahen die Gefahr einer unangemessenen Belastung der Jugendämter durch eine Vielzahl von weder erforderlichen noch für die Aufgabenerfüllung der Jugendämter hilfreichen Meldungen. Dabei gingen wir davon aus, dass mit der Möglichkeit der anonymen oder pseudonymen Beratung durch Fachkräfte ein Instrument geschaffen wird, um bereits im Vorfeld einer Meldung an die Jugendämter die Einschätzung einer Kindeswohlgefährdung zu ermöglichen, ohne dass in die Datenschutzrechte der Betroffenen eingegriffen wird. Führt die Beratung zu dem Ergebnis, dass eine Kindeswohlgefährdung anzunehmen ist, die nicht anders abgewendet werden kann, so ist eine Übermittlung der erforderlichen Informationen an die Jugendämter bereits nach der gegenwärtigen Rechtslage zulässig.

Mit dem Berliner Gesetz zum Schutz und Wohl des Kindes ist ein datenschutzrechtlich tragbarer Kompromiss gefunden worden. Insbesondere bei der Ausgestaltung des Einladungswesens und Rückmeldeverfahrens ist ein besonderes Augenmerk auf eine datenschutzgerechte praktische Umsetzung zu richten. Diese werden wir weiterhin kritisch, aber konstruktiv begleiten.

### 7.1.3 Akteneinsicht bei den Jugendämtern

Aus der Praxis

Immer wieder erreichen uns Anfragen, in denen sich Bürgerinnen und Bürger über die Ablehnung von Anträgen auf Akteneinsicht bei Jugendämtern beschweren. Zumeist handelt es sich um Fallkonstellationen, in denen sich Geschiedene um das Sorge- bzw. Umgangsrecht für gemeinsame Kinder streiten. Die Akten enthalten neben den Sozialdaten des Kindes Informationen sowohl über den einen als auch den anderen Elternteil. Begehrt ein Elternteil Einsicht in die Akten, stellt sich häufig das Problem, dass der andere Elternteil ein Interesse an der Geheimhaltung der ihn betreffenden Informationen hat. Lehnt ein Jugendamt ein Akteneinsichtsgesuch ab, führt dies häufig zu Unverständnis bei den Antragstellenden.

In erster Linie kommt im Bereich der Jugendhilfe der datenschutzrechtliche Auskunftsanspruch[98] zum Tragen. Er regelt einen Anspruch der oder des Betroffenen auf Auskunft u. a. über die zur eigenen Person gespeicherten Sozialdaten. Die Form der Erteilung der Auskunft wird vom Jugendamt nach pflichtgemäßem Ermessen bestimmt, d. h., das Jugendamt kann den Betroffenen statt der Auskunft eine Einsicht in Akten bzw. Aktenteile gewähren, muss dies aber nicht. Der Auskunftsanspruch gilt zudem nicht uneingeschränkt. So darf eine Auskunft nicht erteilt werden, wenn die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss[99]. Das Jugendamt hat insofern vor der Erteilung einer Akteneinsicht bzw. Auskunft zu prüfen, ob die Daten des anderen Elternteils oder weiterer Dritter der Auskunftserteilung entgegenstehen. In diese Abwägung der Interessen ist auch die Frage einzubeziehen, ob Teilauskünfte gewährt werden können. Schließlich kann auch eine differenzierte Aktenführung die teilweise Gewährung von Akteneinsicht erleichtern.

Sozialdaten, die dem Jugendamt im Vertrauen auf dessen besondere Verschwiegenheit anvertraut worden sind[100], unterliegen einem besonderen Schutz und dürfen in der Regel von vornherein nicht herausgegeben werden, sodass sich eine Auskunft auf diese nicht erstrecken kann. Auch wenn aus den genannten rechtlichen Gründen die vollständige Akteneinsicht bzw. Auskunft häufig nicht möglich ist, so kann in den meisten Fällen eine Teilauskunft bzw. -einsicht gewährt und damit den Interessen der Betroffenen zumindest teilweise Rechnung getragen werden.

Die Jugendämter sollten die Betroffenen ausführlicher über die Rechtslage und – soweit möglich – über die inhaltlichen Gründe einer Auskunftsverweigerung aufklären. Auf diese Weise lassen sich viele Streitigkeiten vermeiden.

98 § 61 Abs. 2 SGB VIII i. V. m. § 83 SGB X
99 § 61 Abs. 2 SGB VIII i. V. m. § 83 Abs. 4 Nr. 3 SGB X
100 Vgl. dazu § 65 SGB VIII

## 7.2 Gesundheit

### 7.2.1 Versorgungsforschung der Krankenkassen – noch eine zentrale Datenbank?

Bereits im Sommer 2008 trat das Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland mit der Bitte an uns heran, ein deutschlandweites Projekt der Kassenärztlichen Vereinigungen (KV) datenschutzrechtlich zu begleiten. Das Projekt beabsichtigt eine Verknüpfung von Abrechnungsdaten aller Kassen-Ärzte mit den Daten aus den von ihnen ausgestellten Rezepten. Die verknüpften Daten sollen für die Vorbereitung von Verhandlungen zwischen Kassenärztlichen Vereinigungen und Krankenkassen ausgewertet, die Rezeptdaten allein zur Beratung von Ärzten verwandt werden. Mit der Federführung bei der Beratung und Bewertung des Projekts wurden wir von den anderen Landesbeauftragten für Datenschutz beauftragt.

Durch die Umsetzung des komplexen Projekts entsteht eine Datenbank, in der enorme Mengen an medizinischen Daten über alle gesetzlich Versicherten Deutschlands gespeichert sind: Für alle Versicherten sämtliche Verordnungen der letzten fünf Jahre, angereichert mit den Diagnosen, welche von den Ärztinnen und Ärzten den Kassenärztlichen Vereinigungen gemeldet wurden. Auch enthalten sind soziale Angaben wie ein Sozialhilfebezug der oder des Versicherten oder eine Gebührenbefreiung. Die Daten sind nicht mit den Namen der Patientinnen und Patienten, sondern mit einem Pseudonym verknüpft. Wer jedoch auch nur wenig über eine Versicherte oder einen Versicherten weiß, wird keine Schwierigkeiten haben, den Datensatz zu finden, der auf diese Person und keine andere passt.

Das Zentralinstitut mit Sitz in Berlin soll die Auswertung der Datenbank zentral im Auftrag einer Reihe von Kassenärztlichen Vereinigungen, u. a.auch der Kassenärztlichen Vereinigung Berlin, vornehmen. Das ursprüngliche, nicht vollständig sozialrechtlich legitimierte Ziel der Auswertungen war, den Kassenärztlichen Vereinigungen und der Kassenärztlichen Bundesvereinigung eine Datengrundlage für eine erfolgreiche Führung der Verhandlungen mit den Krankenkassen über die Vergütung der niedergelassenen Ärztinnen und Ärzte und ihr Arzneimittelbudget zu schaffen. Damit war der Rahmen für Auswertungen

außerordentlich weit gesteckt. Missbräuchliche Auswertungen sind möglich und laufen Gefahr, in der Menge der Datenbankabfragen unterzugehen.

Wir konnten erreichen, dass sich die Kassenärztlichen Vereinigungen auf eine Nutzung der Daten für die gesetzlich vorgegebenen Zwecke beschränkt: Der Gesetzgeber hat vorgesehen, dass Verordnungsdaten von den Kassenärztlichen Vereinigungen nur für die Steuerung des Verordnungsverhaltens verwendet werden dürfen. Des Weiteren konnten wir durchsetzen, dass der Umfang der Abrechnungsdaten, mit denen die Verordnungsdaten angereichert werden sollen, erheblich eingeschränkt wird. So werden Daten von Kostenträgern, die nicht Vertragspartner der vorzubereitenden Verträge sind, nunmehr anonymisiert und nur noch für die Überprüfung der Vollständigkeit der Datenlieferungen verwandt. Schließlich darf das Zentralinstitut lediglich Auswertungen ausführen, die explizit von der beauftragenden Kassenärztlichen Vereinigung spezifiziert worden sind. Die Einhaltung dieser Vorgaben werden wir überprüfen, soweit Berliner Arztpraxen und deren Patientinnen und Patienten betroffen sind.

Dreh- und Angelpunkt für den Schutz der Versicherten in dem Datenbankprojekt ist die gesetzlich vorgeschriebene Pseudonymisierung der Daten. Jeder und jedem Versicherten wird auf der Basis der eigenen Versichertennummer, jeder Ärztin und jedem Arzt auf der Basis der eigenen Arztnummer eindeutig eine Zeichenfolge – ein Pseudonym – zugeordnet, mit dem alle Datensätze, die die Person betreffen, versehen werden. Es ist entscheidend, dass aus diesem Pseudonym keine Rückschlüsse auf die Identität der oder des Versicherten möglich sind. Dazu muss die Zuordnung geheim und darf ohne Kenntnis des Geheimnisses auch mit massivem Aufwand nicht ermittelbar sein. Berechnet werden die Pseudonyme in einer Vertrauensstelle. Angesichts der Sensitivität der zu schützenden Daten ist sie hoch sicher auszugestalten. Der Gesetzgeber schreibt zusätzlich die Trennung der Vertrauensstelle von den Nutzenden der Daten vor.

Auf unsere Empfehlung hin erfolgte eine professionelle Planung der notwendigen technischen Sicherungseinrichtungen. Die zur Berechnung der Pseudonyme notwendigen geheimen Daten werden in einem speziell geschützten Gerät, einem sog. Hardware Security Module, gespeichert und verlassen dieses nie. Mehrfach gestaffelte Schutzmechanismen bewahren die eingesetzten

Computersysteme vor Manipulation und die Daten der Versicherten vor Einsichtnahme.

Gefahrenpotenziale bleiben. Von uns als unzulässig bewertete Rückübermittlungen an Kassenärztliche Vereinigungen stellen die Sicherheit der Pseudonymisierung in Frage. Die Nutzung der Datenbank bedarf der fortlaufenden Überwachung durch den internen Datenschutzbeauftragten. Die Protokollierung der Datenbankzugriffe und der Ausschluss von direkten oder mittelbaren Zugriffen Dritter, etwa der Kassenärztlichen Bundesvereinigung, auf die Datenbank ist noch nicht geklärt. Die örtliche Nähe zwischen Vertrauensstelle und Zentralinstitut erleichtert ein illegitimes Zusammenbringen einzelner Daten der beiden Institutionen. Die Zuverlässigkeit der eingesetzten kryptographischen Verfahren zum Schutz der Daten bei ihrem Transport über das Internet bedarf der ständigen Beobachtung im Zuge der Weiterentwicklung der Technik.

Jede reichhaltig gefüllte Datenbank weckt Begehrlichkeiten. Der Bundesgesetzgeber hat den Beteiligten der gesetzlichen Krankenversicherung vielfach Aufgaben zugewiesen, ohne die Verarbeitung der dafür erforderlichen Daten klar und abschließend zu regeln. Die unscharfe Linie zwischen zulässiger und unzulässiger Verarbeitung und Nutzung der bereits vorliegenden Daten ist schnell überschritten. Der vom Gesetzgeber datenschutzrechtlich sorgfältig vorbereitete Datentransparenzpool[101], der die erforderlichen Daten einheitlich und ohne Mehrfachspeicherungen mit ihrem zusätzlichen Risikopotenzial bereitstellen könnte, wird weder von der Selbstverwaltung der gesetzlichen Krankenversicherung noch von der Bundesverwaltung vorangetrieben.

Aufbau und Betrieb großer Analysedatenbanken im Bereich der gesetzlichen Krankenversicherung bedürfen engmaschiger datenschutzrechtlicher und -technischer Überwachung und Kontrolle, um Wildwüchse und fahrlässigen Umgang zu vermeiden. Für eine datenschutzfreundliche Gestaltung des Verfahrens gilt: Das Datenaufkommen ist den Zwecken entsprechend zu minimieren. Die Daten sind sachgerecht zu pseudonymisieren, technisch und organisatorisch zu schützen sowie frühzeitig zu löschen.

101 §§ 303 a ff. SGB V

## 7.2.2 Gemeinsames Krebsregister

Das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen bat uns im Frühjahr darum, ein Softwareprodukt zu bewerten, welches zur Dateiverschlüsselung eingesetzt werden sollte. Eine Überprüfung der Einsatzumgebung brachte erhebliche Versäumnisse bei der Einhaltung der gesetzlichen Vorgaben zum Schutz dieses hoch sensitiven Datenbestandes zutage: Die Mängel betrafen sowohl die Datenschutzorganisation und gesetzlich vorgegebene, jedoch nicht umgesetzte Verfahrensweisen als auch teilweise völlig unzulängliche technische Verfahren.

Das Gemeinsame Krebsregister hat die Aufgabe, Daten über möglichst alle Diagnosen von Krebserkrankungen und auf solche Erkrankungen zurückführbare Todesfälle in den genannten Ländern zu registrieren, statistisch auszuwerten und der wissenschaftlichen Forschung für genehmigte Vorhaben zur Verfügung zu stellen. Es kann hierzu auf den größten Bestand an epidemiologischen Krebsregisterdaten der Bundesrepublik zurückgreifen. In Berlin sind Ärztinnen und Ärzte sowie Gesundheitsämter verpflichtet, die genannten Daten dem Krebsregister zu melden.

Zur Wahrung des Datenschutzes ist das Krebsregister in zwei getrennte Stellen eingeteilt: Die Vertrauensstelle erfasst und pseudonymisiert die eingehenden Meldungen der Ärztinnen und Ärzte, klinischen Tumorzentren und Gesundheitsämter. Die Registerstelle verwahrt die pseudonymisierten Daten, wertet sie statistisch aus und gibt sie für Forschungsvorhaben frei. Benötigen diese für genehmigte Zwecke den Zugriff auf die Identität der Betroffenen (z. B. um einen Abgleich mit Risikofaktoren zu ermöglichen, denen einzelne Betroffene ausgesetzt waren), so stellt die Vertrauensstelle den Bezug zu den Betroffenen wieder her. Hierzu sind den Registerdaten verschlüsselte Angaben über die Identität der Betroffenen beigegeben.

Mit der Verschlüsselung und Pseudonymisierung werden aus Sicht des Datenschutzes zwei Ziele erreicht. Zum einen beschränken sie die Verfügungsgewalt der Beschäftigten der Registerstelle. Sie haben zwar Zugriff auf einen immensen Bestand von Daten, die für die Betroffenen erhebliche Sensitivität besitzen, können aber weder ein gegebenes Datum einem einzelnen Betroffenen

zuordnen noch für einen namentlich bekannten Betroffenen die medizinischen Daten auffinden. Zum anderen verringern sie die Folgen eines erfolgreichen Einbruchs in die Computersysteme des Registers. Auch Datendiebe können die Daten nicht interpretieren.

Umso wichtiger ist es, die Daten beider Stellen sorgfältig voneinander zu trennen, Verschlüsselungs- und Pseudonymisierungsverfahren entsprechend dem Stand der Technik auszuwählen und die einfließenden geheimen Parameter zu schützen. Der Gesetzgeber hat hierzu klare Normen erlassen. Das Krebsregister ignorierte jedoch teilweise diese Normen, setzte sich nicht mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) ins Benehmen und verzichtete ganz auf externe Expertise. Unabhängige behördliche Datenschutzbeauftragte, welche die Einhaltung der Verfahrensregeln anmahnen und die Datenverarbeitung hätten überwachen können, waren nicht bestellt.

In der Folge wurde ein völlig unqualifiziertes Verschlüsselungsfahren gewählt, dessen Sicherheit bei weitem nicht ausreichend war. Auf unsere Intervention hin wurde ein Wechsel des Verschlüsselungsverfahrens vorgenommen und die existierenden Datenbestände (in einem ungeregelten Verfahren) umgestellt. Das Ersatzverfahren entspricht dem Stand der Technik von vor zehn Jahren. Eine derzeit laufende Abstimmung mit dem BSI soll zu einer Aktualisierung der eingesetzten Techniken führen. Nichtfachgerechtes Vorgehen fand sich ferner beim Schutz des Registers vor Einbruch und Brand wie auch beim Schutz geheimer technischer Daten für die Verschlüsselung und Pseudonymisierung. Im Zusammenwirken mit dem Landeskriminalamt konnten wir erreichen, dass das GKR im ersten Quartal 2010 wieder über eine funktionsfähige, polizeiaufgeschaltete Einbruchsmeldeanlage verfügen wird, welche allerdings noch der Anpassung an den gegenwärtigen Stand der Technik bedarf. Für den Schutz der geheimen technischen Daten lag zum Ende des Berichtszeitraums zumindest ein Grobkonzept vor.

Besonders eklatant sind jedoch die Gefahren, denen die medizinischen Daten bei ihrer obligatorischen Meldung an das Register ausgesetzt sind: Ohne gesetzliche Grundlage begann das Krebsregister, die Tumorzentren zu bitten, ihre Meldungen über das Internet zuzusenden; nach der Schaffung dieser Grundlagen wurde das Verfahren den nunmehr explizit niedergeschriebenen gesetzlichen Erfordernissen nicht angepasst. Wo der Gesetzgeber ein Verfahren auf

dem Stand der Technik erwartete, kam und kommt eine ohne kryptographischen Sachverstand produzierte Eigenentwicklung zur Anwendung, die einem ernsthaften (und nicht feststellbaren) Angriff keinen nennenswerten Widerstand entgegensetzen würde.

Wir haben gefordert, dass die Übertragung derart schwach geschützter mit Namen und Anschrift der Betroffenen versehenen Krebsdiagnosen sofort eingestellt wird. Die Risiken für die Betroffenen sind nicht tragbar. Zu dieser Sofortmaßnahme konnten sich Register und aufsichtführende Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz jedoch nicht entschließen, obwohl gesetzeskonforme und deutlich sicherere Alternativverfahren für einen schnellen Ersatz zur Verfügung stehen. Stattdessen plant das Krebsregister unter der Direktion seines Verwaltungsrates und der Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz eine schrittweise Umstellung, beginnend im ersten Quartal 2010, jedoch noch ohne Frist für ihren Abschluss.

Begonnen wurde gleichfalls mit der Planung der dringend notwendigen Herstellung der technischen Informationssicherheit in beiden Stellen des Registers auf einem Niveau, welches der Sensitivität der dort gespeicherten und verarbeiteten Daten angemessen ist. Die beteiligten Länder sind aufgerufen, die für die Umsetzung der Planungen und die Ausstattung des Gemeinsamen Krebsregisters mit zusätzlichem IT-Personal notwendigen Finanzmittel bereitzustellen sowie für eine zügige Umsetzung der geplanten Maßnahmen zu sorgen.

Im Gemeinsamen Krebsregister sind jahrelange Versäumnisse in der Durchsetzung des technischen Datenschutzes aufzuholen. Dies erfordert kurzfristig eine Rückbesinnung auf etablierte Verfahrensregeln und den Einsatz nicht unerheblicher finanzieller Mittel. Um das Datenschutzniveau nach einer solchen Investition dauerhaft zu halten, ist das Register mit Personal auszustatten, welches den erforderlichen technischen und datenschutzrechtlichen Sachverstand besitzt.

### 7.2.3 Krankenhaus-Zuweiserportale

Ein großes Krankenhausunternehmen hat ein Webportal in Betrieb genommen, über das niedergelassene Ärztinnen und Ärzte Dokumente über die stationäre Behandlung von Kranken einsehen können, die sie in ein Krankenhaus des Unternehmens eingewiesen haben. Wir wollten wissen, ob die sensiblen medizinischen Daten, die über das Internet übermittelt werden, ausreichend geschützt sind.

Die Nutzung des Portals steht Patientinnen und Patienten sowie Ärztinnen und Ärzten auf freiwilliger Basis und kostenfrei zur Verfügung. Aufgrund unserer Forderung werden die Kranken mittlerweile in einer Datenschutzerklärung über die Verarbeitungsvorgänge informiert und können ihre schriftliche Einwilligung auf der Basis dieses Wissens geben oder verweigern.

Unter der Berliner Ärzteschaft wurde das Projekt intensiv beworben. Eine beträchtliche Zahl von Ärztinnen und Ärzten schrieb sich in die Teilnehmerliste ein. Aktiv genutzt wurde es jedoch nur von einem Bruchteil. Dies führte dazu, dass der weit überwiegende Anteil der auf dem Webserver bereitgestellten Dokumente nie abgerufen wurde. Auf unsere Intervention hin begrenzt der Betreiber die Speicherdauer der Dokumente und meldet (nach Rücksprache) Ärztinnen und Ärzte von dem System ab, die über einen Zeitraum von sechs Monaten das Portal nicht nutzen.

Die Daten werden nicht durch das behandelnde Krankenhaus vorgehalten, sondern in dem Rechenzentrum eines rechtlich selbständigen Thüringer Krankenhauses gespeichert und über die an einem dritten Ort befindlichen Server des Mutterkonzerns zur Verfügung gestellt. An beiden Orten ist eine (nicht erforderliche) Kenntnisnahme der Dokumente möglich. Dies steht im Widerspruch zum datenschutzrechtlichen Gebot der Datensparsamkeit und, vor allem, der ärztlichen Schweigepflicht. Wir konnten bewirken, dass eine Verschlüsselung der konzerninternen Datenweitergaben sukzessive eingeführt wird, um die medizinischen Daten auch vor einem Zugriff durch interne und externe IT-Dienstleister zu schützen. Die Möglichkeit der Kenntnisnahme auf den Servern der äußeren Netzgrenze bei der Konzernmutter besteht weiterhin und wird erst mittelfristig beseitigt.

Der größte sicherheitstechnische Schwachpunkt des Projekts besteht jedoch nicht auf der Anbieter-, sondern auf der Nutzerseite: Auch bei einer kryptographischen Absicherung der Übertragung vom Krankenhaus zu niedergelassenen Ärztinnen und Ärzten gelangen die medizinischen Dokumente schlussendlich im Klartext auf einen Rechner in der Praxis, welcher für den allgemeinen Zugriff auf das Internet genutzt wird. Die Gefährdung solcher Computer ist hinlänglich bekannt. Millionen von Privatcomputern werden jährlich von Kriminellen unterwandert und in der Folge von diesen gesteuert. Die Praxiscomputer, auf denen die Arztberichte und Befunde aus dem Portal eintreffen, sind (wir haben uns davon vor Ort überzeugt) nicht besser geschützt. Die Kassenärztliche Vereinigung Berlin und die Berliner Ärztekammer empfehlen verbindlich allen niedergelassenen Ärztinnen und Ärzten, Rechner mit Patientendaten vom Internet zu trennen. Nur speziell geschützte Verbindungen etwa zu den Abrechnungszentralen der Kassenärztlichen Vereinigungen sind zulässig.

Auf Rechnern, die für den allgemeinen Internetzugriff gedacht sind, dürfen medizinische Daten nicht im Klartext gespeichert oder angezeigt werden. Zuweiserportale dürfen daher lediglich verschlüsselte Dokumente anbieten, welche von der Ärztin oder dem Arzt erst im gesicherten Bereich ihrer Praxisverwaltungssysteme entschlüsselt werden. Die einzige Alternative besteht in der Nutzung sog. virtueller privater Netze (VPN),[102] bei denen die beteiligten Rechner nicht am allgemeinen Internetverkehr, sondern nur am Datenaustausch mit im Vorhinein festgelegten Kommunikationspartnern teilnehmen.

### 7.2.4 Schwache Datenschutzorganisation in Klinikkonzernen

Große Krankenhausunternehmen verarbeiten riesige Mengen sensitiver Gesundheits- und Personaldaten. Einige Häuser statten die interne Datenschutzkontrolle nicht dementsprechend aus. So mussten wir mit Befremden zur Kenntnis nehmen, dass die Vivantes Netzwerk für Gesundheit GmbH in der Jahresmitte die Personalressourcen ihres betrieblichen Datenschutzes drastisch reduzierte. Als größter kommunaler Krankenhauskonzern Deutschlands

102 Vgl. dazu 2.6

hat sich Vivantes das Ziel gestellt, Vorreiter einer sich im Wandel befindlichen Branche zu sein. Dazu passt die genannte Entscheidung nicht: Ein modernes Krankenhausunternehmen mit neun Standorten und rund 5.000 Betten ohne einen funktionierenden Datenschutz ist undenkbar, insbesondere bei der starken Technisierung, welche die medizinische Versorgung heutzutage durchdringt, und den vielfältigen Dokumentationserfordernissen, die zu immer umfangreicheren Datenmengen mit sensiblen Informationen über die Patientinnen und Patienten führen.

Der betriebliche Datenschutzbeauftragte ist in alle Planungen von IT-gestützten Verfahren einzubeziehen. Solche Verfahren, die mit besonderen Risiken für die Betroffenen verbunden sind, unterliegen seiner Vorabkontrolle. In seiner Hand liegt das Wissensmanagement auf dem Gebiet des Datenschutzes. Er ist Ansprechpartner für Patientinnen und Patienten wie Beschäftigte. Er berät die Geschäftsführung und holt sich seinerseits in Zweifelsfällen Rat bei uns. Letzteres hat sich insbesondere im Vorfeld von Kontrollen bewährt.

Vivantes ist nicht der einzige in Berlin ansässige Krankenhauskonzern mit Defiziten im Datenschutzmanagement. Die Helios Kliniken GmbH ließ uns über Monate im Unklaren über die Person ihres betrieblichen Datenschutzbeauftragten und zog es vor, unsere Anschreiben zu ignorieren. Erst nach direkter Ansprache sah sich die Geschäftsführung des Konzerns in der Lage, einen aktiv tätigen Datenschutzbeauftragten zu bestellen. Dieser begann im Laufe des Jahres, eine Datenschutzkontrollstruktur und ein Netzwerk von Ansprechpartnern in den einzelnen Häusern aufzubauen. Nichtsdestotrotz ist nicht zu übersehen: Hier ist ein Datenschutzbeauftragter für insgesamt rund 70 Betriebsstätten zuständig.

Krankenhausunternehmen haben für eine rechtskonforme Bestellung und Unterstützung des Datenschutzbeauftragten durch die Bereitstellung von Hilfspersonal, Räumen, Geräten und Mitteln zu sorgen. Dies kommt den behandelten Patientinnen und Patienten sowie dem Personal zugute. Darüber hinaus ist es Voraussetzung für eine positive Wahrnehmung in Politik und Öffentlichkeit.

## 7.2.5 Elektronische Gesundheitskarte

Der verzögerte Aufbau der Gesundheitstelematik-Infrastruktur (TI) und der Einführung der elektronischen Gesundheitskarte (eGK) mit nunmehr stark eingeschränkter Funktionalität dauert an. Wir haben die Ausarbeitung des übergreifenden Datenschutzkonzepts begleitet und nachdrücklich auf die Notwendigkeit hingewiesen, die Voraussetzungen für die Ausübung der Patientenrechte zu schaffen.

Im Großprojekt Gesundheitskarte und Gesundheitstelematik-Infrastruktur sollen große Mengen sensitiver medizinischer Daten der gesetzlich Versicherten verarbeitet werden. Dem Datenschutz und der Datensicherheit muss dementsprechend hohe Priorität eingeräumt werden. Die Defizite auf diesem Gebiet liegen jedoch nicht dort, wo eine zuweilen lautstark in der Öffentlichkeit geäußerte Kritik sie vermuten lässt. Wie unsere Prüfungen gezeigt haben[103], besteht vor allem ein großer Bedarf nach einer sicheren Plattform für den Datenaustausch zwischen Ärztinnen und Ärzten und in die Behandlung eingebundenen Einrichtungen. Die Telematik-Infrastruktur kann eine solche Plattform mit hohem Niveau der Datensicherheit bieten.

Die elektronische Gesundheitskarte wird zunächst nur die Überprüfung des Versichertenstatus einer Patientin oder eines Patienten ermöglichen. Später tritt auf freiwilliger Grundlage ein Basisdatensatz mit medizinischen Daten der oder des Versicherten hinzu, der auf der Karte gespeichert und auf den im Notfall zugegriffen werden soll. Bereits hier, wie auch bei allen späteren Anwendungen, gilt: Die Betroffenen (die Versicherten) müssen ihre Rechte wahrnehmen können. Sie müssen über die Funktionsweise der Karte verständlich unterrichtet werden und sich kostenfrei und ohne Hemmschwellen technischer oder organisatorischer Art über die in der Karte abgelegten Daten informieren können. Fehlerhafte Daten müssen berichtigt und Daten gelöscht werden, deren Nutzung nicht vom Gesetz vorgesehen wurde und die ohne Einverständnis der oder des Versicherten oder trotz des Widerrufs ihres oder seines Einverständnisses gespeichert wurden.

103 Vgl. 7.2.3

Die Gematik, die von den Beteiligten der gesetzlichen Krankenversicherungen errichtete Betriebsgesellschaft für die TI und die Einführung der eGK, hat für die Ausübung der genannten Rechte Verfahren skizziert. Die Versicherten sollen sie in den Räumen der Krankenkassen, bei den Leistungserbringern oder bei sich zu Hause anwenden können. Die Planungen dafür hinken den Anwendungen, die sie begleiten sollen, jedoch beträchtlich hinterher. Eine Einführung der Karte mit echten Daten ohne ihre Umsetzung wäre rechtswidrig und würde die Gefahr bergen, einzelnen Versicherten ernsthaften Schaden zuzufügen.

Aus diesem Grund wirkten wir bei der Durchsicht des übergreifenden Datenschutzkonzepts der Gesundheitstelematik mit. Als turnusmäßiger Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Gematik zur raschen Ausarbeitung und Umsetzung der Konzepte zur Wahrnehmung der Versichertenrechte aufgefordert.

Relativ unbeachtet von der Öffentlichkeit erfolgt die Einführung eines zweiten Kartentyps – des elektronischen Heilberufeausweises – und die Vorbereitung der Anbindung der Gesundheitseinrichtungen und Arztpraxen an eine gemeinsame Telematik-Infrastruktur. Sie ermöglicht authentische und geschützte Übermittlung von medizinischen Dokumenten von Arzt zu Arzt, vom Krankenhaus zum niedergelassenen Arzt sowie zwischen verschiedenen medizinischen Leistungserbringern. Es ist zu hoffen, dass damit den derzeit wild wachsenden Ad-Hoc-Lösungen für einen solchen Austausch ein Ende bereitet wird, sodass einerseits die medizinischen Daten vor unautorisiertem Zugriff bei der Übermittlung geschützt werden und andererseits vermieden wird, dass medizinische Daten vorhaltende Systeme an das freie Internet angebunden und Angriffen ausgesetzt werden.

Uns wurden einige Systeme vorgestellt, die sich das Ziel gesetzt haben, die eGK zu ersetzen oder zu ergänzen. Eines davon, eine Patientenakte, die von einem Frankfurter Unternehmen vorgeschlagen wurde, arbeitet wie auch einige andere Dienstleistungen, die im Internet bereitgestellt werden, „patientengeführt“, d. h., die Patientin oder der Patient bestimmt allein die Verwendung der eigenen Daten. Diese verlassen damit den Schutzbereich des ärztlichen Berufsgeheimnisses. Im Gegensatz dazu kann die Patientin oder der Patient die Daten

der eGK nur einem Arzt oder Therapeuten ihrer oder seiner Wahl offenbaren, nicht beliebigen Dritten, die Druck auf sie oder ihn ausüben können. Unklar ist noch, wie die Daten gegenüber dem Betreiber des vorgeschlagenen Systems geschützt werden: Bei einigen internetbasierten Patientenakten bekannter Anbieter haben diese technisch unbeschränkten Zugriff.

Auch bei einer Beschränkung der Funktionalität der Gesundheitskarte müssen die Voraussetzungen für die Wahrnehmung der Betroffenenrechte – Transparenz für und Kontrolle durch die Versicherten – von Anfang an gewährleistet werden. Die Gesundheitstelematik-Infrastruktur bietet im Hinblick auf die Datensicherheit eine solide Basis für den Austausch von medizinischen Daten.

### 7.2.6 Auskunftsersuchen der Polizei gegenüber Krankenhäusern

Krankenhäuser werden von der Polizei häufig um Auskünfte zum Aufenthalt von bestimmten Patientinnen und Patienten oder zu deren Personalien gebeten. Dies geschieht in der Regel nicht auf schriftlichem Wege, sondern durch direkte Befragung von Personal in der Krankenhausaufnahme.

Die Beantwortung dieser Anfragen bedeutet für die Krankenhausbeschäftigten eine Durchbrechung der ärztlichen Schweigepflicht. Dies ist auch dann der Fall, wenn sich das Auskunftsersuchen nur auf den Umstand bezieht, ob eine bestimmte Person derzeit in Behandlung ist oder zu einem bestimmten Zeitpunkt in Behandlung war. Eine Offenbarung dieser Information ist nur aufgrund einer Erklärung der betroffenen Person zur Entbindung von der Schweigepflicht oder aufgrund einer gesetzlichen Befugnis zulässig.

Die Polizei beruft sich vorrangig auf § 22 Abs. 4 Meldegesetz. Danach ist es zulässig, im Einzelfall Auskünfte aus dem von der Krankenhausleitung zu führenden Verzeichnis über die im Krankenhaus aufgenommenen Personen an Ordnungs- und Sicherheitsbehörden zu erteilen. Das Verzeichnis enthält neben Namen, Anschrift und Geburtsdatum der oder des Kranken auch den Tag der Aufnahme und Entlassung. Es ist für ein Jahr nach dem Ende des Jahres der

Entlassung aufzubewahren. Diese melderechtliche Befugnis zur Übermittlung von Patientendaten steht aber unter dem ausdrücklichen Vorbehalt, dass die ärztliche Schweigepflicht nicht verletzt wird. Daraus folgt, dass die Vorschrift selbst keine Befugnis zum Bruch des Patientengeheimnisses enthält. Weiter gehende Auskunftsrechte für die Polizei ergeben sich im Übrigen auch nicht aus den allgemeinen strafprozessualen Ermittlungsbefugnissen (§§ 161, 163 StPO). Auch diese finden ihre Grenze in den besonderen Geheimhaltungspflichten.

Eine Auskunftserteilung des Krankenhauses kann daher nur dann als zulässig erachtet werden, wenn die Voraussetzungen eines rechtfertigenden Notstands vorliegen, d.h. wenn die Offenbarung von Patientendaten im Einzelfall zum Schutz höherwertiger Rechtsgüter erforderlich ist. Dies ist etwa anzunehmen, wenn nur durch die Datenübermittlung an die Polizei eine gegenwärtige Gefahr für Leib, Leben oder persönliche Freiheit abgewendet werden kann. Dem entspricht auch § 27 Abs. 3 Satz 1 Nr. 3 Landeskrankenhausgesetz. Demgegenüber rechtfertigt das Strafverfolgungsinteresse bezüglich bereits begangener Delikte die Verletzung der ärztlichen Schweigepflicht grundsätzlich nicht. Etwas anderes kann sich nur dann ergeben, wenn die Gefahr besteht, dass die Patientin oder der Patient auch weiterhin erhebliche Straftaten begehen wird (Wiederholungsgefahr). Auch in diesen Fällen ist aber abzuwägen, ob die gefährdeten Rechtsgüter schutzwürdiger sind als das Geheimhaltungsinteresse der oder des Kranken. So wird der Schutz fremder Vermögensinteressen nur ausnahmsweise die Durchbrechung der ärztlichen Schweigepflicht legitimieren können. Anders wäre die Situation zu bewerten, wenn die Patientin oder der Patient die ärztliche Schweigepflicht zur Deckung eigener Straftaten benutzen will.

Mit der im Einzelfall schwierigen Entscheidung, ob eine Durchbrechung der ärztlichen Schweigepflicht gegenüber der Polizei gerechtfertigt ist, sollten nicht die in der Krankenhausaufnahme beschäftigten Personen belastet werden. Wir empfehlen den Krankenhäusern, die Polizei an eine zentrale Stelle (z. B. die Geschäftsleitung oder die ärztliche Direktion) zu verweisen, wo über Auskunftsersuchen nach einheitlichen Maßstäben entschieden werden kann. Ferner sollte die Polizei die Anfragen möglichst schriftlich stellen und dabei den Zweck der Datenerhebung präzise darlegen. Eine erfolgte Auskunftserteilung ist vom Krankenhaus zu dokumentieren.

Auch wenn keine medizinischen Daten übermittelt werden, sondern lediglich der Aufenthalt einer bestimmten Person im Krankenhaus gegenüber der Polizei bestätigt wird, ist damit eine Durchbrechung der ärztlichen Schweigepflicht verbunden. Die Offenbarung des Patientengeheimnisses ist nur im Einzelfall bei konkreter Gefährdung höherwertiger Rechtsgüter zulässig. Eine Verpflichtung zur Auskunftserteilung durch die Krankenhäuser besteht nicht.

Krankenhäuser dürfen der Polizei nur dann Auskunft über Patienten erteilen, wenn dadurch eine gegenwärtige Gefahr für Leib, Leben oder persönliche Freiheit eines Menschen abgewendet werden kann. Die Entscheidung über die Auskunftserteilung sollte der Leitung des Krankenhauses vorbehalten bleiben.

## 7.2.7 Biographiedaten in der Pflege

Ein Bürger beschwerte sich darüber, dass der ihn betreuende häusliche Pflegedienst detaillierte biographische Angaben über seine Person erfassen wollte. Dazu wurde ihm ein Formular mit der Bezeichnung „Biographiebogen“ mit der Bitte übergeben, den darin enthaltenen Fragenkatalog zu beantworten. Die Fragen betrafen zum Teil sehr persönliche, intime Lebensbereiche und -gewohnheiten.

Derartige Fragebögen sind heute fester Bestandteil der sog. Biographiearbeit in der ambulanten und stationären Pflege. Ziel dieser Arbeit ist die Unterstützung der Individualität der oder des Pflegebedürftigen durch die Pflegenden. Es werden Informationen aus der Biographie des pflege- und betreuungsbedürftigen Menschen gesammelt, um durch die Einbeziehung dieser Informationen in den Pflegeprozess eine persönlichkeitsfördernde und individuelle Pflege und Betreuung zu ermöglichen. Der Nutzen der Biographiearbeit ist nicht zu bezweifeln. Gleichwohl darf nicht übersehen werden, dass damit eine umfangreiche Erhebung und Verarbeitung personenbezogener, teilweise äußerst sensitiver Daten verbunden ist. Durch die Sammlung von biographischen Angaben wird in das Recht der oder des Pflegebedürftigen auf informationelle Selbstbestimmung eingegriffen.

Eine gesetzliche oder vertragliche Verpflichtung für die Pflegebedürftigen, dem Pflegedienst diese Daten mitzuteilen, besteht nicht. Biographiearbeit ist nur auf freiwilliger Basis möglich. Die Erhebung und Verarbeitung von Biographiedaten setzt daher die Einwilligung der oder des Pflegebedürftigen bzw. der betreuenden Person voraus. Dazu gehört die vorherige umfassende Information über Sinn und Zweck der Biographiearbeit, über die Dokumentation der Daten sowie über den zugriffsberechtigten Personenkreis. Ferner muss ein ausdrücklicher Hinweis auf die Freiwilligkeit der Angaben erfolgen. Die Freiwilligkeit muss sich auch auf die Beantwortung einzelner Fragen bzw. das Schweigen zu einzelnen Themenblöcken beziehen. Der Umfang der Datenerhebung darf über die für die Durchführung des von dem Pflegedienst praktizierten Konzepts zur Biographiearbeit notwendigen Daten nicht hinausgehen. Die Informationssammlung ist individuell und unter Beachtung der Erforderlichkeit und Verhältnismäßigkeit auf die pflegebedürftige Person abzustimmen. Das gilt insbesondere, wenn es sich um sensitive Daten handelt. So gibt es etwa keinen Bedarf, gezielte Fragen zur politischen oder sexuellen Ausrichtung zu stellen.

Der von der Beschwerde betroffene Pflegedienst hat auf unsere Forderungen umgehend reagiert und den kritisierten Fragebogen angepasst. So wurden die Fragen zur finanziellen Situation, zu „Kriegserlebnissen“ und zu psychosozialen und gerontopsychiatrischen Aspekten (wie Ängsten, Wünschen, Sozialverhalten) vollständig entfernt. Ferner wurde ein Hinweis auf die Freiwilligkeit der Angaben sowie Informationen über den Aufbewahrungsort des Biographiebogens und die zugriffsberechtigten Personen aufgenommen.

Biographiearbeit setzt ein Vertrauensverhältnis zwischen Pflegenden und Pflegebedürftigen voraus. Sie darf nur auf freiwilliger Basis unter Beachtung des Rechts auf informationelle Selbstbestimmung erfolgen. Die Erhebung biographischer Angaben bei Pflegebedürftigen setzt deren informierte Einwilligung voraus.

## 7.2.8 Anforderung von Patientenunterlagen durch die Ärztekammer

Bei der Prüfung einer Bürgereingabe hatten wir die Frage zu beurteilen, ob und auf welcher Rechtsgrundlage die Berliner Ärztekammer im Rahmen eines berufsrechtlichen Beschwerdeverfahrens Patientenunterlagen bei Ärztinnen und Ärzten anfordern darf.

Die Ärztekammer überwacht nach dem Berliner Kammergesetz die Einhaltung der Berufspflichten ihrer Mitglieder. Sie hat daher bei Bekanntwerden von Tatsachen, die den Verdacht einer Berufspflichtverletzung rechtfertigen, von Amts wegen berufsrechtliche Ermittlungen einzuleiten. Dabei ist es in vielen Fällen auch erforderlich, auf die bei der oder dem Beschuldigten geführte Patientendokumentation zuzugreifen, um einen konkreten Pflichtverstoß belegen zu können. Dem steht jedoch die ärztliche Schweigepflicht entgegen, die grundsätzlich auch bei Auskünften gegenüber der Kammer zu beachten ist. Eine Offenbarung von Patientendaten ist nur zulässig, wenn die Ärztin oder der Arzt wirksam von der Schweigepflicht entbunden wurde oder besondere gesetzliche Offenbarungsbefugnisse bestehen. Letztere finden sich im Berliner Kammergesetz nicht. Der Kammer wird nicht in hinreichend konkreter Form gestattet, Zugriff auf Patientenunterlagen und damit auf personenbezogene Daten Dritter zu nehmen. Insoweit unterscheidet sich das Berliner Gesetz von den Regelungen anderer Bundesländer, die zum Teil die Anforderung von Behandlungsunterlagen ausdrücklich vorsehen. Die Ärztekammer will daher eine entsprechende Gesetzesänderung initiieren.

Nach der derzeitigen Rechtslage ist vor der Anforderung von Patientenunterlagen im Rahmen berufsrechtlicher Ermittlungen in aller Regel eine Schweigepflichtentbindungserklärung der betroffenen Patientinnen und Patienten einzuholen. Dabei ist im Hinblick auf die Form der Patienteneinwilligung zu differenzieren:

Wenn eine Patientin oder ein Patient selbst Beschwerde einlegt, das beanstandete Verhalten der Ärztin oder des Arztes unter Bezugnahme auf bestimmte Erkrankungen darlegt und um entsprechende Prüfung durch die Kammer bittet, wird er in der Regel die Einsichtnahme der Kammer in die ärztliche Dokumentation bereits voraussetzen. In diesen Fällen kann von einem kon-

kludenten Einverständnis ausgegangen werden, das dem Berufsgeheimnisträger eine Offenbarung entscheidungserheblicher Tatsachen gegenüber der Kammer erlaubt.

Eine Beschwerde kann aber auch umgekehrt der Kammer nahelegen, keine personenbezogene, d. h. unter Nennung des Patientennamens erfolgende Rückfrage oder Anforderung von Unterlagen bei der Ärztin oder dem Arzt vorzunehmen. Es kommt insoweit auf die konkreten Umstände des Einzelfalls an. Um mögliche Zweifelsfälle zu vermeiden und den diesbezüglichen Willen der Patientin oder des Patienten zu ermitteln, halten wir es für erforderlich, aber auch ausreichend, in der an sie oder ihn gerichteten Eingangsbestätigung darauf hinzuweisen, dass die Kammer die Beschwerde an die Ärztin oder den Arzt zur Stellungnahme weiterleitet und gegebenenfalls Behandlungsunterlagen anfordert. Widerspricht die Beschwerdeführerin oder der -führer dem nicht, kann daraus auf eine entsprechende Schweigepflichtentbindung geschlossen werden. Die Ärztekammer hat diesem Vorgehen zugestimmt und ihr Musterschreiben entsprechend angepasst.

Von dieser Konstellation sind Fälle zu unterscheiden, in denen sich Dritte in der Angelegenheit einer oder eines Kranken bei der Ärztekammer beschweren oder die Kammer auf anderem Wege Hinweise über mögliche Berufspflichtverletzungen erhält. Hier ist das ausdrückliche Einverständnis der oder des Kranken einzuholen, bevor sie oder ihn betreffende Behandlungsunterlagen beim Beschwerdegegner oder bei weiteren Ärzten angefordert werden. Lediglich wenn das aus tatsächlichen Gründen nicht möglich ist, etwa weil die oder der Kranke verstorben ist, kommt eine mutmaßliche Einwilligung als Rechtfertigungsgrund für die Offenbarung in Betracht. Die Ermittlungen sollten allerdings nur weitergeführt werden, wenn ein konkreter Anfangsverdacht besteht.

Die Ärztekammer hat uns des Weiteren auf Fälle hingewiesen, in denen die Patientin oder der Patient selbst kein Interesse an der Aufklärung der Berufspflichtverletzung hat, da sie oder er diese Verletzung als in eigenem Sinne versteht oder sogar mit der Ärztin oder dem Arzt zusammenarbeitet (z. B. Gefälligkeitsbescheinigungen oder ärztliche Verordnungen zur Weiterveräußerung oder zum Missbrauch von Psychopharmaka). Eine Schweigepflichtentbindungser 0klärung wird die Patientin oder der Patient daher gerade nicht abgeben. Die Herausgabe der Patientendokumentation auch gegen ihren oder seinen Willen

kann im Ausnahmefall zwar gerechtfertigt sein. So kann die Ärztin oder der Arzt sich auf die Wahrung eigener Interessen berufen, soweit die Geheimnisoffenbarung zur Abwendung eines drohenden berufsgerichtlichen Verfahrens erforderlich ist. Eine Verpflichtung zur Offenbarung folgt daraus aber nicht. Verweigert daher die Ärztin oder der Arzt unter Berufung auf die Schweigepflicht die Herausgabe der Akten, bleibt der Ärztekammer nur die Möglichkeit, einen gerichtlichen Beschlagnahmebeschluss zu erwirken. Die Vorschriften des Disziplinarrechts finden hier entsprechend Anwendung. Die insoweit zu beachtenden Beschlagnahmeverbote beziehen sich ausschließlich auf das Verhältnis der Ärztin oder des Arztes zu ihren Patientinnen und Patienten als Beschuldigte eines Ermittlungsverfahrens. Sie greifen dann nicht, wenn die Ärztin oder der Arzt selbst beschuldigt ist.

Die Übermittlung von Patientenunterlagen an die Ärztekammer im Rahmen eines berufsrechtlichen Ermittlungsverfahrens ist nur aufgrund einer Schweigepflichtentbindungserklärung der betroffenen Patienten zulässig. Beschwert sich die Patientin oder der Patient selbst bei der Ärztekammer, ist in aller Regel von einem konkludenten Einverständnis auszugehen. Verweigert die Ärztin oder der Arzt die Herausgabe der angeforderten Unterlagen, kann ein gerichtlicher Beschlagnahmebeschluss beantragt werden.

## 7.3 Personalwesen

### 7.3.1 AGG-Hopper-Datei beim Arbeitgeberverband

Ein großer Verband betrieb seit Mai 2007 für seine Mitglieder eine Datei (AGG-Hopper-Datei), die Daten abgelehnter Bewerberinnen und Bewerber enthielt, die sich auf das Allgemeine Gleichbehandlungsgesetz (AGG) und dort auf einen Diskriminierungsgrund berufen hatten. Im Kern ging es um eine Warndatei, in die Personen aufgenommen werden sollten, die rechtsmissbräuchlich Ansprüche nach dem AGG geltend gemacht hatten. Einmeldungen erfolgten ausschließlich durch die Mitglieder des Verbandes, die von einer betroffenen Person nach den Vorschriften des AGG in Anspruch genommen worden waren. In dem AGG-Archiv selbst wurden der Name der betroffenen Person, der betroffene

Arbeitgeber sowie der meldende Verband gespeichert. Im Zuge der Meldung wurde darüber hinaus auch der Schriftwechsel zwischen betroffener Person und Arbeitgeber im Rahmen des Bewerbungsverfahrens sowie der gerichtlichen oder außergerichtlichen Auseinandersetzung in einer gesonderten Akte gespeichert. Dabei wurden weitere, auch sensitive personenbezogene Daten nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) intern gespeichert. Insgesamt waren in der Datei zehn Personen gespeichert.

Unsere Prüfung dieser Datei ergab erhebliche datenschutzrechtliche Mängel. In dem gesamten AGG-Hopper-Verfahren waren keinerlei Hinweise darauf erkennbar, dass und anhand welcher Kriterien das „rechtsmissbräuchliche Verhalten" der eingemeldeten Person überprüft worden wäre. Insbesondere wurde der Ausgang des jeweiligen Verfahrens nicht abgewartet. Darüber hinaus wurde auch kein abschließender Vermerk angefertigt, in dem festgehalten wurde, ob die oder der Betroffene in die Datei aufgenommen werden soll. Spätere Urteile in den jeweiligen Verfahren wurden nicht berücksichtigt. Es existierte auch keine Weisung an die Mitglieder der verantwortlichen Stelle, die einen möglichen Missbrauchsfall gemeldet hatten. So war aus dem AGG-Archiv nicht ersichtlich, ob die dort eingetragene Person tatsächlich rechtsmissbräuchlich gehandelt hatte. Außerdem fand beim Abruf der Daten eine Einzelfallprüfung, ob ein berechtigtes Interesse vorlag, nicht statt; sie wurde dementsprechend auch nicht protokolliert.

Einmeldungen und Auskünfte im Rahmen der AGG-Hopper-Datei wurden über ein dafür eingerichtetes E-Mail-Postfach abgewickelt, auf das nur Beschäftigte der arbeitsrechtlichen Abteilung des Verbandes Zugriff hatten. Eine weiter gehende Verschlüsselung der E-Mails sowie der Anhänge, die den Schriftverkehr zwischen betroffener Person und Arbeitgeber enthielten, erfolgte nicht. Diesbezüglich wiesen wir darauf hin, dass ein solches Verfahren zur Übermittlung von sensitiven Daten nach § 3 Abs. 9 BDSG sowie sog. Personaldaten nicht geeignet ist, da grundsätzlich die Möglichkeit besteht, dass Dritte ohne erheblichen Aufwand Kenntnis der Daten erlangen.

Als Ergebnis unserer Prüfung empfahlen wir, die AGG-Hopper-Datei einzustellen. Der Verband teilte uns Anfang August mit, dass das Archiv nicht weiter betrieben wird.

## 7.3.2 Lehramtsanwärter auf Herz und Nieren geprüft

In einem Merkblatt des Prüfungsamts für Lehramtsprüfungen bei der Senatsverwaltung für Bildung, Wissenschaft und Forschung fand sich eine Regelung zum Nachweis krankheitsbedingter Ausfallzeiten im Zusammenhang mit der zweiten Staatsprüfung. Danach musste das ärztliche Attest bzw. das vertrauensärztliche Zeugnis nicht nur den Hinweis auf ein bestimmtes Krankheitsbild beinhalten, sondern auch die krankheitsbedingten Einschränkungen und Beschwerden, aus denen auf eine erhebliche Beeinträchtigung der Leistungsfähigkeit in der Prüfung geschlossen werden kann. Aus dem Fehlen einer Diagnose sollte die mangelnde Eignung des Attests zum Beleg einer Prüfungsunfähigkeit abgeleitet werden. Dies sollte nur dann nicht gelten, wenn bereits das Krankheitsbild selbst eindeutige Schlüsse auf eine Prüfungsunfähigkeit zulässt.

Die Kenntnis der Diagnose ist für die vom Prüfungsausschuss bzw. dem Prüfungsamt zu treffende Entscheidung grundsätzlich nicht erforderlich. Dementsprechend ist eine Verpflichtung zu einer derartigen Angabe datenschutzrechtlich unzulässig. Bei den Mitgliedern des Prüfungsamtes handelt es sich um medizinische Laien, sodass ihnen eine Überprüfung der Diagnose ohnehin nicht möglich ist. Nach der Rechtsprechung des Bundesverwaltungsgerichts ist es eine Rechtsfrage, ob die Voraussetzungen der Prüfungsunfähigkeit gegeben sind. Diese Frage habe die Prüfungsbehörde anhand des von ihr ermittelten Sachverhalts in eigener Verantwortung zu beantworten. Die ärztliche Verpflichtung beschränke sich hingegen im Wesentlichen darauf, krankhafte Beeinträchtigungen zu beschreiben und darzulegen, welche Auswirkungen sie auf das Leistungsvermögen des Prüflings in der konkret abzulegenden Prüfung haben.[104]

Wir empfahlen daher eine Regelung, die den Lehramtsanwärterinnen und Lehramtsanwärtern gestattet, zunächst ein Attest vorzulegen, das nur eine Beschreibung der Symptome bzw. eine Darstellung der krankheitsbedingten Beeinträchtigungen sowie Angaben zu Beginn und voraussichtlicher Dauer der Erkrankung enthält. Erweist sich dieses Attest aufgrund der Art der beschriebenen Symptome im Einzelfall als für die Subsumtion unter dem

104 Dazu auch JB 2006, 4.3.5

Rechtsbegriff „Prüfungsunfähigkeit" unzureichend, kann das Prüfungsamt ausnahmsweise in einem zweiten Schritt unter Fristsetzung die Vorlage eines substantiierten Attests mit Diagnose verlangen.

### 7.3.3 Dienst- und Vertretungspläne von Lehrkräften online

In letzter Zeit erhielten wir gehäuft Anfragen von Schulleitungen, ob es erlaubt sei, Vertretungspläne unter Nennung des konkreten Namens des Vertreters bzw. des Vertretenen ins Internet zu stellen.

Vertretungspläne enthalten personenbezogene Daten bzw. Personaldaten der als Vertretung vorgesehenen Lehrkräfte. Wir haben bereits früh[105] darauf hingewiesen, dass Personaldaten aufgrund der besonderen Gefährdung des informationellen Selbstbestimmungsrechts der Beschäftigten bei einer (weltweiten) Veröffentlichung ihrer Daten nur unter Berücksichtigung der erforderlichen Sorgfalt und Erforderlichkeit ins Internet gestellt werden dürfen. Es besteht weder eine vertragliche noch eine dienstrechtliche Duldungspflicht der Beschäftigten zur Aufnahme dieser Daten in das Internet. Die Einholung eines Einverständnisses ist in Dienst- und Arbeitsverhältnissen regelmäßig datenschutzrechtlich unzureichend, da aufgrund der bestehenden Abhängigkeit der Beschäftigten zum Dienstherrn und Arbeitgeber eine derartige Erklärung häufig nicht freiwillig ist. Die Freiwilligkeit ist jedoch Voraussetzung für ein wirksames Einverständnis.

Personaldaten von Beschäftigten unterliegen einer gesteigerten Geheimhaltungspflicht des Dienstherrn gegenüber Dritten. Nach § 2 Abs. 2 BlnDSG i. V. m. § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG ist eine Übermittlung dieser Daten nur zulässig, wenn sie für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit der oder dem Betroffenen erforderlich ist bzw. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der oder des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Sowohl

105 JB 1997, 4.7.3; JB 1998, 5.3

der Informationspflicht der Schule als auch dem Informationsbedürfnis von Eltern und Schülerinnen und Schülern ist jedoch durch eine pseudonymisierte oder anonymisierte Fassung der Vertretungspläne Genüge getan, wie sie § 5 a BlnDSG nahelegt.

Auch ist ein Passwortschutz von Internetseiten bzw. Dateien mit Personenbezug nicht ausreichend, da dieses Instrument zwar geeignet ist, die direkte Recherchierbarkeit der auf den Internetseiten veröffentlichten Daten über Suchmaschinen zu verhindern; einen wirksamen technischen Schutz personenbezogener Daten vor Weitergabe und Veröffentlichung stellt es hingegen nicht dar.

Wir haben den Schulleitungen empfohlen, bei den Vertretungsplänen im Internet auf einen Namensbezug zu den entsprechenden Lehrkräften gänzlich zu verzichten.

# 8. Kultur

## 8.1 Ehrenamtliche Tätigkeit im Bibliotheksverbund

Aus der Praxis

Uns erreichten Beschwerden darüber, dass das Bezirksamt Pankow die Kurt-Tucholsky-Bibliothek in die Trägerschaft eines privaten Vereins gegeben habe, der seinerseits die Aufgaben der Bibliothek insgesamt durch ehrenamtliche Mitarbeiterinnen und Mitarbeiter erledigen ließ. Die diesen eingeräumten Zugriffsbefugnisse auf den Rechnerverbund der öffentlichen Bibliotheken Berlins erlaubten es, im Einzelfall landesweit auf einzelne Datensätze von Bibliotheksnutzenden ohne deren Mitwirkung zuzugreifen und somit Einblick in ihr Ausleihe- bzw. Leseverhalten zu nehmen.

Wir haben in dem Bemühen, die grundsätzlich anerkennenswerte ehrenamtliche Mitarbeit zu ermöglichen, alle in Frage kommenden rechtlichen Möglichkeiten daraufhin überprüft, ob sie einen so weitgehenden landesweiten Datenzugriff legitimieren können.

Eine „Datenverarbeitung im Auftrag“ nach § 3 BlnDSG scheidet aus, weil sich die ehrenamtliche Tätigkeit auf alle, auch die allgemein beratenden Funktionen des Bibliotheksbetriebs erstreckt und nicht auf eine enge, weisungsgebundene Datenverarbeitung beschränkt ist. Die ehrenamtliche Tätigkeit ist also rechtlich nicht als Datenverarbeitung im Auftrag anzusehen, sondern als eine „Funktionsübertragung“[106] aller Bibliotheksaufgaben auf ehrenamtliche Mitarbeiterinnen und Mitarbeiter. Eine Funktionsübertragung kann, jedenfalls soweit sie hoheitliche Befugnisse einräumt, nur durch eine formelle „Beleihung“ erfolgen, die ihrerseits eines Gesetzes bedarf, in dem die Befugnisse der Beliehenen klar definiert und die Rechtsaufsicht über sie sichergestellt sind. Ohne gesetzliche Regelung konnten wir die Funktionsübertragung folglich nicht befürworten.

Die ehrenamtlich Tätigen sind auch nicht als bloße „Verwaltungshelfer“ der öffentlichen Verwaltung einzustufen. Denn als Verwaltungshilfe kommen

106 Zur Abgrenzung vgl. JB 1997, 4.8.1.

grundsätzlich nur untergeordnete Hilfsfunktionen in Betracht, die letztlich doch der umfassenden Kontrolle und Verantwortung der Verwaltung unterliegen, wie z. B. bei Schülerlotsen oder bei Abschleppdiensten, die von Polizei- oder Ordnungsbehörden mit der Umsetzung von Kraftfahrzeugen beauftragt werden.

Der Datenzugriff der ehrenamtlich Tätigen kann schließlich nicht auf das Verpflichtungsgesetz gestützt werden, denn es ist nicht dazu da, Zugriffsbefugnisse zu schaffen. Es bildet nur die Rechtsgrundlage für die Verpflichtung von Beschäftigten auf den Datenschutz. Es käme einer systemwidrigen Umkehrung des Datenschutzrechts gleich, wenn durch eine einfache Verpflichtungserklärung der Zugriff auf so umfangreiche öffentlich-rechtliche Datenbestände wie beim Rechnerverbund der bezirklichen Bibliotheken ermöglicht würde. Das Berliner Datenschutzgesetz lässt in § 8 ohnehin nur eine Verpflichtung von Dienstkräften von Behörden oder sonstigen öffentlichen Stellen bzw. von Personen zu, die bei nicht-öffentlichen Auftragnehmern öffentlicher Stellen Zugang zu personenbezogenen Daten haben. Die Kurt-Tucholsky-Bibliothek erfüllt diese Voraussetzung ebenso wenig wie die Thomas-Dehler-Bibliothek im Bezirk Tempelhof-Schöneberg, die ebenfalls ehrenamtlich betrieben wird.

Angesichts der bildungspolitischen Bedeutung der Berliner Bibliotheken haben sich sowohl die Senatskanzlei mit dem Bereich Kulturelle Angelegenheiten als auch der Unterausschuss „Datenschutz und Informationsfreiheit“ damit befasst, ehrenamtlich betriebene Bibliotheken datenschutzgerecht zu erhalten. Es wurden verschiedene Möglichkeiten diskutiert, die allerdings erhebliche Mehrkosten verursachen. Wir haben für die Übergangszeit gefordert, dass der Datenzugriff der ehrenamtlich Beschäftigten durch dienstrechtliche Aufsicht begrenzt werden muss, um missbräuchliche Datenzugriffe auszuschließen. Die im Gespräch befindlichen technischen Verbesserungen für die weitere Zukunft durch Einführung eines elektronischen Verbuchungssystems (unter Einsatz der RFID-Technik) lassen Wege als gangbar und geeignet erscheinen, die den Benutzerdatenschutz auch beim Einsatz ehrenamtlich Beschäftigter nicht gefährden. Zwischenzeitlich soll ihr Datenzugriff technisch auf den örtlichen Bezug der bezirklichen Nutzenden beschränkt werden und nur vorgenommen werden können, wenn die Nutzerin oder der Nutzer ihn autorisiert.

Wir gehen davon aus, dass es für ehrenamtliche Tätigkeiten in den öffentlichen Bibliotheken viele Möglichkeiten gibt, die datenschutzgerecht realisiert werden können und müssen. Die Umsetzung der angedachten Möglichkeiten sollte von den betroffenen Bezirken im Interesse aller Bibliotheken und Bibliotheksnutzenden zügig in Angriff genommen werden, damit der Betrieb der Bibliotheken bürgerfreundlich und datenschutzgerecht aufrechterhalten werden kann. Denn die Benutzerfreundlichkeit darf die datenschutzgerechte Gestaltung nicht ausschließen, vielmehr bedingen sich beide gegenseitig.

## 8.2 Forschung mit Friedhofsdaten

Aus der Praxis

Ein Bezirksamt legte uns die Anfrage eines unternehmerisch tätigen Anbieters von Familienforschungsdaten vor, der eine Kooperation mit dem Bezirksamt anstrebte, um Daten Verstorbener ins Internet einstellen zu können und kommerziell anzubieten. Der Anbieter bekundete seine Absicht, Daten verstorbener Berliner ab 1950 weiter rückdatierend in seinen Internetseiten darstellen zu wollen. Hierzu würden auch Kooperationsvereinbarungen mit namhaften Verlagshäusern und ähnlichen Institutionen vorliegen.

Der Persönlichkeitsschutz des Einzelnen wirkt für eine begrenzte Zeit über den Tod der Betroffenen hinaus. Die Fortdauer dieser „Schutzwirkung über den Tod hinaus“ unterliegt im Einzelfall unterschiedlichen Bewertungen. Besonders geschützte Daten, etwa im Bereich der ärztlichen Schweigepflicht, unterliegen längeren Schutzfristen als andere, nicht besonders geschützte Daten. In Anlehnung an das Mephisto-Urteil des Bundesverfassungsgerichts[107] kann jedoch im Normalfall von einer Fortwirkungsdauer von etwa 25 Jahren über den Tod hinaus ausgegangen werden, falls keine besonderen gesetzlichen Vorschriften vorliegen. Die Aufbewahrung von Daten Verstorbener auf Friedhöfen und in der Friedhofsverwaltung ist nach dem Friedhofsgesetz und der Friedhofsdatenverarbeitungsverordnung[108] zeitlich begrenzt. Nach § 6 Abs. 2 dieser Verordnung sind die Daten Verstorbener aufzubewahren, solange ein Nutzungsrecht

107 BVerfGE 30, 173 (195)

108 Verordnung über die Verarbeitung personenbezogener Daten im Bereich der landeseigenen Friedhöfe Berlins vom 16. Dezember 1993 (GVBl. S. 645)

an einer Grabstätte besteht. Danach dürfen die Daten der Verstorbenen nur noch gesondert, durch technische und organisatorische Maßnahmen gesichert, aufbewahrt werden. Sie dürfen dann nur noch genutzt werden, wenn auskunftsbegehrende Angehörige ein berechtigtes Interesse geltend machen können oder die Daten für wissenschaftliche Zwecke erforderlich sind.

Mit der Senatsverwaltung für Stadtentwicklung haben wir uns darauf verständigt, dass diese Regelung im Lichte der verfassungsrechtlichen Rechtsprechung anzuwenden ist. Dies bedeutet, dass der Schutzbedarf von Daten Verstorbener mit zunehmendem Zeitablauf abnimmt. Da bei der Schutzbedürftigkeit auf den Einzelfall und nicht auf Datenkategorien abzustellen ist, können große Datenmengen nicht ohne Weiteres pauschal aus der Schutzwirkung des über den Tod hinaus fortwirkenden informationellen Selbstbestimmungsrechts entlassen werden. Anhaltspunkte für die Einzelfallentscheidung ergeben sich insbesondere aus der archivrechtlichen Nutzungsregelung[109]. Die Regelung zur Nutzung von personenbezogenem Archivgut kann auf die Daten Verstorbener in der Friedhofsverwaltung angewendet werden. Unter das Archivgesetz fallen nicht nur Daten, die im Landesarchiv gespeichert werden, sondern auch Daten, die in dezentralen Bereichen als Archivgut der Bezirke verwaltet werden[110].

Die Senatsverwaltung für Stadtentwicklung hat den bezirklichen Friedhofsverwaltungen empfohlen, Daten Verstorbener für Forschungszwecke und zur Erteilung von Auskünften grundsätzlich bereitzuhalten. Nach einer Schutzfrist von zehn Jahren nach dem Tod dürfen aus diesem Datenbestand grundsätzlich Einzelauskünfte über Verstorbene erteilt werden. Vor Ablauf dieser Schutzfrist dürfen Auskünfte erteilt werden, wenn die Nutzungsberechtigten zugestimmt haben oder die Daten auf dem Grabstein öffentlich zugänglich sind. Auskünfte können dann versagt werden, wenn schutzwürdige Belange Dritter erkennbar entgegenstehen oder ein nicht vertretbarer Verwaltungsaufwand entstünde. Sammelanfragen müssen nicht beantwortet werden. Es war aus unserer Sicht nicht nötig, über die Verpflichtung zur Abgabe der Daten an Anbieter von Familienforschung insgesamt zu entscheiden. Denn unsere Aufgabe beschränkt sich allein auf die datenschutzrechtliche Fragestellung, eine Befugnis zur Datenweitergabe.

109 § 8 Abs. 3 Archivgesetz von Berlin – ArchGB
110 § 1 Abs. 3, § 10 ArchGB

Die Senatsverwaltung für Stadtentwicklung hat entsprechend unserem Rat die Verordnung zur Verarbeitung von Friedhofsdaten so interpretiert und zur Anwendung empfohlen, dass sowohl die Rechte der Verstorbenen als auch der Familienforscher gewahrt werden.

## 8.3 Euthanasie-Gedenkbuch



Im Rahmen eines mit öffentlichen Geldern geförderten Forschungsprojekts hat die Stiftung Brandenburgische Gedenkstätten eine Datenbank über Berliner Psychiatriepatienten aufgebaut, die die 1940 in der „Euthanasie-Anstalt" Brandenburg/Havel ermordeten Menschen enthält. Bei diesem Projekt waren die Daten von Verstorbenen in der Friedhofsverwaltung zwar nicht unmittelbar relevant, aber zur Klärung von Einzelfällen waren auch diese Daten eine nicht unwesentliche Forschungsquelle. Vornehmlich mussten die Daten jedoch aus Krankenunterlagen, Patientenakten, Aufnahme- und Abgangsbüchern der psychiatrischen Anstalten ausgewertet und erforscht werden. Am Ende sollte eine Publikation als Gedenkbuch erscheinen, um die Dimension der Verbrechen im „Gedenkbuch für die in Brandenburg/Havel ermordeten Euthanasie-Opfer aus Berlin" greifbar zu machen.[111] In alphabetischer Reihenfolge sollten die Namen (Nachname, Vorname) aller ermittelten Opfer und deren Geburts- und Sterbejahre aufgelistet werden. Anliegen des Projekts war es, mit der Namensnennung die Würde der Opfer wiederherzustellen, sie wieder zu personalisieren und in der Erinnerung der Nachwelt zu verankern.

Informationen über die Morde an den Patientinnen und Patienten unterlagen zu keinem Zeitpunkt der ärztlichen Schweigepflicht, da die ärztliche Schweigepflicht die Kranken schützen, nicht aber die Geheimhaltung von Straftaten ermöglichen soll. Gleichwohl war zu bedenken, dass die Euthanasie-Akten Patientenakten waren, die der ärztlichen Schweigepflicht unterlagen, aber mit dem Mordgeschehen unmittelbar verbunden waren. Bedenken gegen die wissenschaftliche Verwertung, Auswertung und angemessene Publikation

111 Das Gedenkbuch ist am 13. Januar 2010 dem Staatssekretär für Kulturelle Angelegenheiten in der Senatskanzlei übergeben worden.

(reduziert auf Namen und Lebensdaten) bestanden trotz des Arztgeheimnisses jedoch nicht, weil auch das Arztgeheimnis – als Teil des allgemeinen Persönlichkeitsrechts der Patientinnen und Patienten – nicht für immer über den Tod hinaus andauert. Im Fall der Euthanasie konnte nach einem Zeitraum von über 70 Jahren seit Begehung dieser Verbrechen die Einsicht in die Patientenakten für wissenschaftliche Zwecke, insbesondere für die hier bezeichnete historische Forschung, generell als rechtlich zulässig erachtet werden. Die Sichtung der Akten diente – über das Gedenken hinaus – auch der Erforschung und Nennung der Namen der Ermordeten und damit dem wissenschaftlichen Nachweis für die Verbrechen des Dritten Reichs. Insofern war hinsichtlich der Veröffentlichung dieser Daten im Interesse der historischen Forschung generell von dem Ende der Schutzwirkung für die Patientendaten auszugehen.

Allerdings haben wir empfohlen, der ursprünglichen Sensitivität der Daten gleichwohl Rechnung zu tragen. Denn ungeachtet der Wirkung des individuellen Persönlichkeitsschutzes über den Tod hinaus verdienen die Opfer dieser Verbrechen Respekt auch da, wo Rechtsansprüche nicht mehr bestehen. Deshalb haben wir den Verzicht auf die Angabe von Diagnosen begrüßt. Da auch heute noch der Begriff der „Geisteskrankheit", der mit den Euthanasieverbrechen untrennbar verknüpft ist, allzu oft abfällig gebraucht und möglicherweise von den noch lebenden Hinterbliebenen als belastend empfunden wird, sollte hinsichtlich der Euthanasie immer wieder klargestellt werden, dass es nicht um Bewertungen individueller Krankheitsbilder ging, sondern dass pauschal ein staatliches Tötungsprogramm in Gang gesetzt worden war.

Bei der Erstellung von Gedenkbüchern über Opfer nationalsozialistischer Gewaltverbrechen ist zwischen dem historischen Interesse und dem Respekt vor den Opfern ein angemessener Ausgleich zu finden.

# 9. Wissen und Bildung

## 9.1 Schule

### 9.1.1 Meldung von Schüler-Fehlzeiten an die Jobcenter

Aus der Praxis

Ein Oberstufenzentrum (OSZ) übersandte regelmäßig Listen mit den Fehlzeiten von Schülerinnen und Schülern als Serienbrief an alle Jobcenter. In den Listen waren zu den Betroffenen die Namen, Anschriften, Geburtsdatum, Träger und eine Auflistung der versäumten Tage oder Stunden sowie Verspätungen angegeben. In einem Begleitschreiben der Schulleitung wurde mitgeteilt, dass nur die Auszubildenden in einer Trägerausbildung in die Auflistung einbezogen worden wären, bei denen auch wegen der hohen Fehlzeiten ein erfolgreicher Schulabschluss stark gefährdet sei. Es sei daher unerklärlich, warum die Förderung in diesen Fällen überhaupt fortgesetzt werde.

Dass viele Teilnehmende an der überbetrieblichen Schulausbildung Probleme mit der Pünktlichkeit, Zuverlässigkeit und der Schulmotivation haben, ist bekannt. Auch ist offensichtlich, dass sich dieser Umstand erschwerend auf die Arbeit mit den Jugendlichen und negativ auf deren schulischen Erfolge auswirkt. Insofern ist das Anliegen der Schulleitung, dagegen etwas zu unternehmen, verständlich. Allerdings sind die Agentur für Arbeit bzw. die Jobcenter hier die falschen Ansprechpartner. Zuständig ist vielmehr der jeweilige (private) Bildungsträger, mit dem die oder der Jugendliche den Ausbildungsvertrag geschlossen hat. Dieser ist den Schulen auch in jedem Einzelfall bekannt. Die Schule darf diesen privaten Bildungsträgern personenbezogene Daten der Schülerinnen und Schüler übermitteln, soweit dies im Rahmen der dualen Ausbildung, insbesondere zur Gewährleistung des Ausbildungserfolges, erforderlich ist[112]. Häufige Fehlzeiten in der Schule gefährden ohne Zweifel den Ausbildungserfolg. Ihnen ist durch gezielte und wirkungsvolle pädagogische Maßnahmen zu begegnen. Diese sind dann erfolgreich, wenn sie mit den

112 § 64 Abs. 5 SchulG

jeweiligen Ausbildungsbetrieben abgestimmt werden. Dazu ist die Übermittlung der Fehlzeiten an die Bildungsträger erforderlich und zulässig. Eine Übermittlung dieser personenbezogenen Daten an die unzuständigen Jobcenter ist dagegen unzulässig.

Die Senatsverwaltung für Bildung, Wissenschaft und Forschung hat das OSZ – unserer Empfehlung folgend – angewiesen, in Zukunft nur trägerspezifische Listen zu erstellen und an die direkten Ansprechpartner in den Bildungsträgern zu versenden.

Auch wenn das Anliegen, Fehlzeiten entgegenzuwirken, verständlich ist, sind die datenschutzrechtlichen Bestimmungen einzuhalten. Dies führt oft zum gleichen Erfolg.

## 9.1.2 Fragebogen im Betriebspraktikum

Im Rahmen der zweijährigen Bildungsgänge an einer Fachoberschule haben die Schülerinnen und Schüler ein Praktikum zu absolvieren. Die Praktika werden in der Regel in Betrieben, Behörden und sonstigen außerschulischen Einrichtungen durchgeführt. Ungeachtet dessen handelt es sich um eine schulische Veranstaltung, für deren Ausgestaltung und Durchführung die Fachoberschule die Verantwortung trägt. Am Ende des Praktikums hat die Praxisstelle über die Teilnehmerinnen und Teilnehmer eine schriftliche Beurteilung abzugeben. Dazu wurde von einer Fachoberschule ein Fragebogen zur „Praxisbeurteilung“ entwickelt. Ein Unternehmen, das Zweifel an der Zulässigkeit der umfangreichen Datenerhebung hatte, bat uns, den Erhebungsbogen zu überprüfen.

Für die Bewertung der Datenerhebung ist § 64 Abs. 1 SchulG heranzuziehen. Die Erhebung der Schülerdaten ist danach nur zulässig, wenn sie für die Erfüllung der schulbezogenen Aufgaben erforderlich ist. Neben den Angaben zur Person, wie Name, Vorname, Geburtsdatum, wurden auch Daten zum Verhalten der Praktikantin oder des Praktikanten erhoben. Unter anderem wurde gefragt, ob sie oder er sich in der Lage zeigte, materielle und psychische Notlagen zu erkennen, wie ihr oder sein Umgang mit persönlichen oder fremden Grenzsituationen war und wie sie oder er mit eigenen Gefühlen umgegan-

gen ist. Bei der Frage zu den materiellen und psychischen Notlagen bestehen erhebliche Zweifel an der Erforderlichkeit. Diese könnte allenfalls im Fachbereich Sozialwesen – und dort nur unter sehr engen Voraussetzungen – gegeben sein. Der Umgang mit persönlichen Grenzsituationen unterliegt dagegen dem absoluten Kernbereich der Persönlichkeit, also der Intimsphäre der Praktikantin bzw. des Praktikanten. Eine Erhebung derartiger verhaltensbezogener Daten ist für die Praktikumsbeurteilung in keinem Fall erforderlich und damit unzulässig. Soweit der Umgang mit fremden Grenzsituationen abgefragt wird, ist eine Erforderlichkeit der Datenerhebung wiederum allenfalls im Fachbereich Sozialwesen – und nur unter engen Voraussetzungen – gegeben. Der Umgang der Praktikantin oder des Praktikanten mit eigenen Gefühlen unterliegt ebenfalls dem absolut geschützten Kernbereich der Persönlichkeit. Auch solche Fragen sind grundsätzlich unzulässig.

Die Senatsverwaltung für Bildung, Wissenschaft und Forschung hat die Fachoberschule angewiesen, diese Fragestellungen zukünftig zu unterlassen und ggf. durch andere Fragestellungen zu ersetzen, die ausgerichtet auf das Bildungsziel der jeweiligen Fachrichtung eine geringere Eingriffsintensität aufweisen.

Auch bei der Erhebung von Daten im Rahmen der Beurteilung eines Praktikanten gilt der Erforderlichkeitsgrundsatz. Insbesondere ist der Kernbereich der Persönlichkeit zu achten.

### 9.1.3 Die neugierige Schule – Verwendungszweck von Schulbescheinigungen

Ein aufgebrachter Vater beschwerte sich darüber, dass die Schule seines Sohnes die erbetene (allgemeine) Schulbescheinigung nur unter der Voraussetzung ausstellen würde, dass zuvor der Verwendungszweck angegeben wird. Dieser sei auf Anweisung der Schulleitung schriftlich im Sekretariat festzuhalten. Die Schulleitung bestätigte das Verfahren und gab als Begründung für die Erhebung und Speicherung des Verwendungszwecks die „Vermeidung des Missbrauchs von Schulbescheinigungen“ gegenüber Dritten an.

Eine Schule darf nur die personenbezogenen Daten von Schülerinnen und Schülern sowie deren Erziehungsberechtigten verarbeiten, die zur Erfüllung

von schulbezogenen Aufgaben erforderlich sind[113]. Eine Schulbescheinigung dient (ähnlich wie der Schülerausweis) als Nachweis für den Schulbesuch einer bestimmten Person zum Zeitpunkt der Ausstellung. Für die Ausstellung einer solchen Bescheinigung ist es erforderlich, die Personendaten (Namen, Vornamen, Schuljahr und die besuchte Klasse) der Schülerin oder des Schülers schulintern zu verarbeiten. Zur Dokumentation des (schulbezogenen) Handelns ist es ausreichend, den Namen der oder des Betroffenen und das Datum der Ausstellung zu erfassen. Dagegen stehen die Erhebung und Speicherung des Verwendungszwecks einer Schulbescheinigung in keinem erkennbaren Zusammenhang mit schulbezogenen Aufgaben. Bei der „Vermeidung des Missbrauchs von Schulbescheinigungen" gegenüber Dritten handelt es sich – unabhängig von der Frage der Geeignetheit – jedenfalls nicht um eine schulbezogene Aufgabe. Schulbescheinigungen werden in der Regel im außerschulischen Bereich (z. B. zur Beantragung von Sozialleistungen, Aufnahme in ein Sportstudio, in Bewerbungsverfahren) genutzt. Zu welchem Zweck der Schulnachweis tatsächlich genutzt wird, geht die Schule nichts an. Die Verarbeitung derartiger Angaben ist für ihre Aufgabenerfüllung nicht erforderlich und damit unzulässig.

Die Schulleitung hat zugesagt, zukünftig auf die Erhebung und Speicherung des Verwendungszecks bei der Ausstellung einer Schulbescheinigung zu verzichten.

Eine Schule muss nicht alles wissen.

### 9.1.4 Was wäre die Schule ohne Hausaufgaben?

Uns wurde ein Fragebogen vorgelegt, mit dem eine Grundschule die Eltern der Schülerinnen und Schüler der Klassenstufe 5/6 zum Thema Erledigung der „Hausaufgaben" befragt hatte. Die Eltern empörten sich darüber, dass in dem Fragebogen auch Angaben über sehr persönliche und familiäre Verhältnisse gemacht werden sollten (z. B.: Erzwingt das Kind Ihre Hilfe mit Weinen, Schreien, Betteln? Wird das Kind bei den Hausaufgaben geschlagen? Wird das Kind für sein Verhalten bei den Hausaufgaben bestraft?).

113 § 64 Abs. 1 SchulG

Die Schulleitung erklärte uns, dass die Schule in einen partiellen gebundenen Ganztagsbetrieb umgewandelt worden sei. In diesem Zusammenhang habe sich die Frage des Umgangs mit den „Hausaufgaben" gestellt. Angesichts der Ganztagsbetreuung in der Schule seien diese zur Belastung für die Schülerinnen und Schüler und die Elternhäuser geworden. Viele Eltern hätten sich darüber beklagt, dass die Kinder im häuslichen Bereich noch zu Schularbeiten gezwungen würden. Demgegenüber gäbe es aber auch einen großen Teil von Eltern, die Hausaufgaben als Vorbereitung auf die Anforderungen der Oberschulen begrüßen würden. Teilweise ergäben sich sogar Schnittmengen von Eltern aus beiden Gruppen, die das eine beklagen und dennoch das andere anstreben würden. Ähnlich ambivalent seien die Haltungen der Lehrkräfte und der Schülerinnen und Schüler. Der Zweck der Fragebogenaktion sei gewesen, einen Einblick in die häusliche Belastungssituation zu erhalten, um zu einer Einschätzung über die Notwendigkeit zu kommen, die Elternhäuser in Bezug auf Hausarbeiten zu entlasten. Es habe sich um eine absolut freiwillige und anonyme Befragung der Eltern gehandelt. Der Fragebogen sei im Wesentlichen der wissenschaftlichen Standardliteratur entlehnt. Die besonders kritisierten Fragen sollten dabei helfen, die Beeinträchtigung des Hausfriedens, der immer wieder von den Eltern als gestört dargestellt werden würde, einschätzen zu können. Der Rücklauf der Fragebögen sei weder von den Klassenleitungen noch der Schulleitung kontrolliert worden. In den Klassen seien die Bögen in Urnen (Kartons) und im Sekretariat in einem Sammelkasten aufbewahrt worden. Die Auswertung sei ohne vorherige Durchsicht von einer schulfremden Fachkraft erfolgt.

In der Sache selbst konnte kein datenschutzrechtlicher Mangel festgestellt werden. Wir haben der Schulleitung jedoch empfohlen, die Eltern im Vorfeld zukünftiger Befragungen in einem Schreiben über das Verfahren der anonymisierten Datenerhebung, des Rücklaufs der Unterlagen und deren Auswertung umfassend zu informieren.

**Anonyme Befragungen sind grundsätzlich datenschutzrechtlich unproblematisch. Eine umfassende Aufklärung der Befragten ist jedoch unerlässlich.**

## 9.1.5 Es wird gegessen, was auf den Tisch kommt!

Ein bezirkliches Schulamt hatte die Schulaufsichtsbehörde (Senatsverwaltung für Bildung, Wissenschaft und Forschung) darum gebeten, den Schulleiter einer Grundschule anzuweisen, eine Liste mit allen Personensorgeberechtigten der Schule an das Schulamt zu übermitteln. Hintergrund der Bitte war die streitbehaftete Vergabe des Essens-Catering-Vertrages für die Grundschule. Nach zwei erfolglosen Probeessen einer Essenskommission, bei denen sich die Beteiligten nicht auf einen Anbieter verständigen konnten, wurde vom Kammergericht empfohlen, eine dritte „Blindverkostung" durchzuführen. Da die bisher handelnde Essenskommission nach Auffassung des Gerichts „emotional verhärtet ist", sollten neue Mitglieder ausgewählt werden, „die nicht in erkennbarem Maße voreingenommen sind". Um freiwillige Probeesserinnen und -esser zu finden, wollte das Schulamt alle Personensorgeberechtigten der Schule mit einem Informationsbrief über den normalen Postweg anschreiben. Von der Schulaufsicht wurden wir gebeten zu prüfen, ob hierfür die Namen und Adressen der Betroffenen von der Schule an das Schulamt übermittelt werden dürfen.

Bei den Namen und Anschriften der Personensorgeberechtigten handelt es sich um personenbezogene Daten, die dem Datenschutz unterliegen. Die Schule darf sie nach § 64 Abs. 3 SchulG an das bezirkliche Schulamt übermitteln, soweit dies zur rechtmäßigen Erfüllung der gesetzlichen („schulbezogenen"[114]) Aufgaben der Schule oder des Schulamtes erforderlich ist. Bei der Auswahl von freiwilligen Eltern, die an einem Probeessen für die Auswahl einer Catering-Firma teilnehmen sollen, handelt es sich erkennbar nicht um eine schulbezogene Aufgabe der Schule bzw. des Schulamtes. Unabhängig davon ist es zur Durchführung des Vorhabens auch nicht erforderlich, dass dem Schulamt von der Schule eine Liste mit allen Namen und Anschriften der Personensorgeberechtigten übermittelt wird. In vergleichbaren Fällen ist es üblich, Informationsschreiben in der Schule (z. B. durch die Klassenleitung) an die Schülerinnen und Schüler zur Weitergabe an die Personensorgeberechtigten austeilen zu lassen. Eine entsprechende Weisung der Schulaufsicht an den Schulleiter, im vorliegenden Fall ebenso zu verfahren, ist möglich. Der Empfang des Schreibens

114 § 64 Abs. 1 SchulG

kann (wie ebenfalls üblich) von den Erziehungsberechtigten gegenüber der Klassenleitung bestätigt werden.

Wir haben der Schulaufsicht mitgeteilt, dass die Übermittlung von Daten der Schülerinnen und Schüler oder deren Erziehungsberechtigten an das Schulamt zur Information über das Vergabeverfahren und Durchführung des Probeessens nicht erforderlich und damit unzulässig ist.

Auch wenn alle Beteiligten davon ausgehen, bei der Datenübermittlung an das Schulamt für einen guten Zweck zu handeln, dürfen datenschutzrechtliche Bestimmungen nicht umgangen werden.

## 9.2 Lernunterstützungssystem Blackboard

Seit einiger Zeit werden an Berliner Hochschulen Lernunterstützungs- bzw. Lernmanagementsysteme wie das LMS Blackboard eingesetzt. Diese Systeme ermöglichen die Bereitstellung von Lehrmaterialien für die Teilnehmerinnen und Teilnehmer einer Lehrveranstaltung, oft aber auch die Kommunikation zwischen der oder dem Lehrenden und den Studierenden bzw. den Studierenden untereinander – beispielsweise innerhalb von Projekt- oder Lerngruppen. Datenschutzrelevant ist der Einsatz derartiger Systeme, da die Nutzenden sich zur Teilnahme bei diesen Plattformen unter Angabe personenbezogener Daten anmelden müssen und auch bei der Nutzung personenbezogene Daten (wie Profildaten und gesendete Nachrichten) anfallen. Das LMS Blackboard bietet als zusätzliche Funktion die Erstellung und Absolvierung von Online-Tests an, deren Ergebnisse u. U. sensitive personenbezogene Daten sind. Allerdings werden diese Tests bisher als reine Selbsttests (d. h. ohne Prüfungsrelevanz) eingesetzt.

Wir haben den Einsatz des LMS Blackboard an der Freien Universität Berlin (FUB) geprüft. Der technische Betrieb erfolgt unter den für Webangebote nötigen Sicherheitsmaßnahmen: Nutzende erhalten Zugang zum LMS über SSL-verschlüsselte Verbindungen; die Server werden physisch ausreichend gesichert im Rechenzentrum der FUB betrieben; bei der Anmeldung werden nur die notwendigen Daten erhoben, und die Voreinstellungen zur Privatsphäre sind

restriktiv gewählt. So existiert zwar die Möglichkeit, ein eigenes Nutzerprofil innerhalb des Systems zu veröffentlichen und in einem globalen Verzeichnis gelistet zu werden. Diese Optionen sind jedoch standardmäßig abgeschaltet.

Datenschutzrechtlich basiert der Einsatz des Systems an der FUB bisher auf der Einwilligung der Nutzenden. Eine solche Einwilligungslösung setzt voraus, dass es den Studierenden möglich ist, jede angebotene Lehrveranstaltung auch ohne die Nutzung des LMS diskriminierungsfrei zu besuchen. Dies ist aufgrund des Funktionsumfanges des Systems zumindest fraglich – allein schon der Zugang zu Lehrmaterialien, die üblicherweise innerhalb des LMS angeboten werden, wird sich „offline" als schwierig herausstellen. Die Offline-Durchführung von Online-Tests dürfte unmöglich sein. Da eine andere Rechtsgrundlage nicht ersichtlich ist, haben wir die FUB aufgefordert, eine Satzung nach § 6 Abs. 1 Ziffer 6 Berliner Hochschulgesetz (BerlHG) für den Einsatz von Lernunterstützungssystemen zu schaffen. Das Gleiche gilt für die Charité, weil sie plant, das LMS der FUB mit zu nutzen. Zudem muss die Charité die FUB nach § 6 Abs. 2 BerlHG mit der Verarbeitung der Daten der Studierenden der Charité beauftragen.

Die Datenverarbeitung bei der Nutzung von IT-Verfahren zur Unterstützung der Lehre an Hochschulen kann nicht mit der Einwilligung zur Verarbeitung von Studierendendaten gerechtfertigt werden, wenn diese Nutzung faktisch für die erfolgreiche Durchführung eines Studiums erforderlich ist.

# 10. Wirtschaft

## 10.1 Die Deutsche Bahn AG stellt Weichen für besseren Arbeitnehmerdatenschutz

Unternehmen überwachen ihre Beschäftigten weitaus umfangreicher und massiver als gemeinhin angenommen und als es datenschutzrechtlich zulässig ist.

Aus der Praxis

Gegenstand des Bußgeldverfahrens gegen die Deutsche Bahn AG war u. a. die unrechtmäßige Speicherung der Ergebnisse anlassloser heimlicher Screenings von 2002 bis 2005, bei denen Daten von einer Vielzahl von Beschäftigten und deren Angehörigen mit Daten von Lieferanten abgeglichen wurden.

Bei anderen einzelnen Revisionsfällen, die wir im Bußgeldbescheid berücksichtigt haben, durchleuchtete das Unternehmen die verdächtigen Mitarbeiterinnen und Mitarbeiter vollständig: So wurden die Festplatten und die im Netz gespeicherten Dateien am Arbeitsplatz kopiert und die Büros durchsucht, der Lebensstil wurde durch ein privates Ermittlungsbüro überprüft, private Geld- und Kontobewegungen aufgelistet sowie die Reisetätigkeit und Familienverhältnisse festgehalten. Die dazugehörigen Ermittlungsberichte und die darin enthaltenen personenbezogenen Daten hob die Deutsche Bahn AG jahrelang auf - auch nachdem der Korruptionsverdacht sich nicht bestätigte. Das Grundrecht auf informationelle Selbstbestimmung schützt aber auch vor einer solchen latenten Dauerverdächtigung. Eine unbegrenzte Speicherung von personenbezogenen Daten ist nicht zulässig.

Ferner nahm die Deutsche Bahn AG eine systematische Überwachung der E-Mails von Beschäftigten und deren Kontakten vor, um herauszufinden, von wem Informationen z. B. bei kritischen Presseberichten aus dem Unternehmen weitergegeben worden waren. Insbesondere Kontakte mit Journalistinnen und Journalisten und Beschäftigten von Bundestagsabgeordneten, aber auch mit Kritikern wurden überwacht.

In dem gegen die Deutsche Bahn AG erlassenen Bußgeldbescheid haben wir über diese und weitere datenschutzrechtliche Gesetzesverletzungen entschie-

den und jeweils gesonderte Geldbußen festgesetzt. In der Summe ergab sich damit ein Gesamtbetrag von rund 1,12 Millionen Euro. Dies ist das höchste Bußgeld, das eine einzelne deutsche Datenschutzaufsichtsbehörde bisher gegen ein Unternehmen festgesetzt hat. Die Deutsche Bahn AG hat den Bußgeldbescheid akzeptiert und das Bußgeld gezahlt.

Das Bußgeldverfahren hat auch dazu geführt, dass die Deutsche Bahn AG technische und organisatorische Maßnahmen als Vorkehrung gegen datenschutzrechtliche Verstöße im Unternehmen eingeleitet hat. Der neue Unternehmensvorstand hat den Datenschutz zu einer seiner obersten Prioritäten erklärt. Datenschutz wurde auf höchster Managementebene in einem eigenen Vorstandsressort „Compliance, Datenschutz und Recht“ angesiedelt. Die Zahl der Mitarbeiterinnen und Mitarbeiter im Bereich Datenschutz soll auf 25 erhöht werden.

Die Deutsche Bahn AG hat sich zum Ziel gesetzt, beim Datenschutz insbesondere für Beschäftigte künftig positive Maßstäbe zu setzen. Wir werden sie hierbei nach Kräften unterstützen.

## 10.2 Datenschutzprobleme von Bahnkunden

**Bahnkunde wider Willen**

Ein Kunde der Deutschen Bahn AG hatte sich darüber beschwert, dass seine Daten für vier weitere Jahre nach Ablauf seines BahnCard-Vertrags gespeichert werden. Die Deutsche Bahn verwies auf die entsprechenden Hinweise zum Datenschutz. Dort sei klargestellt, dass eine Datenspeicherung über das Vertragsende hinaus zur Kundenbetreuung erfolgen würde. Während der Vertragsdauer erfolge die Datenverarbeitung bzw. -nutzung für die Vertragsabwicklung. Erst nach Kündigung des Vertragsverhältnisses setze die Kundenbetreuung (z. B. zur Rückgewinnung) ein. Insoweit läge eine zulässige Zweckänderung der Datenverarbeitung vor. Die weitere Speicherung des Geburtsdatums sei erforderlich, da viele Bürgerinnen und Bürger den Wohnort häufig wechseln und nur das Geburtsdatum eine Adressermittlung über die Einwohnermeldestelle und damit die Kontaktierung mit dem Ex-Kunden gewährleisten würde.

Dem ist zu entgegnen, dass während der Vertragsdauer sowohl Maßnahmen zur Vertragsabwicklung als auch zur Kundenbetreuung stattfinden. Nach Beendigung des Vertragsverhältnisses kann dagegen keine Kundenbetreuung im eigentlichen Sinne mehr stattfinden. Eine Betreuung darf daher ohne Kenntnis der oder des Betroffenen nicht mehr erfolgen, allenfalls können Bemühungen der Deutschen Bahn AG zur Rückgewinnung als Kunden einsetzen. Nach Ablauf eines Jahres nach Vertragsende (zu Clearingzwecken) kann die Kundin oder der Kunde davon ausgehen, dass die zur Person gespeicherten Daten vom Unternehmen gelöscht werden. Will das Unternehmen die in § 28 Abs. 3 BDSG genannten Daten der Kundschaft zu Werbe- oder Rückgewinnungszwecken nutzen, so hat sie ein Widerspruchsrecht. Dies gilt erst recht für Daten, die über den in § 28 Abs. 3 BDSG genannten Datenkatalog hinausgehen. Daher ist die Kundin oder der Kunde erneut darüber in Kenntnis zu setzen, dass seine Vertragsdaten (Gültigkeitstermin, Klasse, BahnCard-Art sowie das Geburtsdatum) weiterhin für Werbezwecke gespeichert werden sollen. Hierbei ist explizit auf das Widerspruchsrecht hinzuweisen.

Eine Verarbeitung von Kundendaten nach Ende der Vertragsbeziehung zu Werbezwecken ist unzulässig, wenn die Kundinnen und Kunden nicht auf ihr Widerspruchsrecht hingewiesen werden.

### Online-Tickets und Vorlage der Kreditkarte im Zug

Ein Kunde der Deutschen Bahn AG hatte uns darauf hingewiesen, dass der Fahrgast bei einer Online-Ticket-Buchung zu seiner Legitimation neben dem ausgedruckten Ticket eine gültige BahnCard oder eine EC- bzw. Kreditkarte bei der Kontrolle im Zug vorlegen müsse. Das Unternehmen teilte dazu mit, bei der Fahrkartenkontrolle müsse geprüft werden, ob das ausgedruckte Ticket nur einmal verwendet wird. Dies werde über die Vorlage der gültigen Kreditkarte, EC-Karte oder (falls vorhanden) einer BahnCard gewährleistet, die der Kunde bei der Buchung als Identifikationsmittel angegeben hat. Beim Auslesen des Tickets mit dem mobilen Terminal und der Legitimationskarte werde die Übereinstimmung geprüft. Maßgeblich sei nicht, mit welcher Kreditkarte die Zahlung erfolge, sondern die hinterlegte ID-Kartennummer des angemeldeten Kunden. Prozesstechnisch sei dies so festgelegt, da das Online-Ticket eine personalisierte Fahrkarte darstelle.

Diese Vorgehensweise stieß auf datenschutzrechtliche Bedenken. Die Vorlage der EC- oder Kreditkarte dient weder der Zweckbestimmung des Vertragsverhältnisses noch war sie zur Wahrung der berechtigten Interessen der Deutschen Bahn AG erforderlich. Bezahlt werden muss das Online-Ticket (mit EC-, Kreditkarte oder im Lastschriftverfahren) ohnehin, bevor es ausgedruckt werden kann. Es gibt aber keinen Grund, den Bahnkunden ohne BahnCard zu zwingen, sich im Zug mit einer EC- oder Kreditkarte auszuweisen. Die Voraussetzungen einer zulässigen Datenverarbeitung nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG waren deshalb nicht gegeben.

Wir haben der Deutschen Bahn AG mitgeteilt, dass wir die Vorlage der gültigen Kredit- oder EC-Karte (falls der Kunde keine BahnCard besitzt) nicht für erforderlich halten, und darum gebeten, auch die Personalausweisnummer als Identifikationsmittel zu akzeptieren. Diesen Vorschlag hat die Deutsche Bahn aufgenommen; sie plant, kurzfristig auch die Nutzung des Personalausweises zu ermöglichen.

## 10.3 Datenübermittlung an Finanzdienstleister

Die Kundinnen und Kunden einer Berliner Bank erhielten auf einem Kontoauszug die Information, dass die Bank mit ihrem IT-Dienstleister eine Servicegesellschaft gegründet habe. Diese werde zukünftig bestimmte Dienstleistungen – insbesondere die Konto- und Depotverwaltung und Kreditsachbearbeitung – aus dem sog. Back Office Center der Bank erbringen. Ziel der Auslagerung war es, Kosten zu sparen, da die Beschäftigten der Servicegesellschaft nicht mehr unter den Bankentarif fallen. Außerdem sollte die Servicegesellschaft versuchen, weitere Banken als Kunden für ihre Dienstleistung zu gewinnen. Die Bank hat dem Servicecenter alle Kundendaten zugeleitet, soweit diese für die Arbeit des Servicecenters erforderlich sind.



Da es im Bundesdatenschutzgesetz kein Konzern- bzw. Verbundprivileg gibt, ist der Datenfluss zwischen der Bank und dem Servicecenter mangels einer Einwilligung der Betroffenen nur dann rechtmäßig, wenn eine Rechtsvorschrift

diesen erlaubt[115]. Auch wenn die Bank ein berechtigtes Interesse an der Verbesserung der Kostenstruktur hat, ist die Datenübermittlung an die Servicegesellschaft rechtswidrig, da die Bankkundinnen und -kunden ein überwiegendes Interesse an dem Ausschluss der Verarbeitung haben[116]. Eine Bankkundin oder ein Bankkunde muss darauf vertrauen können, dass die Bank interne Vorgänge selbst bearbeitet und diese nicht durch Dritte erledigen lässt, zu dem sie oder er keine vertragliche Beziehung hat. Bei datenschutzrechtlichen Verstößen der Servicegesellschaft könnte sich die Bank als Vertragspartnerin unter Verweis auf die neue verantwortliche Stelle exkulpieren. Da die Servicegesellschaft noch weitere Banken als Kundinnen gewinnen wollte, bestände außerdem die Gefahr, dass der Dienstleister etwa eine Bank darüber informiert, dass eine andere Bank die Bonität der Kundin oder des Kunden aufgrund anderer Erkenntnisse anders bewertet.

Die Information lediglich auf einem Kontoauszug führte dazu, dass Kundinnen und Kunden, die sich nur unregelmäßig Kontoauszüge beschaffen, erst im Nachhinein über die geplante Umstrukturierung informiert wurden. Die Information selbst war auch nicht ausreichend, um sie über die geplanten Datenübermittlungen an die Gesellschaft in Kenntnis zu setzen. Da die allgemeinen Geschäftsbedingungen der Bank nicht geändert wurden, wurde den Kundinnen und Kunden auch kein Widerspruchsrecht eingeräumt.

Aufgrund unserer Intervention hat die Bank das Verfahren gestoppt. Die Bank selbst bleibt Herrin aller Kundendaten, das Servicecenter darf nur als Auftragsdatenverarbeiter unter den strengen Vorgaben des § 11 BDSG für die Bank Daten verarbeiten.

Vor der Teilung eines Unternehmens oder einer Verlagerung von Funktionen auf Servicegesellschaften ist zu berücksichtigen, dass bisher mögliche Datenflüsse aufgrund des fehlenden Konzern- bzw. Verbundprivilegs rechtswidrig werden können.

115 § 4 Abs. 1 BDSG
116 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

## 10.4 Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)



Das HIS der Versicherungswirtschaft wird in den Sparten Leben, Unfall, Kraftfahrt, Rechtsschutz, Sachversicherungen, Transport und Haftpflicht geführt. Jeder Teil soll die Versicherungsbranche nicht nur vor Versicherungsbetrügern bei Vertragsabschluss und Schadensregulierung warnen, sondern auch vor Versicherungsnehmern, bei denen ein erhöhtes Risiko besteht, dass ein Versicherungsfall eintritt. Lange Zeit wurde die Warndatei der Versicherungswirtschaft als „Blackbox" geführt[117]. Betroffene erhielten keine Informationen über den Inhalt des Warnsystems.

Die langjährigen Verhandlungen der Aufsichtsbehörden mit der Versicherungswirtschaft haben zu ersten Erfolgen geführt. Seit April werden Versicherungskundinnen und -kunden, die in das HIS eingemeldet werden, von ihrer Versicherung benachrichtigt. Außerdem besteht die Möglichkeit, beim Gesamtverband der Deutschen Versicherungswirtschaft, dem in Berlin ansässigen Betreiber der HIS-Datei, Auskunft über die zur Person gespeicherten Daten zu fordern. Durch die nun gewährte Transparenz besteht auch die Möglichkeit, Löschungs- oder Berichtigungsansprüche durchzusetzen. Verbesserungen konnten auch für die Rechtschutzkundinnen und -kunden erreicht werden. Diese werden zukünftig erst ab vier Streitfällen binnen zwölf Monaten (bisher zwei) eingemeldet.

In den nächsten zwei Jahren wird die Versicherungswirtschaft das HIS nach den Vorgaben der Aufsichtsbehörden auf eine datenschutzrechtlich sichere Grundlage stellen. Hier die wichtigsten Eckpunkte:

- Das HIS wird als Auskunftei geführt.
- Die Einmeldung in die Auskunftei erfolgt nur bei Vorliegen einer Rechtsvorschrift (Interessen der Versicherungswirtschaft sind höher zu bewerten als schutzwürdige Interessen der Betroffenen).
- Nur bei berechtigtem Interesse darf eine Versicherung Daten über einen Versicherungsnehmer abfragen.

117 JB 2006, 2.3

- Versicherungswirtschaft und Auskunftei werden größtmögliche Transparenz gewähren. Allerdings müssen keine Einmeldekriterien bekannt gegeben werden, die für den unredlichen Versicherungsnehmer von Interesse sein könnten.
- Die Einmeldekriterien unterliegen einer ständigen Evaluierung.
- Bei versicherungsrechtlichen Zweifelsfragen sollte die Versicherungsombudsstelle eingeschaltet werden können.
- Die am HIS beteiligten Beschäftigten in den Versicherungen arbeiten nach strengen Compliance-Regelungen.

Das HIS der Versicherungswirtschaft ist seit April keine „Blackbox" mehr. Es ist auf dem Weg zu einer rechtmäßig arbeitenden Auskunftei.

## 10.5 Verpflichtung zum Abgleich mit Terrorlisten

Aus der Praxis

Die Antiterrorismus-Verordnungen (EG) Nr. 2580/2001 und (EG) Nr. 881/2002 gelten unmittelbar in jedem EU-Mitgliedstaat. Beide Verordnungen haben hauptsächlich das Ziel, dass den in Listen genannten terrorverdächtigen Personen und Organisationen keine Gelder, finanziellen Vermögenswerte, wirtschaftlichen Ressourcen zur Verfügung gestellt, sondern eingefroren werden. Die Listen werden vom Rat der EU und vom UN-Sanktionsausschuss erstellt und öffentlich gemacht. Mehrere Großunternehmen haben uns gefragt, ob sie aufgrund der Verordnungen verpflichtet seien, vor jeder Geldüberweisung oder Gewährung von Sachvorteilen gegenüber Arbeitnehmern, Kunden und Lieferanten einen Datenabgleich mit den in den Terrorlisten genannten Personen und Organisationen durchzuführen.

In den Verordnungen ist nicht geregelt, welche organisatorischen Maßnahmen die Unternehmen ergreifen müssen oder dürfen, um ihre Sorgfaltspflichten zu erfüllen. Insbesondere sind die Verordnungen zu unbestimmt, um eine Verarbeitung und Nutzung personenbezogener Daten zu erlauben. Die Verordnungen selbst kommen somit nicht als Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG in Betracht. Die Datenschutzbeauftragten des Bundes und der Länder

haben schon 2006 darauf hingewiesen, dass die Terrorlisten rechtsstaatlichen Standards nicht genügen[118].

Unternehmen haben allerdings ein berechtigtes Interesse[119] daran, personenbezogene Daten ihrer Kunden, Lieferanten und Beschäftigten in dem Umfang zu verarbeiten und zu nutzen, wie dies zur Umsetzung der o. g. Verordnungen erforderlich ist, und um insbesondere sicherzustellen, dass eine Überweisung nicht nach § 34 Außenwirtschaftsgesetz (AWG) strafbar ist. Ein Verstoß gegen § 34 Abs. 4 Nr. 2 AWG liegt vor, wenn die in den EU-Verordnungen enthaltenen Ge- und Verbote vorsätzlich oder fahrlässig nicht eingehalten werden, also Gelder nicht eingefroren bzw. ohne Genehmigung zur Verfügung gestellt werden oder den aufgelisteten Personen und Organisationen auf andere Weise zugute kommen. Soweit in Einzelfällen Datenverarbeitungen erforderlich sind, um eine Strafbarkeit nach § 34 AWG zu verhindern, liegen keine überwiegenden schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung vor. In diesen Einzelfällen ist der Datenabgleich daher zulässig.

Es gibt aber keine Rechtsvorschrift, die Unternehmen **verpflichtet**, die Daten aller Kunden, Lieferanten und Beschäftigten mit den Terrorlisten abzugleichen. Bei Überweisungen ist dies schon deshalb nicht erforderlich, weil Banken in ihren Zahlungsverkehrsregelungen Sicherungen eingebaut haben, die eine Geldüberweisung an Terrorverdächtige verhindern. Es wirft ein bezeichnendes Licht auf die Effektivität des Datenabgleichs mit den Terrorlisten, dass seit 2001 in Deutschland aufgrund solcher Maßnahmen insgesamt 203,93 Euro eingefroren wurden[120].

Die Antiterrorismusverordnungen verpflichten Unternehmen nicht, die Daten aller Vertragspartner mit den Terrorlisten abzugleichen. Ein Abgleich kann nur im Einzelfall zulässig sein.

118 Entschließung vom 16./17. März 2006: Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige, Dokumentenband 2006, S. 11; vgl. auch den Beschluss des Düsseldorfer Kreises vom 24. April 2009, Dokumentenband 2009, S. 24

119 § 28 Abs. 1 Satz 1 Nr. 2 BDSG

120 So die Antwort der Bundesregierung vom 4. Januar 2010 auf die Kleine Anfrage der Abgeordneten Ulla Jelpke u. a., BT-Drs. 17/388, S. 5

## 10.6 Cold Calls und kein Ende

Die Anzahl der Beschwerden wegen unzulässiger Werbeanrufe (Cold Calls)[121] hat sich weiter erhöht. Hieran änderte auch das im August in Kraft getretene Gesetz zur Bekämpfung unlauterer Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen nichts. Das Gesetz verlangt nun für rechtmäßige Telefonwerbung eine **ausdrückliche** Einwilligung der Verbraucherin oder des Verbrauchers. Cold Calls werden durch die Bundesnetzagentur für Telekommunikation verfolgt. Außerdem ist eine Rufnummernunterdrückung nicht mehr gestattet. Ein Verstoß dagegen kann als Ordnungswidrigkeit verfolgt werden.

Die illegal arbeitende Call-Center-Szene hat die Gesetzesverschärfungen natürlich nicht zum Anlass genommen, sich auf rechtskonforme Werbung zu beschränken. Sie verfügt über die personenbezogenen Daten von vielen hunderttausend, möglicherweise von Millionen Bürgerinnen und Bürgern. Da die Call-Center die berechtigten Löschungs- und Sperrungsforderungen der Betroffenen nicht erfüllen, werden Bürgerinnen und Bürger, deren Daten einmal in rechtswidrige Hände gelangt sind, häufig von verschiedenen Call-Centern mehrmals täglich belästigt. Die Call-Center entwickeln ständig neue Maschen. So gibt sich ein Anbieter als Berliner Datenschutzbeauftragter aus, mit dessen Hilfe die oder der Angerufene einen angeblich langjährig laufenden Glücksspielvertrag beenden kann, wenn er einige Monate Gebühren (in der Regel um 60 Euro) zahlt.

Um sich vor straf- und zivilrechtlichen Konsequenzen zu schützen, haben die Call-Center verschiedene Maßnahmen ergriffen. So geben sie in der Regel keine Adresse mehr an, Postanschrift ist meistens ein Postfach. Falls eine Adresse angegeben wird, handelt es sich um ein Büroserviceunternehmen, das Briefe nur weiterleitet. Die Call-Center-Beschäftigten melden sich nicht mit richtigem Namen. Die Namen der anrufenden Unternehmen ändern sich teilweise wöchentlich. Es soll ihnen inzwischen auch gelungen sein, mit manipulierten Rufnummernanzeigen Betroffene zu täuschen. Teilweise arbeiten Call-Center vom außereuropäischen Ausland aus, teilweise wird dies aber nur vorgetäuscht.

121 JB 2008, 2.1

Cold-Call-Unternehmen sind heute Teil der organisierten Kriminalität. Diese lässt sich nicht durch halbherzige Gesetzesverschärfungen abschrecken; es muss vielmehr verhindert werden, dass diese Kreise überhaupt in den Besitz von personenbezogenen Daten kommen.

## 10.7 Widerspruchsrechte – wertlos ohne Aufklärung!

Das Bundesdatenschutzgesetz erlaubt in § 28 Abs. 3 die Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Werbung, falls die Betroffenen nicht bei der verantwortlichen Stelle der Nutzung oder Übermittlung ihrer Daten für Zwecke der Werbung widersprechen. Deshalb sind die Betroffenen gemäß § 28 Abs. 4 Satz 2 „bei der Ansprache zum Zwecke der Werbung" über ihr Widerspruchsrecht nach § 28 Abs. 4 Satz 1 BDSG zu unterrichten. Denn anderenfalls wäre dieses Recht wertlos. Die Unterrichtungspflicht wird aber oft übersehen oder vergessen, sodass sie hier anhand zweier typischer Fälle verdeutlicht werden soll. Der Gesetzgeber hat der Unterrichtungspflicht über das Widerspruchsrecht eine so große Bedeutung beigemessen, dass er das Unterlassen der Unterrichtung in § 43 Abs. 1 Ziff. 3 BDSG zur Ordnungswidrigkeit erklärt hat.

### Die „angediente" Kreditkarte

Zahlreiche Kundinnen und Kunden eines Dienstleistungsunternehmens beschwerten sich bei uns darüber, dass ihre personenbezogenen Daten an eine Bank übermittelt worden waren und diese versucht habe, ihnen werbend eine Kreditkarte (Mastercard) „anzudienen". Dabei war dem Werbeangebot bereits eine Plastikkarte beigefügt, die einer echten Mastercard täuschend ähnlich sah. Sie enthielt sogar eine Kontonummer der betreffenden Kundinnen und Kunden. Sie sollten lediglich noch eine Einwilligungserklärung unterzeichnen, damit die Kreditkarte „freigeschaltet" werden könne. Die Werbeaktion war äußerlich so ausgestaltet, dass viele Kundinnen und Kunden nicht unterscheiden konnten, ob die Werbung von dem einen oder dem anderen Unternehmen stammte. Sie vermuteten daher eine rechtswidrige Übermittlung ihrer Daten wie Name, Anschrift und Kontonummer. Wir stellten fest, dass ein Kooperationsvertrag abgeschlossen worden war, durch den ein weiteres Unternehmen,

das bereits als „Datenverarbeiter im Auftrag“ agierte, die Kundendaten beider Unternehmen verknüpfen und im Auftrag für den anderen verarbeiten sollte. Insoweit sollte es als Auftragnehmer für die Datenverarbeitung[122] des einen und des anderen Unternehmens zugleich in Aktion treten und die Daten ohne Kenntnisnahme der einzelnen Datensätze durch die Auftraggeber selbst, aber in deren Interesse und nach deren Weisungen verknüpfen.

Es lag ein Datenverarbeitungsauftrag in einem Dreiecksverhältnis vor, bei dem die beiden Auftraggeber die Kundendaten von dem gemeinsamen Auftragnehmer so verarbeiten ließen, dass die Kunden eine Werbebroschüre, verbunden mit einer gebrauchsfertig ausgestanzten Kreditkarte, erhielten. Das Dienstleistungsunternehmen begründete die Zulässigkeit dieses Vorgehens mit einer „Einwilligungserklärung“, die im Opt-Out-Verfahren (also durch einen unterlassenen Widerspruch) per Internet durch die Kundinnen und Kunden erklärt worden sei. Daran allerdings konnten sich viele Beschwerdeführerinnen und -führer später nicht mehr erinnern.

Der Fall zeigt, dass bei rechtsrelevanten Erklärungen per Internet das Opt-Out-Verfahren unzulänglich ist, weil den Betroffenen oft nicht bewusst wird, rechtlich relevant gehandelt zu haben. Im Zuge unserer Überprüfung erklärte sich das betroffene Unternehmen bereit, künftig nur mit einem eindeutigen Opt-In-Verfahren zu operieren. Auch der nach § 28 Abs. 4 BDSG gebotene Hinweis auf die Widerspruchsrechte müsste deutlicher herausgestellt werden. Für die weiter gehende Werbeoption und Datenübermittlung an Dritte ist eine wirksame Einverständniserklärung im Sinne des § 4 a BDSG erforderlich. Die setzt jedoch voraus, dass das Einverständnis „ohne jeden Zweifel“ erklärt wird. Ein Opt-Out-Verfahren lässt immer Zweifel offen, ob die Kundin oder der Kunde eine rechtsverbindliche Erklärung abgeben wollte. Denn es kann nicht ausgeschlossen werden, dass Texte mit rechtserheblichen Auswirkungen übersehen oder falsch verstanden wurden. Einwilligungserklärungen und die Belehrung über den Widerspruch müssen die verantwortliche Stelle benennen.

Unabhängig davon bestanden Bedenken gegen einzelne Vereinbarungen des Datenverarbeitungsauftrags zwischen den beiden Auftraggebern: Der Wortlaut ließ nicht eindeutig erkennen, ob die Daten anderen Zwecken zugeführt

122 § 11 BDSG

und insofern rechtlich „übermittelt“ wurden. Die Auftragsverarbeitung nach § 11 BDSG setzt aber voraus, dass die datenschutzrechtliche Verantwortlichkeit eindeutig beim Auftraggeber verbleibt. Dazu gehört insbesondere, dass der Auftraggeber „jederzeit“ für die Verarbeitung verantwortlich bleibt und seine Verantwortung stets ausüben kann. Regelungen, die es dem Auftraggeber nur dann erlauben, die Verarbeitung der Daten zu kontrollieren, wenn er „nach schriftlicher Vorankündigung von zwei Wochen“ und „in Abstimmung mit dem Partnerunternehmen bei Vorliegen eines sachlichen Grundes“ sich über die Überprüfung mit dem zu Überprüfenden verständigt hat, vertragen sich nicht mit den gesetzlichen Anforderungen des § 11 BDSG. Zudem war von Anfang an beabsichtigt, die Kundendaten den Geschäftszwecken des anderen Unternehmens (zur Führung von Kreditkartenkonten) zuzuführen. Das „datenabgebende“ Dienstleistungsunternehmen hätte seine Kundschaft deshalb besonders deutlich auf die Verwendungszwecke und auf die datenschutzrechtlichen Verantwortlichkeiten und auf ihr Widerspruchsrecht hinweisen müssen. Da die gesamte Werbeaktion aufgrund der von uns unverzüglich eingeleiteten Überprüfung kurzfristig abgebrochen wurde und eine unzulässige Datennutzung durch das jeweils andere Unternehmen nicht festgestellt werden konnte, haben wir von ordnungsrechtlichen Maßnahmen abgesehen. Auch wurde uns versichert, dass die datenschutzrechtlichen Grundsätze künftig beachtet werden.

Die Verschachtelung von Datenverarbeitungsverträgen macht die Verarbeitung für die Betroffenen undurchsichtig, verunsichert sie und erzeugt Misstrauen auch gegenüber seriös erscheinenden Unternehmen. Die klare Trennung von Verantwortlichkeiten und Zuständigkeiten und die Respektierung der Unterrichtungspflichten und Widerspruchsrechte bei der Werbung sind notwendige Voraussetzungen einer kundenfreundlichen Transparenz bei der Datenverarbeitung.

**Werbung mit Meldedaten von Hotelgästen?**

Mehrere Gäste beschwerten sich darüber, dass die Daten der Meldeformulare, die nach dem Melderecht von jedem Hotelgast auszufüllen sind, von den Unternehmen zu Werbezwecken genutzt werden, ohne dass die Gäste zuvor über ihr Widerspruchsrecht informiert worden wären.

Eine Nutzung von melderechtlich zu erhebenden Daten für Werbezwecke ist rechtlich nicht zulässig. Vielmehr sind die aufgrund des Melderechts erhobenen Daten strikt von den sonstigen Geschäftszwecken des Unternehmens zu trennen. Die Meldedaten dürfen auch nicht um Angaben aus dem zugrunde liegenden Beherbergungsvertrag angereichert werden. Die Betroffenen, d. h. die Übernachtungsgäste, müssen eindeutig unterscheiden können, welche Daten ausschließlich für melderechtliche Zwecke und welche Daten für die Geschäftszwecke nach § 28 Abs. 1 Satz 1 BDSG erhoben und verarbeitet werden. Es muss insbesondere auf die melderechtliche Erhebungsgrundlage hingewiesen werden. Die Zweckbindung der für melderechtliche Zwecke erhobenen Daten ist strikt zu beachten, weil es im Interesse der Beherbergungsgäste liegt, dass ihre Daten, die auch von Polizeibehörden genutzt werden dürfen, nicht um zusätzliche „private" Daten angereichert werden. Denn die besonderen Meldescheine in den Beherbergungsstätten sind jederzeit für die Einsichtnahme durch die Polizei bereitzuhalten und auf Verlangen auszuhändigen.

Die Erhebung und Nutzung personenbezogener Daten für Zwecke der Kundenbetreuung sind ebenfalls, soweit diese Zwecke über den konkreten Geschäftszweck hinausgehen, von den nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhobenen Daten zu unterscheiden. Eine Verarbeitung und Nutzung für Werbezwecke ist nur zulässig, wenn sie sich auf den Datensatz nach § 28 Abs. 3 Satz 2 BDSG beschränkt und wenn die Betroffenen gemäß § 28 Abs. 4 Satz 2 BDSG bei der Ansprache über ihr Widerspruchsrecht unterrichtet werden. Werden über § 28 Abs. 3 und 4 BDSG hinausgehende Werbezwecke verfolgt, ist eine ausdrückliche Einwilligung nach § 4 a BDSG erforderlich.

**Polizeibehörden dürfen nur solche Angaben über Hotelgäste zugänglich gemacht werden, deren Erhebung das Melderecht vorschreibt. Die Nutzung dieser oder weiter gehender Daten für Werbezwecke ist ohne Information der Gäste über ihr Widerspruchsrecht unzulässig.**

## 10.8 Digitalisierte Unterschriften bei der Sparkasse



Die Berliner Sparkasse setzt ein neuartiges Verfahren ein, das die eigenhändige Unterschrift auf Papier ersetzen soll. Vorteil ist, dass z. B. für die Eröffnung eines Girokontos keine Verträge mehr ausgedruckt, unterschrieben und archiviert werden müssen, sondern der Vertrag nur noch elektronisch vorliegt und in elektronischer Form handschriftlich auf einer druckempfindlichen Schreibunterlage (sog. PenPad) unterzeichnet wird.

Aus datenschutztechnischer Sicht halten wir die eingesetzte, mittlerweile von verschiedenen Organisationen ausgezeichnete Technik aus folgendem Grund für problematisch:

Durch das PenPad werden mehr biometrische Daten aufgezeichnet, als bei der Analyse einer auf Papier vorliegenden Unterschrift ermittelbar wären. So werden die Schreibgeschwindigkeit und der Schreibdruck sehr detailliert aufgezeichnet. Die erhaltenen Unterschriftsdaten werden zwar verschlüsselt im Dokument gespeichert, diese Dokumente aber zentral auf einem Server der Sparkassen abgelegt. Die nötigen Entschlüsselungsschlüssel sind ebenfalls im Besitz der Sparkasse. Zudem erfolgt die Übertragung der biometrischen Daten aus patentrechtlichen Gründen bisher streckenweise (allerdings nur innerhalb einer Bankfiliale) unverschlüsselt.

Wir hatten angeregt, über eine Anpassung des Verfahrens in der Art nachzudenken, dass nicht die biometrischen Daten selbst, sondern, wie auch bei anderen biometrischen Verfahren üblich, ein sog. Template im Dokument gespeichert wird. Ein Template enthält wesentlich weniger Daten, die so berechnet sind, dass bei Vorhandensein eines Originals (eine weitere Unterschrift auf dem PenPad) die Echtheit bzw. Übereinstimmung mit sehr hoher Wahrscheinlichkeit bestimmt werden kann. Ausgeschlossen wäre jedoch die Reproduktion der Originaldaten allein aus dem Template. Mit den bei der Sparkassentechnik vorhandenen Originaldaten (und dem Entschlüsselungsschlüssel) ist hingegen prinzipiell die Fälschung anderer elektronischer Dokumente und sogar die Fälschung von Papierdokumenten (mit geeigneten automatischen Schreibgeräten, die Druck und Geschwindigkeit reproduzieren können) möglich.

Problematisch ist auch, dass diese biometrischen Daten gesammelt werden, ohne dass dadurch eine hohe Rechtssicherheit erreicht würde. Eine Prüfung der Unterschrift ist im Konzept des Arbeitsablaufes nicht vorgesehen, im Gegenteil: Die Prüfung ist nur bei Vorlage des sicher aufzubewahrenden Entschlüsselungsschlüssels – also mit hohem organisatorischen Aufwand – manuell möglich. Bei kryptographischen digitalen Signaturen (z. B. der qualifizierten digitalen Signatur) ist die Prüfung der Signatur fester Bestandteil der Einsatzvorgaben und jeder Person möglich, der das Dokument vorliegt. Auch kann die Technik nicht sicherstellen, dass eine Unterschrift wirklich zu dem vorliegenden Dokument geleistet wurde, da unter Verwendung des Entschlüsselungsschlüssels – der einer der Vertragsparteien zugänglich ist – prinzipiell die entschlüsselte biometrische Unterschrift problemlos unter jedes andere Dokument gesetzt werden könnte. Um dies zu verhindern, haben wir angeregt, dass eine oder einer der Sparkassenbeschäftigten den Zeitpunkt und den Vorgang des Unterzeichnens mit einer qualifizierten digitalen Signatur als Zeugin oder Zeuge bestätigt.

Dem Missbrauchsrisiko der zentralen Speicherung von biometrischen Unterschriftsdaten potentiell aller Kundinnen und Kunden der Berliner Sparkasse steht kein adäquater Sicherheitsgewinn gegenüber. Die Effizienzverbesserung der Abläufe wird mit einer problematischen Speicherung biometrischer Überschussinformationen und der im Vergleich zu Papierdokumenten nur beschränkten Nachweisbarkeit der Echtheit der Dokumente und damit geringerer Rechtssicherheit erkauft. Unsere Kritik hat bisher zu keiner Änderung des Systems geführt.

## 10.9 Umsetzung der EU-Dienstleistungsrichtlinie in Berlin

Die für die Umsetzung der Dienstleistungsrichtlinie in Berlin notwendigen gesetzlichen Regelungen sind rechtzeitig am 28. Dezember 2009 in Kraft getreten.[123] Wesentliches Element der landesrechtlichen Umsetzung ist das

123 Vgl. Gesetz zur Umsetzung der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt, GVBl. S. 674 ff.

Gesetz über den Einheitlichen Ansprechpartner (EA-Gesetz Berlin). Es regelt die Aufgaben und die Zuordnung dieser Stelle in der Berliner Verwaltung. Danach gibt es in Berlin – anders als in anderen Bundesländern – nur einen einzigen Einheitlichen Ansprechpartner. Er ist bei der für die Wirtschaft zuständigen Senatsverwaltung eingerichtet und soll auf Wunsch eines Unternehmens als Verfahrensbegleiter die mit der Aufnahme und Ausübung von Dienstleistungstätigkeiten verbundenen Verfahren und Formalitäten koordinierend abwickeln. Daneben ist er Kontakt- und Informationsstelle für Unternehmen und Empfangende von Dienstleitungen.

Bereits im letzten Jahr haben wir ausführlich über die datenschutzrechtlichen Fragestellungen bei der Tätigkeit des Einheitlichen Ansprechpartners berichtet.[124] Wir hatten gefordert, für den Umgang mit personenbezogenen Daten durch den Einheitlichen Ansprechpartner eine normenklare gesetzliche Grundlage zu schaffen, die die zentralen Grundsätze der Erforderlichkeit, Zweckbindung und Transparenz der Datenverarbeitung berücksichtigt.

Die für den Gesetzentwurf federführende Senatsverwaltung für Wirtschaft, Technologie und Frauen hat unsere Vorschläge vollständig aufgegriffen und eine umfassende Regelung zur Datenverarbeitung in das EA-Gesetz Berlin aufgenommen. Die Vorschrift präzisiert in besonderer Weise das Zweckbindungsprinzip, indem sie vorschreibt, dass personenbezogene Daten aus sachlich nicht zusammengehörigen Verwaltungsvorgängen getrennt verarbeitet werden müssen. Ferner sind enge Vorgaben für die Übermittlung von Daten durch den Einheitlichen Ansprechpartner an nicht-öffentliche Stellen vorgesehen. Im Falle einer Übermittlung sind die betroffenen Personen darüber zu unterrichten.

Für die Wahrnehmung der Betroffenenrechte schafft die Vorschrift eine bemerkenswerte Verfahrenserleichterung. In den Fällen, in denen der Einheitliche Ansprechpartner als Informationsstelle oder Verfahrensbegleiter tatsächlich in Anspruch genommen wird, nimmt er Anträge der betroffenen Dienstleistungserbringer auf Auskunft und Akteneinsicht, Berichtigung und Löschung sowie Widersprüche gegen die Datenverarbeitung nach den §§ 16 ff. Berliner Datenschutzgesetz entgegen. Soweit erforderlich leitet der Einheitliche Ansprechpartner diese Anträge zur Bearbeitung an die mit ihm kooperierenden zuständigen

124 JB 2008, 11.5.

Stellen in der Verwaltung weiter. Der Dienstleistungserbringer kann damit auch bei der Geltendmachung seiner Datenschutzrechte die Vorteile einer zentralen Anlaufstelle nutzen.

Die gesetzlichen Grundlagen für eine datenschutzkonforme Arbeit des Einheitlichen Ansprechpartners wurden geschaffen. Jetzt gilt es, sie bei der technischen und organisatorischen Gestaltung der zugrunde liegenden Verfahren zu berücksichtigen. Wir werden auch diesen Prozess aufmerksam begleiten.

## 10.10 Appetit auf Stollen und Datenschutz

Aus der Praxis

Der Frankfurter Rundschau wurde von einem Kurierdienst ein Paket zugestellt, das personenbezogene Daten von rund 130.000 Kreditkartenkundinnen und -kunden der Landesbank Berlin enthielt. Im Paket waren Mikrofiches, die den Namen und die Adresse der Kundin oder des Kunden enthielten, außerdem Kreditkartennummer, Kundennummer und Kreditkartenabrechnungen mit sämtlichen Buchungen. Die Daten stammten aus dem Jahr 2008. Die polizeilichen Ermittlungen ergaben, dass zwei Kurierfahrer ein Paket an die Frankfurter Rundschau öffneten und den Inhalt – einen Stollen - verzehrten. Als Ersatz für das Stollenpaket etikettierten sie ein anderes Paket um. Hierbei wählten sie zufällig eines aus, das von einem technischen Dienstleistungsunternehmen an die Landesbank Berlin geschickt wurde. Dieses hatte von der Landesbank Berlin die o. g. Kundendaten mit dem Auftrag erhalten, sie zu verfilmen und die Mikrofiches zur Archivierung an die Bank zurückzusenden. Hierzu bediente sich der Dienstleister eines Logistikunternehmens, das den Auftrag allerdings an den Kurierdienst weitergab.

Mikrofilme können nachträglich nicht manipuliert werden und sind aufgrund ihrer Haltbarkeit für Archivierungszwecke besonders geeignet, haben allerdings den Nachteil, dass eine Verschlüsselung nicht möglich ist. Wenn man diese Technologie nutzt, muss man die Sicherheit auf dem Transportweg erhöhen. Daten dürfen nicht wie Weihnachtsgebäck als normale Paketsendung, sondern

müssen wie Bargeld verschickt werden, also in verschlossenen Containern und mit lückenlosen Versendungsnachweisen.

Das bei dieser „Stollenaffäre“ zutage getretene Kernproblem besteht darin, dass Unternehmen, die mehrere Auftragnehmer und Subunternehmer einsetzen, die Verantwortung für diese Verarbeitungsketten entweder bewusst oder fahrlässig vernachlässigen, weil sie der irrigen Auffassung sind, Verantwortung für den Datenschutz ließe sich „outsourcen“. So enthielt der Vertrag der Landesbank Berlin mit dem Dienstleister zur Auftragsdatenverarbeitung verschiedene Mängel. Insbesondere wurden der datenschutzgerechte Transport und die Einsetzung der Subunternehmer nicht geregelt. Auch hat es die Landesbank Berlin versäumt, ihre nach § 11 BDSG bestehenden Kontrollpflichten bei den Auftragsdatenverarbeitern zu erfüllen.

Die Landesbank Berlin hat sofort reagiert. Die Mikrofilme werden nun von Beschäftigten der Landesbank Berlin in sicheren Behältnissen transportiert. Sie hat außerdem ihre sämtlichen Auftragsdatenverarbeitungen durch ein externes Beratungsunternehmen überprüfen lassen und hierdurch das Datenschutzniveau der Bank insgesamt erhöht. Es ist zu hoffen, dass andere Unternehmen sich an diesem Vorgehen ein Beispiel nehmen.

Daten von Bankkundinnen und -kunden dürfen nicht wie Weihnachtsgebäck als normales Paket versandt werden. Vielmehr sind solche Daten wie Bargeld im verschlossenen Container mit lückenloser Transportkontrolle zu versenden. Auftraggeber können ihre datenschutzrechtliche Verantwortung nicht „outsourcen“.

# 11. Europäischer und internationaler Datenschutz

## 11.1 Europäische Union

Für großen Wirbel sorgten die neuen Entwicklungen zum Thema SWIFT[125], über das wir mehrfach berichtet hatten.[126] Aufgrund des internationalen politischen Drucks, aber auch auf Drängen der Datenschutzbeauftragten in Europa, hatte die belgische Firma zugesagt, künftig die Spiegelung der Daten zum Zahlungsverkehr ohne US-Bezug nicht mehr auf einem Server in den USA vorzunehmen, sondern auf einem Server in der Schweiz. Dadurch sollte verhindert werden, dass die US-Sicherheitsbehörden weiterhin auf die internationalen und innereuropäischen Zahlungsströme zugreifen. Um dies dennoch zu dürfen, hat die US-Regierung mit der Europäischen Kommission Verhandlungen über ein Abkommen aufgenommen, das den Zugriff auf den Schweizer Server legalisiert. Dieses Abkommen wurde in Windeseile ausgehandelt und unter schwedischer Ratspräsidentschaft in gleicher Eile noch Ende November beschlossen.[127] Das sorgte insbesondere deshalb für Wirbel, weil ab dem 1. Dezember nach dem neuen EU-Vertrag von Lissabon eine Beteiligung des Europäischen Parlaments an solchen Abkommen zwingend ist. Nun aber entstand in der Öffentlichkeit der Eindruck, dass das Abkommen „am Parlament vorbei" in Kraft gesetzt werden soll. Dieses hatte erhebliche datenschutzrechtliche Defizite kritisiert. Tatsache ist, dass auch zu diesem Abkommen, das für einen Übergangszeitraum bis längstens Oktober 2010 gelten sollte, die Zustimmung des Europäischen Parlaments formal notwendig war. Die Bundesregierung enthielt sich im Rat der Stimme. Das war umso bedauerlicher, als zuvor nicht nur die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[128], sondern auch der Bundesrat einstimmig die Zeichnung des Abkommens abge-

125 Society for Worldwide Interbank Financial Telecommunication

126 Zuletzt JB 2007, 10.1

127 Beschluss des Ministerrats vom 27. November 2009, 16110/09

128 Entschließung vom 8./9. Oktober 2009: Kein Ausverkauf von europäischen Finanzdaten an die USA!, Dokumentenband 2009, S. 19

lehnt hatte. Mittlerweile hat sogar das Bundeskriminalamt – im Gegensatz zum Bundesinnenminister – die Bankdatentransfers als nutzlos bezeichnet[129].

Insgesamt ist bereits bedenklich, dass die Terrorismusbekämpfung in Europa offenbar maßgeblich den USA anstatt den europäischen Sicherheitsbehörden überlassen werden sollte - noch dazu mit Befugnissen, die nicht einmal deutsche Sicherheitsbehörden haben. Besonders kritisch an dem teilweise geheim gehaltenen Abkommen war, dass die US-Sicherheitsbehörden Zugriff auf Millionen personenbezogene Daten gehabt hätten, die nicht nur internationale und europaweite, sondern auch innerdeutsche Zahlungsvorgänge betreffen. Die Abfrage von Kontobewegungen sollte zwar nur bei konkreten Verdachtsmomenten, dass die Zahlungen mit dem Terrorismus in Verbindung stehen, erlaubt werden. Wann eine solche Verbindung zum Terrorismus vorliegen sollte, war allerdings unklar. Auch war fraglich, ob der im Abkommen zugesicherte Rechtsschutz realisierbar ist, denn es deutete alles darauf hin, dass US-Sicherheitsbehörden den europäischen Datenschutzbeauftragten keine Einsicht in die Datenbestände zugebilligt hätten. Dann aber wäre eine unabhängige Datenschutzkontrolle in den USA nicht gewährleistet. Erfreulicherweise hat das Europäische Parlament dem bis zuletzt wachsenden Druck der US-Regierung standgehalten und das Abkommen mit großer Mehrheit am 11. Februar 2010 abgelehnt.

Ebenfalls unter schwedischer Ratspräsidentschaft wurde das sog. **Stockholmer Programm** als Nachfolge des sog. Haager Programms am 11. Dezember verabschiedet.[130] Es umfasst die politischen Ziele für 2010 bis 2015 für einen „Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger". Die Freiheitsrechte der Bürgerinnen und Bürger zu wahren und deren Privatsphäre zu schützen, wird zwar zur Priorität erhoben. Im Gegensatz zu diesem Programmsatz sind aber zugleich neue, zentrale EU-Datenbanken (wie für Ein- und Ausreisen in die oder aus der EU) geplant, die nicht nur die europäischen Bürgerinnen und Bürger „gläsern" machen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat gefordert, in Europa ein ausgewogenes Verhältnis zwischen Freiheit und Sicherheit, insbesondere im Bereich

129 Der Spiegel vom 4. Januar 2010, S. 15

130 Draft / The Stockholm Programme – An open and secure Europe serving the citizen, 14449/09, 16 October 2009

der polizeilichen und justiziellen Zusammenarbeit, herzustellen.[131] Diese Forderung wird vom Europäischen Parlament unterstützt[132].

Die Europäische Kommission hat eine **öffentliche Konsultation zum Rechtsrahmen für ein Grundrecht auf Datenschutz**[133] durchgeführt. Ziel war zu sondieren, welche neuen Anforderungen an den Datenschutz zu stellen sind, um einen effektiven und verständlichen Rechtsrahmen zum Schutz der Privatsphäre des Einzelnen innerhalb Europas zu schaffen. Hierzu hat die Art. 29-Datenschutzgruppe ein grundlegendes Papier[134] beschlossen, in dem u. a. ein einheitlicher, die drei Säulen umfassender Rechtsrahmen befürwortet wird, der im neuen EU-Vertrag von Lissabon vorgesehen ist. Auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat im Rahmen der Konsultation Stellung genommen.

Die **Aufgabenverteilung in der Europäischen Kommission** wird geändert. Künftig sind die Bereiche Justiz und Inneres in der Kommission getrennt. Es soll eine Kommissarin für Justiz, Grundrechte und bürgerliche Freiheiten sowie eine Kommissarin für Innenpolitik und Migration geben. Die Trennung entspricht der Situation in fast allen EU-Mitgliedstaaten und ist angesichts des natürlichen Spannungsverhältnisses zwischen den Sicherheitsinteressen einerseits und den Freiheitsrechten andererseits zu befürworten. Auch die Senatsverwaltung für Justiz hat sich für diese Trennung eingesetzt und wurde dabei von uns unterstützt.

Großbritannien avanciert offenbar zum „Europameister" in Sachen Überwachung. Unter Berufung auf die britische Gesetzgebung für Grenzkontrollen verlangt Großbritannien im Rahmen von **eBorders** die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungs-

131 Entschließung vom 8./9. Oktober 2009: Datenschutzdefizite in Europa auch nach Stockholmer Programm, Dokumentenband 2009, S. 20

132 Entschließung vom 25. November 2009, BR-Drs. 910/09

133 http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

134 vom 1. Dezember 2009 (WP 168): Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der öffentlichen Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf Schutz der personenbezogenen Daten, Dokumentenband 2009, S. 81

datenbanken der Fluggesellschaften. Der Düsseldorfer Kreis hat festgestellt, dass die Übermittlung dieser Passagierdaten durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist.[135] Zugleich wurde die Bundesregierung gebeten, solchen Forderungen der britischen Behörden entgegenzutreten. Von den deutschen Fluggesellschaften wird erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben. Diese Bewertung ist noch nicht abgeschlossen.

Die **Art. 29-Datenschutzgruppe** hat mehrere Stellungnahmen verabschiedet. Sie befasste sich mit den Vorschlägen zur Änderung der Europäischen Datenschutzrichtlinie für die elektronische Kommunikation[136] sowie mit der Nutzung sozialer Online-Netzwerke[137]. Auch hat sie erneut zum Schutz personenbezogener Daten von Kindern[138] Stellung genommen sowie zum internationalen Datenschutzstandard der Welt-Anti-Doping-Agentur (WADA)[139]. Schließlich hat sie sich mit dem Entwurf internationaler Wirtschaftsverbände von sog. Alternativen Standardvertragsklauseln für die Auftragsdatenverarbeitung[140] befasst, der die bisher gültigen Standardvertragsklauseln für die Auf-

135 Beschluss vom 13. Juni 2009: Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!, Dokumentenband 2009, S. 25

136 Stellungnahme 1/2009 vom 10. Februar 2009 (WP 159) über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation), vgl. 14.2

137 Stellungnahme 5/2009 vom 12. Juni 2009 (WP 163) zur Nutzung sozialer Online-Netzwerke, Dokumentenband 2009, S. 62; vgl. 14.1

138 Stellungnahme 2/2009 vom 11. Februar 2009 (WP 160) zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen)

139 2. Stellungnahme 4/2009 vom 6. April 2009 (WP 162) zum Internationalen Standard der Welt-Anti-Doping-Agentur (WADA) zum Schutz der Privatsphäre und personenbezogener Informationen, zu entsprechenden Vorschriften des WADA-Codes und zu anderen Datenschutzfragen im Bereich des Kampfes gegen Doping im Sport durch die WADA und durch (nationale) Anti-Doping-Organisationen

140 JB 2008,12.2; Stellungnahme 3/2009 vom 5. März 2009 (WP 161) über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter), Dokumentenband 2009, S. 54

tragsdatenverarbeitung[141] ablösen soll. Eine erste Arbeitsunterlage zur Datenübermittlung an US-Unternehmen im Rahmen von zivilrechtlichen Verfahren (Pre-trial Discovery) hat die Art. 29-Datenschutzgruppe ebenfalls verfasst.[142]

**Die Regierungen der EU-Mitgliedstaaten und die Kommission sind offenbar zunehmend bereit, europäische Datenschutzstandards abzusenken und die Terrorismusbekämpfung entweder US-Behörden zu überlassen oder deren Methoden in Europa zu übernehmen. Es bleibt zu hoffen, dass das durch den Vertrag von Lissabon mit erweiterten Kompetenzen ausgestattete Europäische Parlament dem wirksam entgegentreten wird.**

## 11.2 Internationale Datenschutzstandardisierung

Die Internationale Standardisierungsorganisation (ISO) arbeitet derzeit an der Entwicklung eines Rahmenstandards für den Datenschutz. An dem Beitrag der deutschen Normungsorganisation DIN zu diesem Standard haben wir uns maßgeblich beteiligt.

Das primär mit der Standardisierung von Techniken der Informationssicherheit befasste Komitee SC27 der ISO hat 2007 eine Arbeitsgruppe (WG5) unter deutscher Leitung eingerichtet, die technische Standards zum Datenschutz und zum Identitätsmanagement formulieren soll. Daneben beschäftigen sich je nach den bereichsspezifischen Erfordernissen weitere Komitees der ISO mit Datenschutzfragen. Die WG5 hat eine Koordinierungsfunktion für alle datenschutzrelevanten Aktivitäten der ISO übernommen.

Datenschutzstandards erleichtern es multinational tätigen Organisationen und Unternehmen, die nationalen Anforderungen einzuhalten, ermöglichen es nationalen Behörden, ihre Anforderungen in einem international verständlichen Vokabular zu fassen, und erlauben die transparente Darstellung der Einhaltung von Datenschutzanforderungen nach außen. So bergen die internati-

141 ABl. L 006 vom 10. Januar 2002, S. 52

142 Arbeitsunterlage 1/2009 vom 11. Februar 2009 (WP 158) über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (Pre-trial Discovery), Dokumentenband 2009, S. 35; zum Hintergrund vgl. zuletzt JB 2008, 12.2

onalen Standardisierungsbemühungen sowohl Chancen als auch Risiken. Es kommt darauf an, dass die Einhaltung deutschen und europäischen Rechts mit Hilfe des Standards abgebildet werden kann und die Einhaltung der in den Standards niedergelegten Datenschutzprinzipien hinreichend aussagekräftig ist.

Der Entwurf des Datenschutz-Rahmenstandards 29100 legt die Datenschutzterminologie fest (z. B. was ein personenbezogenes Datum ist) und definiert die grundlegenden Prinzipien des Datenschutzes wie die Einwilligung und Wahlfreiheit der Betroffenen oder die Bindung der Verarbeitung von personenbezogenen Daten an den Zweck, zu dem sie erhoben wurden. Angesichts der möglichen Auswirkungen des Standardisierungsvorhabens 29100 auf die eigene Aufsichtstätigkeit haben wir an der Formulierung des Standards mitgewirkt und unsere Empfehlungen über das Deutsche Institut für Normung (DIN) und in Zusammenarbeit mit der Art. 29-Datenschutzgruppe eingebracht. Erfreulicherweise basierten die deutschen Kommentare zu den Entwurfsvorlagen maßgeblich auf unseren Beiträgen und konnten sich auch bei der internationalen Abstimmung vielfach durchsetzen. Dadurch ist es gelungen, die Terminologie des Standards in einigen Punkten dem deutschen Recht anzugleichen und die Datenschutzprinzipien aussagekräftig normativ zu fassen. Aufgrund des US-amerikanischen und ostasiatischen Widerstands belässt es der Standardentwurf bei der unverbindlichen Empfehlung, die Prinzipien auch einzuhalten. Dies ist sehr unbefriedigend, da ein Unternehmen die Einhaltung des Standards 29100 behaupten könnte, die Bedeutung dieser Aussage jedoch unklar bliebe. Es besteht die Gefahr, dass Kundschaft und potenzielle Auftraggeber durch eine derartige Behauptung irregeführt werden.

Internationale Standards bieten Chancen und Risiken für die Einhaltung des Datenschutzes bei transnationaler Datenverarbeitung. Die europäischen Datenschutzbehörden sind gefordert, auf den Standardisierungsprozess so einzuwirken, dass das hohe europäische Datenschutzniveau nicht unterlaufen, sondern seine Verbreitung gefördert wird.

## 11.3 AG „Internationaler Datenverkehr“

Die AG „Internationale Datenverkehr“ des Düsseldorfer Kreises hat unter unserem Vorsitz erneut Fragestellungen zur Datenübermittlung durch deutsche Unternehmen an US-Unternehmen im Vorfeld von zivilrechtlichen Streitigkeiten (**Pre-trial Discovery**) erörtert. Angesichts des Arbeitspapiers der Art. 29-Datenschutzgruppe[143] wurde die bisher vertretene Auffassung des Düsseldorfer Kreises, dass Pre-trial Discovery-Ersuchen vom BDSG i. V. m. dem „Erledigungsverbot“ nach HBÜ grundsätzlich nicht gedeckt seien[144], modifiziert. Vor Klageerhebung darf weiterhin nichts übermittelt werden, während eine Übermittlung nach Klageerhebung auf der Grundlage von § 4 c Abs. 1 Satz 1 Nr. 4 BDSG zulässig ist, weil der Anspruch „vor Gericht“ anhängig ist. Dies gilt allerdings nur unter der Voraussetzung, dass ein zweistufiges Verfahren beachtet wird: Zunächst sind die prozessrelevanten E-Mails vor Übermittlung in die USA zu pseudonymisieren. Erst in einem zweiten Schritt dürfen personenbezogene Daten wie Namen in die USA übermittelt werden, wenn es im Einzelfall erforderlich ist.

Im Hinblick auf das immer mehr Anklang findende Verfahren zur gegenseitigen Anerkennung von verbindlichen Unternehmensregelungen in der EU (**Mutual Recognition**)[145] wurde beschlossen, dass bei deutscher Beteiligung am europäischen Koordinierungsverfahren nach dessen Abschluss kein Beschluss des Düsseldorfer Kreises mehr erforderlich ist, mit dem ausreichende Datenschutzgarantien attestiert werden. Künftig reicht die Benachrichtigung des Düsseldorfer Kreises durch die federführende deutsche Aufsichtsbehörde aus.

143 Vgl. Fn. 140

144 JB 2007, 10.3 (vorletzter Absatz)

145 Neben Deutschland sind bislang Belgien, Bulgarien, Frankreich, Großbritannien, Irland, Island, Italien, Lettland, Liechtenstein, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Slowenien, Spanien, Tschechien und Zypern beteiligt.

# 12. Technik und Organisation

## 12.1 Videoüberwachung – auch in Geschäften kein Patentrezept



Seit ca. einem Jahr häufen sich die Beschwerden von Bürgerinnen und Bürgern wegen der zunehmenden Videoüberwachung in Geschäften mittelständischer und kleiner Unternehmen mit Kundenverkehr. Hierzu zählen auch die unzähligen Filialen der Lebensmittelketten. Betroffen sind fast alle Branchen wie Friseurgeschäfte, Videotheken, Apotheken, Boutiquen, Imbissbuden, Kioske und Zeitungsstände.

Die verantwortlichen Stellen (die Ladenbesitzer) berufen sich auf § 6 b Abs. 1 Nr. 3 BDSG. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Als Gründe für eine Videoüberwachung werden häufig generalpräventive Zwecke wie die Furcht vor Warendiebstahl, Einbruch, Sachbeschädigung und der Schutz der Beschäftigten vor tätlichen Übergriffen gewalttätiger Kunden genannt. Bevor jedoch eine Videoüberwachungsanlage installiert wird, müssen drei grundlegende Kriterien geprüft werden: Die Erforderlichkeit, die Geeignetheit und die Verhältnismäßigkeit einer solchen Maßnahme. Nur wenn alle drei Kriterien erfüllt sind, ist eine Videoüberwachung gerechtfertigt.

Es liegt im ureigenen Interesse einer Ladenbesitzerin oder eines -besitzers, sich vor Diebstahl, Einbruch und Übergriffen zu schützen. Allerdings ist eine Videoüberwachung nur dann erforderlich, wenn es auch tatsächlich zu solchen Vorfällen gekommen ist. Ladenbesitzerinnen und -besitzer sollten diese Vorfälle durch die Vorlage einer Strafanzeige bei der Polizei belegen können. Die Erforderlichkeit kann in Einzelfällen aber auch angenommen werden, wenn ein besonderes Schutzbedürfnis dargestellt werden kann, z. B. wenn das videoüberwachte Geschäft in einer Umgebung mit hoher Kriminalitätsdichte liegt.

Einige Geschäfte neigen dazu, ihre Verkaufsräume lückenlos mit Videokameras auszustatten. Das ist aber nur dann verhältnismäßig, wenn ausschließlich solche Bereiche im Beobachtungsfeld der Kameras liegen, die geschützt werden sollen. Wenn etwa Bezahlvorgänge dokumentiert oder an der Kasse Beschäftigte vor tätlichen Übergriffen geschützt werden sollen, muss sich die Kameraüberwachung auf den Kassenbereich beschränken.

Es gibt Geschäfte, die ihre hochwertigen Artikel offen in Regalen anbieten oder nah am Eingangsbereich platzieren. Zum Schutz dieser Ware ist die Installation einer Videoüberwachung jedoch nicht geeignet. Diebstähle könnten wirkungsvoller durch das Aufstellen leerer Flaschen und Kartons oder Verpackungen verhindert werden. Möglich wären auch Glasvitrinen oder abschließbare Regale. Diese Alternativen wären mildere Mittel, die einerseits die gewünschten Zwecke der verantwortlichen Stelle erreichen und andererseits die Persönlichkeitsrechte der betroffenen Kundinnen und Kunden berücksichtigen würden.

Vor der Installation von Videoüberwachungskameras in Geschäften mit Kundenverkehr muss ihre Zulässigkeit nach § 6 b BDSG geprüft werden. Videoüberwachung muss erforderlich, geeignet und verhältnismäßig sein, und es ist zu prüfen, ob andere Mittel, die nicht in Persönlichkeitsrechte der Kundschaft und der Beschäftigten eingreifen, nicht in gleicher Weise zum Ziel führen.

## 12.2 Neue Bedrohungen durch Schadprogramme

Obwohl ständig neue Schadprogramme bekannt werden, geraten sie immer weniger in den Blickpunkt der Medien. Dies mag daran liegen, dass das öffentliche Interesse an diesen mittlerweile allgegenwärtigen Problemen ermüdet sein könnte, auch weil zumindest in Europa[146] spektakuläre Angriffe auf die IT-Sicherheit bedeutender Anwender nicht bekannt wurden. Dies sollte aber nicht dazu führen, dass die Computeranwender in Wirtschaft und Verwaltung

146 Nach Redaktionsschluss wurden massive – offenbar von China ausgehende – Hackerangriffe auf Google und andere Unternehmen bekannt.

sich in trügerischer Sicherheit wähnen. Untersuchungen[147] haben gezeigt, dass Computer durchschnittlich bis zu einem Jahr mit Schädlingen befallen sind, bevor diese sich bemerkbar machen. An dieser langen Verweildauer sind oft sog. Botnetze Schuld, die die Computer infizieren, dann aber ihre Funktionen im Verborgenen ausführen, z. B. indem sie im Rahmen eines Denial-of-Service-Angriffs (Überflutungsangriffs) mit tausenden anderen infizierten Rechnern gleichzeitig wichtige Internetportale aufrufen, um diese zum Absturz zu bringen. Während die klassischen Viren, die z. B. die Festplatte formatieren, kaum noch auftreten, spielen heute Trojaner, Rootkits und Würmer eine viel gefährlichere Rolle. Auffällig ist, dass immer mehr Schadprogramm-Angriffe über soziale Netzwerke erfolgen. Gründe dafür sind die Neugierde der Nutzenden oder die Einfachheit der Web-Weiterleitung. Es gibt z. B. folgende aktuelle Bedrohungen, zu denen aktuelle Hinweise zur Gefahrenabwehr gegeben werden.

### Trojaner

Trojaner sind schon seit längerem die am häufigsten auftretende Art von Schadprogrammen. Die meist in einem vorgeblich harmlosen Programm verborgenen, Schaden stiftenden Routinen dienen dazu, heimliche Zugänge (Hintertüren) zu öffnen oder die System- und Internet-Identitäten der Anwendenden auszuspionieren. Verbreitet sind sog. Keylogger, die die Tastaturanschläge protokollieren und die Protokolle zu einem späteren Zeitpunkt an eine zuvor definierte Adresse im Internet verschicken. Die Infektion erfolgt häufig beim Empfang einer E-Mail mit einem für Nutzende wichtigen Betreff und der Aufforderung, eine Anlage zur E-Mail aufzurufen, um Näheres zu erfahren. Wichtige Beispiele sind fingierte E-Mails mit dem Absender von Postdienstleistern wie UPS oder DHL, in denen darauf hingewiesen wird, dass es mit der Auslieferungsadresse Probleme gibt und Genaueres in der Anlage zu lesen ist. Eine Sonderform des Trojaners sind Spyware-Programme, die z. B. Surfgewohnheiten ausspionieren.

### Rootkits

Rootkits wurden als Sammlung von Schaden bringenden Tools für Unix und Unix-ähnliche Betriebssysteme bekannt, die vergleichbar mit Trojanern einen Computer infizieren, um danach weitere Zugriffe des Eindringlings zu tarnen

147 Trend Micro, http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/

und Prozesse und Dateien von Schadsoftware zu verstecken. Da sie von den meisten Antivirus-Programmen nicht aufgespürt bzw. erkannt werden können, gehören die Rootkits zu den gefährlichsten Schadprogrammen. Als Weiterentwicklung können die Bootkits gesehen werden, die sich im Master Boot Record verstecken und somit vor dem Start des Betriebssystems aktiv werden. Wird später ein Antivirenprogramm gestartet, ist ein Auffinden sehr unwahrscheinlich. Das Bootkit „Kon-Boot 1.1“ entfernt z. B. den Passwortschutz von diversen MS Windows-Betriebssystemen sowie Linux-Distributionen.

### Würmer

Würmer sind eigenständige Programme, die sich systematisch in einem Computernetz verbreiten, z. B. über die bereits beschriebenen E-Mail-Anhänge. Sie haben meist keine eigene Schadfunktion, richten jedoch wirtschaftlichen Schaden durch die Beanspruchung von Rechner- und Netzkapazitäten an. Seit Anfang des Jahres verbreitet sich der Conficker-Wurm weltweit über das Internet. Die Verbreitung erfolgte ursprünglich über eine Lücke im Windows-Betriebssystem, obwohl schon seit Ende 2008 ein Patch zur Beseitigung der Lücke zur Verfügung stand. Innerhalb kürzester Zeit waren mehrere Millionen Computer verseucht. Auch die sozialen Netzwerke Facebook oder Twitter werden inzwischen verstärkt genutzt, um den Wurm zu verbreiten. Der Conficker-Wurm leitet die Nutzenden über einen geschickten Link zu einer gefälschten Webseite, wo sie veranlasst werden, ihre Authentifizierungsdaten einzugeben. Meist erscheint eine Fehlermeldung, die oder der Betrügende erhält jedoch korrekte Anmeldedaten.

### Exploits

Sicherheitslücken, kleine Fehler in Betriebssystemen oder Programmen, werden von Cyber-Kriminellen ausgenutzt, indem sie speziell zur Nutzung einer bekannt gewordenen Lücke entwickelte Programme zum Angriff auf ein System verwenden. Diese sog. Exploits[148] öffnen ohne Zutun des Benutzers die Zugänge zum System für den Angreifer. Man unterscheidet Exploits meist nach der Art des Angriffs. Lokale Exploits werden aktiviert, wenn eine Anwendung geöffnet wird, die die Lücke enthält, für deren Ausnutzung das Exploit geschaffen wurde. Remote Exploits nutzen Schwachstellen der Netzsoftware für Angriffe aus dem Internet. Deshalb sollten Updates bzw. Patches, die der

148 to exploit = ausnutzen

Behebung der Schwachstelle dienen, unverzüglich nach ihrer Bereitstellung installiert werden. Dies hilft allerdings nicht gegen die sog. Zero-Day-Exploits, die bereits vor oder am selben Tag, an dem die Lücke bekannt wird, für Angriffe auf dann in der Regel noch ungeschützte Rechner erfolgt.

### Web-Verbreitung

Spezielle Tools erzeugen perfekt nachgebildete Webseiten (z. B. von YouTube), die anschließend per Link in entsprechenden SPAM-Mails versendet werden. Wird dieser Link am angegriffenen Rechner ausgeführt, so öffnet der Browser die vermeintlich korrekte Internetseite. Hier erscheint dann eine Fehlermeldung, die zur Installation eines fehlenden Programms auffordert. Tatsächlich wird aber ein Schaden verursachender Code, z. B. ein Trojaner, aus dem Internet nachgeladen. Auf diese Weise werden täglich ca. 16.000 Webseiten infiziert.

### Drive-by-Download oder Drive-by-Infektion

Bereits beim Betrachten eines Videoclips im Web oder dem Besuch einer Website kann der Computer mit Schadcode infiziert werden. Die Angreifer nutzen immer mehr Sicherheitslücken bei Browsern zum Einschleusen von Schadcode aus. Hilfreich sind hier Add-ons (Browsererweiterungen), die z. B. Java bzw. Javascript blockieren, bis die Nutzerin oder der Nutzer die Java- oder Javascript-Anwendung selbst freigibt, damit also der spontanen Infektion mit Schadcode entgegenwirkt.

### Botnetze

Manche Programmierer von Schadcode sind darauf aus, möglichst viele Computer zu infizieren, um mit deren Hilfe an dritter Stelle großen Schaden anzurichten. Gelangt ein sog. Software-Bot auf einen fremden Computer, kann dieser von einem Botnetz-Operator ferngesteuert werden. Bis zu hunderttausend gekaperte Computer – manchmal Zombie-PCs genannt - werden zu einem Botnetz zusammengeführt. Diese Netze dienen meist der Verteilung von SPAM oder gezielter Denial-of-Service-Attacken, die z. B. dazu führen, dass Netzwerkdienste in einem angegriffenen Netz außer Funktion gesetzt werden.

### Scareware

Immer wieder wird die Angst der Computernutzenden vor Schaden verursachenden Programmen ausgenutzt, um ihnen tatsächlich Schaden zu bereiten. Mit Scareware[149] wird dem Anwender eine Software verkauft, die vor Angriffen schützen soll, die ihm vorher durch aufpoppende Fenster suggeriert wurden. Im Anschluss werden nur diese Warnungen ausgeschaltet, denn ein Angriff durch Schaden verursachende Software lag nicht vor. So wurde z. B. eine E-Mail mit dem Betreff „Conficker.B Infection Alert“ versandt, die der Auffindung des Conficker-Wurms dienen soll. Der besorgte Nutzer prüft seinen PC mit dem angehängten Scanfile. Dieser findet natürlich den im Betreff genannten schadhaften Code und bietet seine kostengünstige Entfernung an. Wenn man Glück hat, ist man danach nur um ein paar Euro ärmer, andernfalls um ein paar Schadprogramme „reicher“, die der sog. Scanfile zusätzlich installiert hat. Die Zahl der gefälschten Antiviren-Programme hat sich seit dem letzten Jahr versechsfacht. Das Antivirenprogramm von Kaspersky enthält ca. 30.000 Signaturen gefälschter Antivirenprogramme[150].

### Phishing

Beim Phishing wird versucht, durch massenhaften Versand von SPAM-Mail durch den Einsatz eines Trojaners in einem Anhang oder durch Leitung auf die gefälschte Webseite eines Kreditinstituts an Authentisierungsdaten für das Online-Banking oder an Kreditkarteninformationen zu gelangen. Die Nutzerin oder der Nutzer wird z. B. aufgefordert, mit Hilfe einer angehängten Datei eine Rechnung zu begleichen oder zu stornieren. Als Absender wird meist ein seriöses Großunternehmen genannt.

### Erste Hilfe

Bereits 2007 haben wir Mindestanforderungen zum Schutz vor schadhaftem Code aufgeführt[151]. Hierzu zählen ein aktuelles Virenschutzprogramm, eine sichere Firewall, die Aktualisierung von Programmen, Systemüberwachungstools und gesundes Misstrauen. Hier soll zusätzlich auf die speziellen Tools hingewiesen werden, die gezielt z. B. gegen Rootkits, Trojaner oder Spyware vorgehen.

149 to scare = erschrecken

150 Newsletter ZDNet.de vom 18. November 2009

151 JB 2007, 4.9

Aber es muss auch darüber nachgedacht werden, wie die Entwicklung zum Schutz vor schädlichen Codes tatsächlich vorangeht. Die rein signaturbasierte Suche nach Schadcodes wurde schon seit einiger Zeit um verhaltensbasierende Analysen ergänzt. Vielleicht wird es jedoch Zeit für einen grundsätzlichen Paradigmenwechsel, da die Signaturfiles immer umfangreicher werden, sodass teilweise dazu übergegangen wird, diese in Speichern im Internet (in the cloud) auszulagern.

Trotz der „medialen Ruhe" zum Thema Schadprogramme begleiten ihre Gefahren die Computernutzerinnen und -nutzer täglich. Die Verursacher sind längst nicht mehr die Anerkennung suchenden Computerfreaks, sondern Kriminelle. Nicht die Zerstörung von Daten, sondern die Erlangung von Informationen für die materielle Schädigung der Nutzerinnen und Nutzer steht heute im Vordergrund.

## 12.3 Was Programme so ausplaudern

Nicht nur die in der Presse gelegentlich behandelten Spionageprogramme, die alle an einem Computer ausgeführten Handlungen (wie die Eingabe von Text, z. B. von Passwörtern oder PINs, das Lesen und Schreiben von E-Mails, den Besuch von Webseiten, Start von Programmen) protokollieren können, verbreiten Informationen über unser Nutzerverhalten heimlich im weltweiten Netz. Hier soll über die Geschwätzigkeit von Betriebssystemen und „normalen" Standardprogrammen berichtet werden, die immer wieder Daten in das Internet übertragen. Manchmal wird der Anwender über einen beabsichtigten Verbindungsaufbau unterrichtet, meist verlaufen solche Aktionen jedoch unbemerkt im Hintergrund ab. Die Gründe hierfür können sehr vielschichtig sein, wie z. B. ein Versionsabgleich, damit benötigte Updates oder Patches installiert werden können. Welche Informationen jedoch übertragen werden, ist für die „einfachen" Computernutzenden nicht nachvollziehbar. Welche bekannten Plaudertaschen gibt es, und was kann man gegen sie tun?

### MS Windows

Da sind zunächst die Betriebssysteme, ohne die ein Rechner nicht auskommt. So stellt z. B. **MS Windows XP** regelmäßig eine Internetverbindung her,

damit überprüft werden kann, ob Updates oder Patches („Flicken“) für das Betriebssystem vorhanden sind und installiert werden sollten. Diese Aktualisierungen mögen ihre Berechtigung haben, doch es gibt auch andere Wege, das Betriebssystem auf einem aktuellen Stand zu halten, ohne dass automatisch eine Internetverbindung initiiert wird. Hier helfen sog. Update Packs, die eine Zusammenstellung der wichtigsten Patches beinhalten und von diversen Webseiten wie z. B. WinFuture.de oder WinBoard.org ohne die Übertragung von Betriebssystemdaten heruntergeladen werden können. Außerdem gibt es spezielle Software, die den Computer überprüft, ob alle wichtigen Updates oder Patches installiert sind. Auch hier erfolgt eine Überprüfung des Rechners, die zwar von der Nutzerin oder dem Nutzer initiiert wird. Sie oder er erfährt aber nicht, welche Daten übertragen werden. Wer sich also vor der automatischen Update-Prüfung schützen will, sollte die automatischen Updates deaktivieren.

Wird das Betriebssystem installiert, wird die Nutzerin oder der Nutzer aufgefordert, Windows zu aktivieren. Hierbei werden die ersten Daten an Microsoft übermittelt. Bisher ist diese Aktivierung auch noch anonym per Telefon möglich. Die sog. **WGA-Notifikation** wurde als wichtiges Patch unter WindowsXP installiert und nimmt regelmäßig Kontakt zu Microsoft auf, um zu prüfen, ob eine gültige Windows-Lizenz vorliegt. Laut Aussage von Microsoft ist dieser Patch nicht deinstallierbar, im Web findet man jedoch Hinweise, wie er gelöscht werden kann[152]. Wenn sich z. B. eine Anwendung vorzeitig beendet hat, erscheint ein Fenster, in dem der Hersteller bittet, zwecks Prüfung des Fehlers einen **Fehlerbericht** an ihn zu übertragen. Dieser kann jedoch je nach Anwendung Daten enthalten, die man nicht versenden möchte. Die Nutzerin oder der Nutzer kann dann per Dialogfeld das Versenden unterbinden oder das Erscheinen der Fehlerberichterstattung in den Systemeigenschaften deaktivieren. In **Windows Vista** muss der Windows-Fehlerberichterstattungsdienst ausgeschaltet werden.

Auch die **Dokumenten-Liste** kann einen Einblick in die Privatsphäre der Nutzenden ermöglichen, wenn sie nicht unter einer eigenen Kennung arbeiten. Ansonsten hilft ausschließlich die Deaktivierung dieser Option oder der Einsatz von Tools, die die Spuren beseitigen. Wenn man den **elektronischen Papierkorb** leert, wird lediglich der Speicherplatz zum Überschreiben freige-

152 com: Das Computer Magazin 1/2008

geben. Wenn sie endgültig gelöscht werden sollen, müsste dies mit speziellen Löschtools geschehen, die durch mehrfaches Überschreiben die Daten sicher beseitigen.

Abschließend sei auf diverse kostenfreie Tools hingewiesen, die z. B. die unbemerkte Kontaktaufnahme mit dem Hersteller unterbinden (z. B. XP-Antispy). Andere Tools wie das Programm ccleaner beseitigen Windows- und Internet-Explorer-Spuren.

### MS Office

Bis zum ServicePack 3 von **MS Office 2003** enthielten die gespeicherten Dateien sehr viele Zusatzinformationen (wie Entstehungsgeschichte, Änderungen, Speicherort, Autor), die mit der elektronischen Weitergabe von der Nutzerin oder dem Nutzer meist unwissentlich verbreitet werden. Gerade die Bearbeitungshistorie, bei der evtl. veränderte Textteile wiederhergestellt werden können, kann zu manchen Peinlichkeiten führen. Microsoft hat inzwischen spezielle Tools entwickelt, die solche Zusatzinformationen (Metadaten) aus den Dokumenten entfernen können[153].

### Adobe Acrobat Reader

Auch der Acrobat Reader von Adobe nimmt ständig Kontakt mit dem Hersteller auf, um zu prüfen, ob Updates vorliegen. Das Programm zum Deaktivieren wird mitgeliefert, liegt jedoch sehr versteckt. Wer „AdobeUpdater.exe“ aufruft, kann die Funktion „Automatisch nach Updates suchen“ deaktivieren.

### Medienabspieler

Wurde ein Stück mit dem **Real Player** in der Version 10.5 abgespielt, wurden gleichzeitig Nutzerdaten an den Hersteller gesendet. Es sollten die Eigenschaft „Player“ konfiguriert werden und in den Datenschutzeinstellungen alle Häkchen entfernt werden. Wird der **Quicktime Player** gestartet, wird eine Internetverbindung zum Hersteller aufgebaut, damit Werbung heruntergeladen werden kann. Diese lässt sich durch Deaktivierung der Funktion „HotPicks“ verhindern. Der **iTunes-Player von Apple** lädt nicht nur z. B. Podcasts herunter, es werden auch Daten über die abgespielten Lieder gesendet. Alles lässt sich

153 P. Schnoor: Spionageabwehr in Office, http://software.magnus.de/office-buero/artikel/persoenliche-daten-in-office-dokumenten.html

deaktivieren, z. B. durch Ausblendung des Ministore. Auch der **MediaPlayer** sendet Daten (auch Nutzerdaten) per Internet an den Hersteller. In den Optionen kann über den Reiter Datenschutz sehr viel deaktiviert werden, z. B. Lizenz-Downloads, Player-ID, Medieninformationen zu CDs/DVDs sowie Codec-Updates.

### Bilder

Die Datei **thumbs.db** findet sich in Ordnern, die Fotos enthalten. Darin sind in stark verkleinerter Auflösung alle Bilddateien des Ordners. Mit speziellen Tools können die Bilder vergrößert und sogar die Bildinformationen (z. B. Aufnahmedatum) angezeigt werden. Wird in den Ordneroptionen die Option „Miniaturansicht nicht zwischenspeichern" aktiviert, wird diese verräterische Datei nicht angelegt. Das gängige Format für die Speicherung von Fotos ist **jpeg** (als Dateikürzel auch jpg). Dass hier außer dem eigentlichen Bild auch noch Metadaten wie Datum und Uhrzeit oder Standortdaten (GPS) der Aufnahme aufgezeichnet werden, dürfte nicht allgemein bekannt sein. Kleine Freeware-Programme können diese Metadaten löschen.

### Browser

In Browsern befinden sich im Cache (bzw. Temporären Internetdateien), in der History (bzw. Chronik), in der URL-Anzeige (bzw. Browserverlauf) diverse Informationen wie Downloads, Formulardaten und Kennwörter. Auch wenn der Browser nichts „erzählt", bedienen sich die Webseitenbetreiber diverser Tricks. So setzen sie Cookies, vom Server gesendete und im Browser gespeicherte Informationsschnipsel, die inzwischen als Super-Cookies bis zu 5 MB groß sein können. Bei regelmäßig besuchten Seiten entstehen mit Hilfe dieser Cookies ausführliche Nutzerprofile. Auch werden Protokolle angelegt, die z. B. den Ablauf des Besuchs von Webseiten festhalten. Über die Datenschutzoptionen oder den Einsatz spezieller Tools lassen sich viele Daten nach Beenden des Programms automatisch löschen. Die Browserentwickler haben ebenfalls Abhilfe geschaffen, sodass in sog. „privaten Sessions" gesurft werden kann, ohne dass das Programm vertrauliche Daten speichert. Unter dem Betriebssystem MS Vista funktioniert die automatische Löschfunktion im Protected Mode wegen eines Programmfehlers leider nicht wie gewollt. **Google Chrome** vergibt eine persönliche Identifikationsnummer (ID) während der Installation, die

bei Updates übertragen wird. Hinweise zum Setzen einer anderen ID finden sich in der Fachliteratur[154].

### Software-Updates

Die Problematik der Software-Updates hat die internationale und die nationale Konferenz der Datenschutzbeauftragten veranlasst, schon 2003 entsprechende Entschließungen zu fassen[155]. Gerade in der nationalen Entschließung wird auf den Tatbestand hingewiesen, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Insbesondere greift das Berliner Datenschutzgesetz diese Problematik auf und benennt in § 3 a Anforderungen, die bei einer Wartung zu erfüllen sind. Zusammenfassend kann nur empfohlen werden, dass ausschließlich überprüfbare, benutzerinitiierte Update-Verfahren eingesetzt werden sollten, die keinen Datenaustausch mit dem Zielrechner erfordern.

Nutzende sollten Update-Funktionalitäten des Betriebssystems und von Anwendungsprogrammen sowie nicht benötigte Internetfunktionen (z. B. Cookies) deaktivieren. Es sollten ausschließlich überprüfbare, benutzerinitiierte Update-Verfahren eingesetzt werden, die keinen Datenaustausch mit dem Zielrechner erfordern. Auch im Übrigen sollten alle empfohlenen technischen Werkzeuge zum Schutz vor „geschwätzigen" Programmen auf dem Computer genutzt werden.

154 G. Salvisberg: So schützen Sie Ihre Daten im Browser, www.pctipps.ch.

155 Vgl. Dokumentenband 2003, S. 32, 97

## 12.4 Behördliche Datenschutzbeauftragte

### 12.4.1 Behördliche Datenschutzbeauftragte an den Berliner Hochschulen

Wir haben alle Universitäten und Hochschulen im öffentlichen Bereich einer Kontrolle unterzogen, um uns über die Stellung ihrer Datenschutzbeauftragten und insbesondere die nach § 19 a Abs. 3 Berliner Datenschutzgesetz geforderte Unterstützung und Ausstattung zu informieren. Die Kontrolle erfolgte zunächst auf schriftlichem Weg, in Einzelfällen erfolgten Nachfragen.

Die **Humboldt-Universität zu Berlin (HUB)** tut sich seit längerem schwer mit der Bestellung von Datenschutzbeauftragten und ihren Stellvertretern. Nachdem der langjährige Datenschutzbeauftragte aus dem Dienst ausgeschieden war, fiel auf, dass es die HUB versäumt hatte, eine nach dem Berliner Datenschutzgesetz zwingend vorgeschriebene Stellvertretung zu regeln. Anfang 2009 schloss eine neue behördliche Datenschutzbeauftragte die entstandene Lücke. Jedoch blieb es dabei, dass die Bestellung einer Stellvertretung versäumt wurde. Im September informierte uns der Gesamtpersonalrat der HUB, dass die Datenschutzbeauftragte vorübergehend nicht im Dienst sei und nunmehr mangels einer Stellvertretung die Funktion nicht wahrgenommen würde, was dazu führe, dass aktuelle Mitbestimmungsvorgänge, die den Umgang mit personenbezogenen Daten berühren, mangels Mitwirkung des behördlichen Datenschutzes nicht bearbeitet werden könnten. Unsere Aufforderung an den Präsidenten der HUB, endlich die Stellvertretung für die behördliche Datenschutzbeauftragte zu regeln, blieb zunächst unbeantwortet, sodass der Verstoß gegen § 19 a Abs. 1 BlnDSG förmlich beanstandet wurde. Das Beanstandungsschreiben kreuzte sich mit der Mitteilung des Präsidenten, dass ein Ausschreibungsverfahren im zweiten Versuch erfolgreich gewesen, ein stellvertretender Datenschutzbeauftragter eingestellt worden sei und seinen Dienst am 1. Dezember angetreten habe. Nachdem auf besondere Aufforderung das Bestellschreiben zugesandt wurde und uns der Name und die Kontaktdaten der bestellten Person bekannt gegeben wurden, war der Beanstandung abgeholfen worden.

Über den Umgang der **Freien Universität Berlin (FUB)** mit ihrer Datenschutzbeauftragten und mit uns haben wir im Vorjahr berichtet[156]. Unsere Beanstandungen führten zunächst dazu, dass ein stellvertretender Datenschutzbeauftragter benannt wurde, indem für die behördliche Datenschutzbeauftragte der FUB eine gegenseitige Stellvertretung mit dem behördlichen Datenschutzbeauftragten des Botanischen Gartens festgelegt worden ist. Für eine gewisse Zeit schien es, dass hinsichtlich der Versuche der FUB-Leitung, die Datenschutzbeauftragte in ihrer Arbeit zu behindern, eine gewisse Ruhe eingekehrt wäre. Als Rückfall ist zu bewerten, dass für die behördliche Datenschutzbeauftragte jetzt ein Umzug angeordnet wurde. Zunächst wurden ihr weit abseits des FU-Campus Räume zugewiesen, sodass ein großer Teil ihrer ohnehin zu knapp bemessenen Arbeitszeit in Wegezeiten vergeudet worden wäre. Dann fiel die Entscheidung für am Campus gelegene, aber unangemessen kleine Räume, in der sie die umfangreichen Materialien und Vorgänge nicht unterbringen kann, die sich in einem Jahrzehnt Datenschutzarbeit angesammelt haben. Immerhin ist sie bei der Einführung von IT-Verfahren an der FUB zu beteiligen und kontrolliert derzeit mehr als 240 IT-Verfahren der FUB. Ihr Protest wurde von einem dafür Verantwortlichen damit kommentiert, dass sie eigentlich nur Anspruch auf acht Quadratmeter habe. Wir haben Verständnis dafür, dass die behördliche Datenschutzbeauftragte die Umzugsposse als eine bewusste Behinderung ihrer Arbeit einstuft. Dies zeigt zweierlei: Selbst leitende Beschäftigte der FUB machen sich keine Vorstellung von dem Amt der behördlichen Datenschutzbeauftragten einer großen Universität und ihren Unterstützungsansprüchen. Nach unserer Intervention wurde ein Raumtausch veranlasst, mit dem sie einen deutlich größeren Raum erhält. Ob dies ausreicht, bleibt abzuwarten.

Zwar scheinen demgegenüber die Verhältnisse an der **Technischen Universität Berlin (TUB)** vergleichsweise geordnet zu sein, da die behördliche Datenschutzbeauftragte, die Arbeitnehmervertretung oder andere Beteiligte bisher keinen Anlass sahen, Beschwerden nach außen zu tragen. Bei der Bestimmung der Stellvertretung erlaubt sich die TUB eine Besonderheit, indem sie das Amt des Stellvertreters an ein anderes Amt und nicht an eine Person knüpft. Vertreterin oder Vertreter ist die jeweilige Leitung des Referats für Angelegenheiten der akademischen Selbstverwaltung. Zum Zeitpunkt der Umfrage war

156 JB 2008, 10.1.5

diese Stelle unbesetzt, und somit gab es auch keine Stellvertretung im Datenschutz. Hinzu kommt, dass eine solche Regelung im Widerspruch zum Berliner Datenschutzgesetz steht, wonach eine Person zu bestellen ist, die auch nur unter restriktiven Voraussetzungen aus ihrem Amt entlassen werden kann.

Die Bestellung einer Stellvertretung für den behördlichen Datenschutzbeauftragten haben auch die **Hochschule für Technik und Wirtschaft** und die **Hochschule für Musik** bisher versäumt. Bei der **Universität der Künste und den übrigen Fachhochschulen** ergab die Umfrage, dass zumindest hinsichtlich der Bestellungen den gesetzlichen Vorgaben entsprochen wurde.

Zu den übrigen Fragestellungen zu Status, Rechten und Pflichten der oder des behördlichen Datenschutzbeauftragten an den Hochschulen gelangten wir zu folgenden Ergebnissen:

- In keiner Hochschule sind die Rechte und Pflichten der Datenschutzbeauftragten schriftlich festgehalten und den Beschäftigten verbindlich zur Kenntnis gegeben worden. Wenn die Datenschutzbeauftragten lediglich in Telefonverzeichnissen, Studienführern und irgendwo im eigenen Internetangebot erwähnt werden, ist nicht gewährleistet, dass auch wirklich alle Hochschulangehörigen davon Kenntnis erlangen. Diese sollten wissen, bei wem, wo und wann sie in Datenschutzfragen Rat erhalten können.
- Bei den drei großen Universitäten (HUB, FUB, TUB) steht den Datenschutzbeauftragten die volle Arbeitszeit für ihre umfangreiche Tätigkeit zu. Das mag im ersten Augenblick ausreichend erscheinen. Doch bei der Menge der zu verarbeitenden personenbezogenen Daten in Personal- und Studierendenverwaltung, in Prüfungsangelegenheiten und in Forschung und Lehre sowie bei der Vielzahl und Komplexität der eingesetzten informationstechnischen Systeme dürfte eine solche Stellenausstattung unterdimensioniert sein, vor allem dann, wenn wie z. B. bei der Datenschutzbeauftragten der FUB nicht einmal Sekretariatsdienstleistungen bereitgestellt werden. Hilfreich wäre die Benennung von Ansprechpartnern in den wichtigsten Universitätseinrichtungen. Die oder der Datenschutzbeauftragte könnte dann eine federführende Rolle übernehmen und sich regelmäßig mit den Ansprechpartnern in Datenschutzbelangen des Hauses abstimmen.

- Anders sieht es bezüglich der Arbeitszeit für die Datenschutzaufgaben in den übrigen Hochschulen aus. Hier wurden bei der Angabe nach der zur Verfügung gestellten Zeit Stundenzahlen genannt, die bei weitem nicht ausreichen. Wie sollen Hochschul-Datenschutzbeauftragte, die ihre Aufgaben einigermaßen zufriedenstellend erfüllen wollen, mit einer Wochenstunde bzw. 10 % der Semesterwochenstunden auskommen? Vielen Datenschutzbeauftragten werden nur Zeiten nach Bedarf zugestanden. Dies bedeutet nichts anderes, als dass sie die Aufgaben als Datenschutzbeauftragte nur neben ihrer sonstigen Vollzeittätigkeit zu bewältigen haben. Zeiten für die eigene Fortbildung und für die Schulung der Mitarbeiterinnen und Mitarbeiter sind gar nicht berücksichtigt. Wir gehen davon aus, dass je nach Größe und Komplexität einer Hochschule, die nicht zu den drei großen Universitäten gehört, 50-100 % der Arbeitszeit für die Aufgaben als Datenschutzbeauftragte benötigt werden.
- Behördliche Datenschutzbeauftragte können sich nach § 19 a Abs. 2 Satz 4 BlnDSG in Angelegenheiten des Datenschutzes unmittelbar an den Leiter ihrer Behörde wenden. Dies wird ihnen bei einigen Hochschulen nur bedingt zugestanden. Es ist jedoch akzeptabel, wenn anstelle der Präsidentin oder des Präsidenten einer Hochschule ein anderes Mitglied des Präsidiums als ständiger Ansprechpartner benannt wird, sofern dabei sichergestellt werden kann, dass die Leitung der Behörde, also die Präsidentin oder der Präsident, der alleinigen Verantwortung für die Einhaltung der Bestimmungen des Datenschutzes gerecht werden kann.
- Die Pflicht der Hochschulen zur Unterstützung der oder des Datenschutzbeauftragten betrifft die Bereitstellung von Arbeits- und Reisemitteln und die Bereitstellung von Räumlichkeiten, die neben den Ansprüchen auf die Ausstattung eines Arbeitsplatzes den Bedürfnissen einer vertraulichen Aktenhaltung und der vertraulichen Beratung von Betroffenen (Beschäftigten, Studenten) genügen. Für Schreibarbeiten und für Recherche- und Kontrollmaßnahmen ist eine angemessene informationstechnische Ausstattung nötig. Mit Ausnahme der Hochschule für Musik sind alle Hochschulen ihrer Unterstützungspflicht bei der Raum- und PC-Beschaffung nachgekommen.
- Nach eigenem Bekunden stellen die Hochschulen ihren Datenschutzbeauftragten ausreichend finanzielle Mittel für ihre Tätigkeit zur Verfügung. Für Kosten, die mit der Amtsführung zusammenhängen, sind jedoch bis auf

eine Ausnahme keine eigenen Budgets eingerichtet. Die HUB hat als einzige einen eigenen Haushaltstitel eingerichtet, jedoch nur für Literaturbeschaffung. Die Datenschutzbeauftragte der FUB verfügt über ein Budget für Fachbücher und Dienstreisen. Neben Fachbüchern und Gesetzestexten benötigen die Datenschutzbeauftragten weitere Mittel für Aus- und Fortbildungsmaßnahmen, den Besuch von kostenpflichtigen Veranstaltungen mit Datenschutzbezug, für Dienstreisen zu Veranstaltungen und Fortbildungsmaßnahmen, aber auch für die Erstellung von Informationsmaterial.

- Die behördlichen Datenschutzbeauftragten sind über neue automatisierte Datenverarbeitungen rechtzeitig zu unterrichten, insbesondere wenn eine Vorabkontrolle durchzuführen ist. Die Unterrichtung der behördlichen Datenschutzbeauftragten über geplante bzw. neu einzuführende Projekte oder Verfahren verläuft in den befragten Stellen unterschiedlich. In der Regel informieren die IT- oder DV-Organisations-Stellen die Datenschutzbeauftragten. Diese sind meist auch zuständig für die Erstellung und Weiterleitung der Dateibeschreibungen nach § 19 Abs. 2 BlnDSG. Aufgrund der Eigenverantwortlichkeit vieler Hochschulbereiche werden die Datenschutzbeauftragten auch von den Bereichsleitungen über Neuerungen in Kenntnis gesetzt.

Die personelle Ausstattung der Datenschutzbeauftragten der Hochschulen, d. h. die ihnen zugestandene Arbeitszeit bzw. die personelle Unterstützung, ist fast immer unzureichend, zumal einige Hochschulen nicht einmal ihren gesetzlichen Verpflichtungen nachkommen. Die im BlnDSG postulierte Unterstützungspflicht wird dagegen im Wesentlichen eingehalten, wenngleich inakzeptable Ausnahmefälle festgestellt wurden. Die rechtzeitige Unterrichtung über geplante IT-Projekte und neue IT-Verfahren findet nicht immer statt, sodass eine datenschutzgerechte Gestaltung fraglich ist.

### 12.4.2 Gesprächskreis der bezirklichen Datenschutzbeauftragten

Die im regelmäßigen Gesprächskreis der bezirklichen Datenschutzbeauftragten behandelten Probleme sind themenbezogen an anderen Stellen des Berichts abgehandelt worden. Herauszuheben ist jedoch, dass sich im letzten Jahr eine

Arbeitsgruppe[157] herausgebildet hat, die im Wesentlichen aus jenen bezirklichen Datenschutzbeauftragten besteht, denen für ihre Aufgaben die volle Arbeitszeit zur Verfügung steht.

Inzwischen hat sich die Arbeitsgruppe mit der Anfertigung von Muster-Dateibeschreibungen für die bezirklichen Verfahren MUSIKA (Musikschulen) und AUTISTA (Standesämter) befasst. Weitere Musterbeschreibungen sind für SpDi32 (Sozialpsychiatrischer Dienst), EVASTA (Einbürgerung), OPENPROSOZ (Sozialhilfe) und BAIVI iP (Lebensmittel- und Veterinärüberwachung) geplant. Für die Zukunft ist vorgesehen, dass die Arbeitsgruppe das gemeinsame Auftreten der bezirklichen Datenschutzbeauftragten im Intranet bzw. Internet vorbereitet. Dazu soll ein Konzept erarbeitet werden, das berücksichtigt, dass einige Datenschutzbeauftragte bereits eigene Internetangebote entwickelt haben und andere Datenschutzbeauftragte in einem gemeinsamen Internet-Auftritt eine Überschreitung ihrer Befugnisse sehen. Das Konzept soll dann die Grundlage für weitere Diskussionen im Gesprächskreis werden.

### 12.4.3 Workshop der Datenschutzbeauftragten der Gerichte

Der Workshop der Datenschutzbeauftragten der Gerichte befasst sich mit der Abstimmung zu Fragen, die in einzelnen Gerichten aufkommen, aber für alle Gerichte von Interesse sein können.

Hintergrund einer Anfrage bei dem behördlichen Datenschutzbeauftragten eines Amtsgerichts war ein Fall, bei dem die Präsidentin des Kammergerichts das für die Betreuung des Verfahrens AULAK (Automation im Landgericht, in den Amtsgerichten und im Kammergericht) zuständige IT-Dienstleistungszentrum Berlin beauftragt hatte, die Home-Verzeichnisse ihrer Bediensteten zu prüfen, um festzustellen, wer aus dem Intra- bzw. Internet Dateien mit den Endungen .jpg, .exe bzw. .com (also im Wesentlichen Musik-, Programm- und Bilddateien) in das eigene Home-Verzeichnis unerlaubt heruntergeladen hat. Ein direkter Zugriff auf die Home-Verzeichnisse einzelner Bediensteter soll jedoch nicht erfolgt sein. Generell ging es um die Frage, ob Vorgesetzte befugt sind,

157 JB 2008,13.2.1

die eigentlich als privater Bereich geltenden Home-Verzeichnisse der Beschäftigten zu überprüfen. Im Ergebnis gelten in den Gerichten die Regelungen, die der Gesamtpersonalrat ausgehandelt hat: Die private Nutzung dienstlicher Personalcomputer ist generell nicht erlaubt, sodass dem Dienstherrn ein Kontrollrecht unter Beachtung des Verhältnismäßigkeitsprinzips zusteht.

Weiter ging es um die Frage, ob im Rahmen der Tätigkeit im Amtsgericht erlangte Daten bzw. Erkenntnisse an dritte Stellen weitergegeben werden dürfen. So war zu klären, ob Jobcenter Auskünfte aus dem Amtsgericht erhalten dürfen, wenn sie annehmen, dass Antragstellende für das Arbeitslosengeld II Angaben zu ihren Einkünften unterlassen haben. Dabei handelt es sich um die Offenbarung bzw. Weiterleitung personenbezogener Daten an dritte Stellen unter Missachtung der Zweckbindung. Solche Daten und Erkenntnisse aus der Arbeit eines Amtsgerichts dürfen deshalb in der Regel nicht übermittelt werden. Personenbezogene Daten dürfen aber zur Abwehr von Straftaten an die Polizei oder die Staatsanwaltschaft weitergegeben werden, wenn bei Beantragung von Leistungen offensichtlich falsche Angaben gemacht werden. Liegt dagegen nur ein Bußgeldtatbestand vor, dürfen die Informationen nur an die ARGE, also an die für Ordnungswidrigkeiten zuständige Verwaltungsbehörde, und nicht an die Jobcenter übermittelt werden. Das ist etwa dann der Fall, wenn die Leistungsempfängerin oder der Leistungsempfänger Änderungen hinsichtlich der Leistungsberechtigung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitgeteilt hat.

# 13. Telekommunikation und Medien

## 13.1 Soziale Netzwerke



Große Aufmerksamkeit erregte der unberechtigte Download von Daten hunderttausender Nutzerinnen und Nutzer aus dem SchülerVZ. Mehreren Eindringlingen war es unabhängig voneinander gelungen, riesige Datenbestände wegen unzureichender Sicherungen gegen solche automatisierten Downloads, aber auch wegen einer fehlerhaft implementierten Suchfunktion herunterzuladen. In einem Einzelfall gab es ca. 1,6 Millionen Betroffene. Bemerkenswert ist, dass es sich nicht um Hacker-Angriffe von außen handelte. Die Täter machten als angemeldete Nutzerinnen und Nutzer lediglich von den in der Plattform zur Verfügung gestellten Funktionen Gebrauch.

Das Unternehmen hat uns frühzeitig informiert und uns regelmäßig über die getroffenen Maßnahmen auf dem Laufenden gehalten. Insgesamt ist festzustellen, dass die durch die VZ Netzwerke Ltd. getroffenen Gegenmaßnahmen inzwischen ausreichend sind. Zwar waren keine besonders schutzwürdigen Daten betroffen, aber nur deshalb, weil die von den Tätern eingesetzten technischen Werkzeuge nur einen beschränkten Bestand an Datenfeldern „abgegriffen" haben. Versiertere Täter hätten zumindest bis Mitte 2009 weitere Daten aus den Profilen zahlreicher Nutzenden des SchülerVZ herunterladen können.

In einem Einzelfall sind allerdings auch Daten in großem Umfang massenhaft heruntergeladen worden, die aufgrund der Privatsphäre-Einstellungen der Nutzenden für die Täter überhaupt nicht hätten sichtbar sein dürfen. Dies beruhte auf einer fehlerhaft implementierten Suchfunktion. Auf diese Fehler hatten wir im Anschluss an eine Studie[158] bereits im Herbst 2008 hingewiesen. Das Unternehmen hat uns zwar berichtet, diesen Fehler beseitigt zu haben, allerdings – wie sich nun herausgestellt hat – nicht vollständig. Dies geschah erst

158 Fraunhofer-Institut für Sichere Informationstechnologie SIT: Privatsphärenschutz in Soziale-Netzwerke-Plattformen, September 2008

nach Bekanntwerden des oben geschilderten Vorfalls. Aufgrund der unklaren Sach- und Rechtslage haben wir in diesem Fall davon abgesehen, ein Bußgeld zu verhängen. Wir erwarten allerdings von dem Unternehmen, dass derartige Fehler zukünftig umgehend und sorgfältiger behoben werden.

Unabhängig davon haben wir den Anbieter darauf hingewiesen, dass dieser Vorfall zum Anlass genommen werden muss, den Schutz der Privatsphäre der Nutzerinnen und Nutzer bei den verschiedenen Plattformen des Unternehmens weiter zu stärken. Im Einzelnen betrifft dies folgende Bereiche:

- Empfehlung an die Nutzenden, die Profile unter Pseudonym (Spitznamen) statt unter ihrem Klarnamen zu führen,
- restriktivere Standardeinstellungen für die Privatsphäre in neu angelegten Nutzerprofilen (dies war bei SchülerVZ schon umgesetzt, unterdessen sind aufgrund unserer Intervention auch die Einstellungen bei StudiVZ und MeinVZ entsprechend verändert worden),
- deutlicheren Hinweis auf verbleibende Sicherheitsrisiken im Rahmen der Nutzerinformation.

Bei den Betroffenen (insbesondere Jugendlichen) besteht nach wie vor großer Beratungsbedarf im Hinblick auf den Schutz der Privatsphäre in sozialen Netzwerken. Wir haben daher mit dem Berliner Landesprogramm Jugendnetz-Berlin eine Broschüre herausgegeben, die Tipps für Jugendliche zum Datenschutz in sozialen Netzwerken enthält[159].

**Bei der Veröffentlichung personenbezogener Daten in sozialen Netzwerken besteht immer die Gefahr der zweckfremden Nutzung dieser Daten durch Dritte. Nutzende sollten den Umfang der Daten in sozialen Netzwerken deshalb auf ein Minimum beschränken und anstelle des wirklichen Namens ein Pseudonym verwenden.**

159 http://www.datenschutz-berlin.de/content/themen-a-z/internet/soziale-netzwerke-und-datenschutz

## 13.2 Europäische Union: Novellierung der Telekommunikations-Datenschutzrichtlinie

Die Überarbeitung des Regulierungsrahmens für elektronische Kommunikationsnetze und -dienste in der Europäischen Union ist abgeschlossen[160]. Das Richtlinien-Paket[161] enthält u. a. Änderungen der „Telekommunikations-Datenschutzrichtlinie". Es gibt im Wesentlichen folgende Neuerungen, die zu einer Verbesserung des Datenschutzes führen können:

- Bei einer Verletzung des Schutzes personenbezogener Daten sind Betreiber von öffentlich zugänglichen elektronischen Kommunikationsdiensten verpflichtet, unverzüglich die zuständige nationale Behörde zu unterrichten. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten diese selbst oder Teilnehmende oder andere Personen in ihrer Privatsphäre beeinträchtigt werden, muss der Betreiber auch die Betroffenen unverzüglich über die Verletzung benachrichtigen[162]. Diese Benachrichtigungspflicht entfällt, wenn der Betreiber zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat, dass er geeignete Schutzmaßnahmen getroffen hat und sie auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Die Aufsichtsbehörden können darüber hinaus eine Benachrichtigung der Teilnehmenden im Einzelfall anordnen. Die Kommission kann in einem festgelegten Verfahren technische Durchführungsmaßnahmen in Bezug auf Umstände, Form und Verfahren der vorgeschriebenen Informationen und Benachrichtigungen erlassen[163].
- Die Speicherung von Informationen oder der Zugriff auf Informationen (betrifft u. a. auch Cookies), die bereits im Endgerät einer oder eines Teil-

160 Zuletzt JB 2008, 14.1

161 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18. Dezember 2009, S. 11

162 Art. 4 Abs. 3 Richtlinie 2002/58/EG

163 Art. 4 Abs. 5 Richtlinie 2002/58/EG

nehmenden oder Nutzenden gespeichert sind, ist nur mit deren oder dessen Einwilligung gestattet[164]. Ein Widerspruch ist nicht mehr ausreichend.

- Die Mitgliedstaaten sollen sicherstellen, dass bei Verstößen gegen die Regelungen über unerbetene Nachrichten natürliche oder juristische Personen, aber auch die Anbieter elektronischer Kommunikationsdienste gegen solche Verstöße gerichtlich vorgehen können[165].
- Generell werden die Mitgliedstaaten zur Festlegung von (ggf. auch strafrechtlichen) Sanktionen verpflichtet, die bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung der Richtlinie zu verhängen sind. Diese müssen wirksam, verhältnismäßig und abschreckend sein[166].

Die Art. 29-Datenschutzgruppe hatte im Februar eine erneute Stellungnahme zu den damaligen Vorschlägen zur Änderung der Telekommunikations-Datenschutzrichtlinie abgegeben[167]. Darin wiederholt sie ihre Empfehlung, die Verpflichtung zur Meldung von Verletzungen des Schutzes personenbezogener Daten auch auf Dienste der Informationsgesellschaft auszuweiten, da diese Dienste eine immer wichtigere Rolle im täglichen Leben der europäischen Bürgerinnen und Bürger spielen und wachsende Mengen an personenbezogenen Daten verarbeiten. Allerdings hat der europäische – anders als der deutsche – Gesetzgeber diesen Vorschlag nicht übernommen[168]. Die Gruppe sprach sich darüber hinaus eindeutig gegen die damaligen Planungen aus, bei der Speicherung von personenbezogenen Daten auf Endgeräten der Nutzenden und dem Zugriff darauf auch Browser-Einstellungen als eine vorherige Einwilligung gelten zu lassen. Dessen ungeachtet hat sich der europäische Gesetzgeber entschlossen, diese Möglichkeit zuzulassen[169].

164 Art. 5 Abs. 3 Richtlinie 2002/58/EG

165 Art. 13 Abs. 6 Richtlinie 2002/58/EG

166 Art. 15 a Abs. 1 Richtlinie 2002/58/EG

167 Stellungnahme 1/2009 vom 10. Februar 2009 (WP 159) über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation)

168 Nach deutschem Recht sind alle privaten Datenverarbeiter zur Information der Aufsichtsbehörden sowie der Nutzerinnen und Nutzer verpflichtet (§ 42 a BDSG), vgl. dazu 2.1

169 Erwägungsgrund (66) der Richtlinie 2009/136/EG, vgl. Fn. 161

Erfreulicherweise wurde die Möglichkeit zur Verarbeitung von Verkehrsdaten durch jedermann zum Zweck der Gewährleistung von Datensicherheit nicht eingeführt[170]. Es bleibt dabei, dass diese Befugnisse nur Anbietern elektronischer Kommunikationsdienste zur Sicherung ihrer eigenen Dienste zustehen.

## 13.3 Änderungen im Telekommunikations- und Telemedienrecht

Das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) wurden geändert.

- Die Regelungen zur Übertragung von Ortungsinformationen im Mobilfunk an Dritte wurden verschärft, um das heimliche Ausspionieren des Standortes von Handynutzenden zu erschweren. Hierzu müssen Teilnehmende ihre Einwilligung ausdrücklich, gesondert und schriftlich erteilen. Außerdem ist der Diensteanbieter verpflichtet, Teilnehmende nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren[171].
- Auch Anbieter von Telemedien nach dem TMG unterliegen Verpflichtungen zur Information der Aufsichtsbehörden bzw. der Betroffenen, wenn bei ihnen gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Nutzerin oder des Nutzers drohen[172].

170 JB 2008, 14.1
171 § 95 Abs. 1 TKG
172 § 15 a TMG i.V. m. § 42 a BDSG

## 13.4 Bewertung von Lehrkräften an Hochschulen im Internet



Der Bundesgerichtshof (BGH) hat erstmals über die Zulässigkeit einer Lehrerbewertung im Internet entschieden[173]. Er hat unsere Auffassung bestätigt, dass die Verarbeitung personenbezogener Daten der Bewerteten nach § 29 BDSG zu beurteilen ist und nicht auf das sog. Medienprivileg des § 41 BDSG gestützt werden kann. Der BGH hat allerdings die Veröffentlichung der personenbezogenen Daten von Lehrerinnen und Lehrern auf der Bewertungsplattform für rechtmäßig erachtet und dem Recht auf Meinungsfreiheit der Bewertenden höheres Gewicht eingeräumt als dem Schutz des informationellen Selbstbestimmungsrechts der Bewerteten. Wir haben erhebliche Zweifel an dieser Rechtsgüterabwägung. Auch ist nicht nachvollziehbar, warum für das nach § 29 Abs. 2 Satz 1 Nr. 1 BDSG erforderliche berechtigte Interesse zum Abruf von Bewertungen schon die Kenntnis des Namens und der Schule eines von der Bewertung Betroffenen genügt. Die vor dem BGH unterlegene Lehrerin hat Verfassungsbeschwerde angekündigt.

Unabhängig davon, ob man die Rechtsgüterabwägung des BGH teilt, lassen sich folgende Gestaltungsanforderungen an Bewertungsportale ableiten:

- Sowohl die Einmeldung von Bewertungen als auch ihr Abruf sind nur innerhalb einer geschlossenen Benutzergruppe mit vorheriger Registrierung der einmeldenden bzw. abrufenden Personen zulässig. Gerade Bewertungsergebnisse dürfen nicht ohne vorherige Registrierung frei im Internet zugänglich sein.
- Eine Personensuche über externe Suchmaschinen ist auszuschließen, soweit keine Einwilligung der Betroffenen vorliegt.
- Auf der Plattform selbst dürfen keine Einzelergebnisse, sondern nur Durchschnittswerte angezeigt werden.
- Es dürfen keine „Freitextfelder“ für Bewertungen verwendet werden.

173 Urteil vom 23. Juni 2009 – VI ZR 196/08

- Auch für registrierte Nutzerinnen und Nutzer ist die Möglichkeit zum Abruf von Bewertungen zu begrenzen (bei dem Lehrerbewertungsportal z. B. auf eine bestimmte Schule).
- Bewertungen müssen innerhalb einer angemessenen Frist gelöscht werden (bei dem Lehrerbewertungsportal nach zwölf Monaten).

Unser Bußgeldverfahren gegen den Anbieter einer Bewertungsplattform für Lehrveranstaltungen an deutschen, österreichischen und schweizerischen Hochschulen[174] ist noch nicht abgeschlossen.

Die gesetzlichen Regelungen sind nicht ausreichend, um das informationelle Selbstbestimmungsrecht der Bewerteten zu schützen. Bislang haben diese keine Handhabe gegen die weltweite Veröffentlichung von Bewertungen in Bewertungsportalen. Zumindest ein Widerspruchsrecht sollte den Betroffenen eingeräumt werden.

## 13.5 Verarbeitung von Nutzungsdaten durch Host-Provider

Viele Webangebote speichern für statistische Zwecke, von welchen Nutzenden eine Webseite abgerufen wurde. Da dies ihre Überwachung ermöglicht, ist diese Datenverarbeitung in personenbeziehbarer Form unzulässig. Mit einem Host-Provider haben wir ein Verfahren entwickelt, das seinen Kunden die Erstellung von Statistiken auf eine datensparsame Weise ermöglicht[175].

Jeder Internet-Rechner muss, um Dienste des Internets nutzen zu können, über eine eindeutige Adresse verfügen, die sog. Internet-Protokoll- oder IP-Adresse. Unter dieser Adresse wird z. B. ein Internetangebot abgerufen, d. h. der Browser sendet ein Datenpaket mit der Anfrage der gewünschten Web-

174 JB 2007, 12.2.3

175 Ein Host-Provider vermietet Speicherplatz auf seinen Webservern, sodass seine Kunden mit geringem Aufwand eigene Webangebote im Internet anbieten können.

seite an die IP-Adresse des Webservers und dieser sendet die Webseite an die im Datenpaket enthaltene IP-Adresse des anfragenden Rechners zurück. Die Angabe „IP-Adresse“ ist dafür notwendig, andernfalls würde man die angefragte Webseite nicht erhalten können. Zugleich ist die IP-Adresse jedoch ein personenbeziehbares Datum, da zumindest der Internetzugangsprovider weiß und nach den Vorgaben der Vorratsdatenspeicherung für sechs Monate protokollieren muss, welcher seiner Kundinnen und Kunden in einem Zeitraum eine IP-Adresse benutzt hat. Bürorechner nutzen meist sogar eine fest zugeordnete IP-Adresse.

Das Telemediengesetz (TMG) schreibt vor, dass personenbezogene Daten nach dem Ende der Verbindung zu löschen sind, falls sie nicht für Abrechnungszwecke benötigt werden[176]. Wir haben jedoch festgestellt, dass viele Webangebote jeden Abruf einer Webseite in einem sog. Server-Logfile protokollieren und dabei rechtswidrig auch die vollständige IP-Adresse speichern. Die Gründe für das Erstellen von Server-Logfiles sind vielfältig: Man möchte erfahren, wie häufig welche Teile des Angebotes abgerufen wurden, wie gut oder schlecht die Nutzenden mit dem Angebot zurechtkommen (Stichwort: Abbruchraten) oder aus welchen Ländern bzw. Regionen die Nutzenden kommen (Stichwort: Geolokalisierung). Dies sind legitime Ziele, solange dabei keine personenbezogenen Daten gespeichert oder über das Verbindungsende hinaus verarbeitet werden. Für die Abrufhäufigkeit der einzelnen Webseiten genügt es, wenn im Logfile nur vermerkt würde, welche Webseite zu einem bestimmten Zeitpunkt abgerufen wurde. Eine Geolokalisierung kann anhand der IP-Adresse stattfinden, da Datenbanken existieren, die die IP-Adressen bestimmten geographischen Regionen zuordnen. Allerdings ist die Nutzung der vollständigen IP-Adresse für die Geolokalisierung nicht zulässig, insbesondere dann nicht, wenn dies dazu führt, dass die IP-Adresse noch nach Verbindungsende (im Logfile) gespeichert bleibt. Jedoch erfolgt gegenwärtig die Geolokalisierung nur relativ grob (und ist daher unproblematisch) – bei Großstädten ist bestenfalls der Stadtteil ermittelbar. Deswegen genügt es, wenn die Geolokalisierung anhand einer um die letzten Stellen gekürzten IP-Adresse erfolgt. Werden ausreichend viele Stellen der IP-Adresse gestrichen, ist die Speicherung zulässig, da die einzelnen Nutzenden nicht mehr identifiziert werden können, es sich folglich nicht mehr um ein personenbezogenes Datum handelt.

176 § 15 Abs. 4 TMG

Ein großer Host-Provider, der es seinen Kunden ermöglicht, eigene Webangebote auf den Servern des Providers zu betreiben, hat aufgrund unserer Kritik an der bisherigen Speicherpraxis ein datensparsames Verfahren entwickelt, das den Anforderungen des Datenschutzes genügt und zugleich die gewünschten statistischen Analysen ermöglicht. Kern des Verfahrens ist

- die Kürzung der IP-Adresse, sodass jede protokollierte Anfrage von ca. 500 verschiedenen IP-Adressen (d. h. ca. 500 verschiedenen Nutzenden) hätte gesendet worden sein können und
- das Berechnen und Abspeichern einer temporären Kennung anstelle der vollständigen IP-Adresse im Logfile, um für einen begrenzten Zeitraum die Anfragen desselben Nutzenden einander zuordnen zu können.

Das von einem Berliner Host-Provider aufgrund unserer Kritik entwickelte Verfahren für eine Nutzungsstatistik stellt einen gelungenen Kompromiss zwischen den Interessen der Betreiber von Webangeboten und dem Schutz der Privatsphäre der Nutzenden dar.

## 13.6 Datenschutzkonforme Web-Reichweitenmessung

Viele Anbieter von Telemedien analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzenden. Zur Erstellung solcher Nutzungsprofile verwenden die Anbieter eine Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden (z. B. Google Analytics). Bei der Ausgestaltung dieser Angebote zur Reichweitenmessung ist das Datenschutzrecht zu beachten, was häufig nicht geschieht. Der Düsseldorfer Kreis sah sich daher veranlasst, darauf hinzuweisen, dass bei der Erstellung von Nutzungsprofilen durch Anbieter von Telemedien das Telemediengesetz (TMG) zu beachten ist, und hat hierfür Anforderungen formuliert[177].

177 Beschluss vom 26./27. November 2009: Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, Dokumentenband 2009, S. 30

## 13.7 Das Recht am eigenen Bild



**Glück gehabt oder Datenpech?**

Ein bekanntes Berliner Boulevard-Blatt veröffentlichte in seiner Wochenendausgabe mit einer gewissen Regelmäßigkeit fotografierte Abbildungen mehrerer Personen in einem mehr oder weniger bestimmbaren räumlichen Zusammenhang (z. B. auf einer stark besuchten Geschäftsstraße). Unter der Überschrift „Haben Sie sich erkannt?“ wurde versprochen, derjenigen Person, die auf diesem veröffentlichen Foto durch eine Markierung besonders gekennzeichnet war, 100 Euro auszuzahlen, wenn diese Person sich „Ihren Gewinn von Montag bis zum nächsten Freitag“ im Kundencenter der Zeitung abholt. Dazu wurde verlangt: „Bitte vergessen Sie Ihren Personalausweis nicht – der Rechtsweg ist ausgeschlossen.“ Habe niemand das Geld abgeholt, so hieß es weiter, komme das Geld in einen Jackpot mit der Maßgabe: „Der nächste Gewinner bekommt 200 Euro oder sogar noch mehr. Diesmal war der Fotograf auf der Karl-Marx-Straße in Neukölln unterwegs. Nächsten Donnerstag wird er in Tegel einen Gewinner suchen.“

Abbildungen von Personen – auch wenn sie nicht mit Namen versehen wurden – sind personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG. Die Abbildungen waren nicht als Presseerzeugnis im Sinne des § 41 Abs. 1 BDSG anzusehen, weil die Verarbeitung der Daten bzw. Abbildungen nicht zu journalistisch-redaktionellen Zwecken, sondern lediglich zum Zweck einer Auslobung zugunsten einer abgebildeten und markierten Person erfolgte. Nach § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten (dazu gehört auch die Veröffentlichung und Verbreitung) nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder die Betroffenen eingewilligt haben.

Obwohl uns zu dieser serienmäßigen Auslobung keine Beschwerden vorlagen, haben wir die Auslobung überprüft und der Zeitung unsere Rechtsauffassung zur Beachtung empfohlen. Wir haben festgestellt (das ergab sich ja bereits aus der Auslobung), dass ein vorheriges Einverständnis der abgebildeten Personen nicht vorlag und sie weder als Personen der Zeitgeschichte gelten noch sonst irgendwie einer publizistischen Berichterstattung zugeordnet werden konnten. Deshalb war schon die Abbildung derjenigen Personen, die nicht als Gewinner markiert waren, in jedem Fall unzulässig: Deren Abbildung konnte nicht

einmal nachträglich durch die Abholung eines „Gewinns“ legitimiert werden; denn Bildnisse dürfen nach § 22 Kunsturhebergesetz (KunstUrhG) nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn die abgebildete Person dafür, dass sie sich abbilden lässt, eine Entlohnung erhält. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht. Die Betroffenen sind auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Diesen gesetzlichen Anforderungen entsprach die geschilderte Auslobung offensichtlich nicht. Eine nachträgliche Zustimmung ist im Gesetz nicht vorgesehen. Sie kommt also schon dann nicht in Betracht, wenn sich die abgebildete Person nicht meldet. Hinzu kam, dass auf dem publizierten Bild auch Personen „scharf“ abgebildet worden waren, die nicht Gewinner werden sollten, deren nachträgliche Zustimmung also gar nicht gewollt war. Publizistische Zwecke, die eine unfreiwillige Verbreitung solcher Abbildungen hätten rechtfertigen können, waren nicht erkennbar. Wir haben die Zeitung darauf hingewiesen, dass etwaige Beschwerdeführerinnen und -führer wegen der Verbreitung derartiger Abbildungen einen Strafantrag nach § 33 KunstUrhG stellen könnten. Insbesondere aber haben wir dringend davon abgeraten, die „Nichtgewinner“ individuell erkennbar abzubilden.

Das Kunsturhebergesetz geht davon aus, dass die Verbreitung einer Abbildung, soweit sie nicht aus anderen rechtlichen Gründen zulässig ist, im Zweifel dann als genehmigt gilt, wenn die abgebildete Person eine Entlohnung (Gewinn) erhielt. Die ungefragte Veröffentlichung der Fotos von Personen, die entweder nichts gewinnen oder den Gewinn ablehnen, kann als Verletzung des Rechts am eigenen Bild strafbar sein.

## 13.8 Neues von Google Street View

Der Dienst Google Street View des US-Konzerns Google bietet den Nutzerinnen und Nutzern die Möglichkeit eines virtuellen Spaziergangs aus der Perspektive einer Fußgängerin oder eines Fußgängers. Das dafür von Google

zur Verfügung gestellte Bildmaterial ist enorm angewachsen und für bestimmte Länder (USA, Frankreich) bereits auf der Internetseite verfügbar. Einen ersten Überblick über die damit zusammenhängenden datenschutzrechtlichen Fragen haben wir bereits im letzten Jahr gegeben[178]. In der Zwischenzeit haben sich viele Neuerungen ergeben.

Google Street View erfreut sich bei einer Vielzahl seiner Nutzerinnen und Nutzer zunehmender Beliebtheit. Die Möglichkeiten praktischer Anwendungen für private oder geschäftliche Zwecke sind von Google im vergangenen Jahr deutlich ausgeweitet worden. Man kann z. B. Touristenattraktionen, Gebäude und Architektur und deren Umgebung betrachten und erhält per Mausklick Links, die dazu Hintergrundinformationen liefern. Die Bilder in Google Street View zeigen u. a. Parks, Bushaltestellen, Einkaufszentren und Parkmöglichkeiten, um vor einem „realen" Besuch in einer bestimmten Gegend eine erste virtuelle Orientierungshilfe zu geben. Die Darstellung von Verkehrskreuzungen, Straßen und Wegen kann darüber hinaus auch als Wegbeschreibung oder der Planung von Freizeitaktivitäten (z. B. Fahrradtouren und Wanderrouten) und als Ergänzung zu GPS-Systemen dienen. Das Bildmaterial kann als Entscheidungshilfe zum Kauf oder zur Anmietung einer Immobilie oder eines Grundstücks dienen. Das Erforschen der Geografie, der Vegetation und der Landschaft verschiedener Gebiete der Welt macht Google Street View zu einem interessanten Hilfsmittel für virtuelle Ausflüge. Um das Serviceangebot noch attraktiver zu gestalten, ist Google bestrebt, den Nutzerinnen und Nutzern flächendeckende Aufnahmen auf Straßenebene von möglichst vielen Metropolen und Regionen weltweit anzubieten.

Trotz der Möglichkeiten der durchaus sinnvollen und attraktiven Nutzung von Google Street View darf nicht vergessen werden, dass die Veröffentlichung des Bildmaterials der Straßenansicht auf der Internetseite Google Maps auch datenschutzrechtliche Risiken für die Wahrung der Persönlichkeitsrechte der abgebildeten Personen birgt. Um datenschutzrechtliche Risiken zu minimieren und die Persönlichkeitsrechte von Betroffenen zu wahren, hat sich Google dazu verpflichtet, die unterschiedlichen länderspezifischen Bestimmungen zu beachten. Aus diesem Grund verzögert sich in vielen Ländern die Veröffentlichung der Bilder, da das entsprechende Bildmaterial mit einer speziellen Software nach-

178 JB 2008, 8.4.1

bearbeitet werden muss, um Gesichter von Personen, Kfz-Kennzeichen und Gebäudefassaden unkenntlich zu machen. Diese zeitaufwendige Nachbearbeitung ist auch der Grund, weshalb noch keine Bilder aus Berlin und Deutschland über Google Street View abrufbar sind, obwohl seit Juli 2008 viele deutsche Regionen bereits erfasst wurden und weiterhin erfasst werden. Da diese Bildnachbearbeitung automatisiert erfolgt, kann es vorkommen, dass Gesichter oder Kfz-Kennzeichen nicht unkenntlich gemacht oder Bereiche behandelt wurden, auf denen gar keine datenschutzrelevanten Objekte zu sehen sind. Unabhängig davon kann es Bilder geben, die die Privatsphäre von Betroffenen nicht direkt, sondern in anderer Art und Weise verletzen (z. B. durch das Abbilden von Grundstücken, Hausfassaden, Fahrzeugen).

In Ergänzung zum Beschluss der Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) zur „Datenschutzrechtlichen Bewertung von digitalen Straßenansichten insbesondere im Internet“[179] hat Google im April gegenüber dem Düsseldorfer Kreis und im Juni gegenüber der für Google Deutschland zuständigen Aufsichtsbehörde in Hamburg Folgendes verbindlich zugesichert:

- eine Technologie zur Verschleierung von Gesichtern und Kfz-Kennzeichen vor der Veröffentlichung von derartigen Aufnahmen einzusetzen;
- für Bewohner oder Eigentümer Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes vorzuhalten und derartige Widersprüche zu bearbeiten;
- Widersprüche zu Personen, Kfz-Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern so zu berücksichtigen, dass diese vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs;
- noch geplante Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu zwei Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat zugesagt, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken. Die Liste der Kreise und

179 Vgl. Dokumentenband 2008, S. 37

Städte, von denen ab Frühjahr 2010 Aufnahmen gemacht werden sollen, ist im Internet abrufbar[180];

- die Widerspruchsmöglichkeit auch noch nach der Veröffentlichung einzuräumen;
- die Löschung bzw. Unkenntlichmachung der Rohdaten vorzunehmen, sobald die Speicherung und Verarbeitung der Rohdaten nicht mehr zur Weiterentwicklung und Verbesserung der unter 1. genannten Technologie erforderlich ist;
- die Löschung bzw. Unkenntlichmachung der Rohdaten von Personen, Kfz-Kennzeichen und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind. Die Löschung oder Unkenntlichmachung dieser Daten in den Rohdaten wird bereits vor der Veröffentlichung vorgenommen, wenn der Widerspruch bis zu einem Monat vor der Veröffentlichung der Bilder bei Google eingeht. Nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung in den Rohdaten binnen zwei Monaten;
- ein Verfahrensverzeichnis zu erstellen;
- eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View vorzulegen. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den Widerspruchsdaten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung bzw. Unkenntlichmachung.

Der Widerspruch kann im Internet[181] oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg eingelegt werden. Die Widersprüche werden zeitnah bestätigt. Wir haben einen Muster-Widerspruch auf unserer Internet-Seite zum Abruf bereitgestellt[182].

180 http://maps.google.de/intl/de/help/maps/streetview/faq.html#q9

181 http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7

182 http://www.datenschutz-berlin.de/content/technik/ratgeber/hinweise-zum-einlegen-von-widerspruechen

Die Aufsichtsbehörden der Länder bewerten die von Google gemachten Zusagen überwiegend positiv und begrüßen, dass Google gewillt ist, den Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger zu gewährleisten. Das Bildmaterial ist bisher nicht veröffentlicht. Es bleibt abzuwarten, ob die Zusagen eingehalten werden.

## 13.9 Aus der Arbeit der „Berlin Group“

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. „Berlin Group“) hat drei Arbeitspapiere verabschiedet:

- Das Arbeitspapier „Bericht und Empfehlungen zu Maut-Systemen („Sofia Memorandum“)“ [183] beleuchtet Risiken für die Privatsphäre von Nutzenden des Individualverkehrs (sowohl PKW als auch LKW), die bei der Erhebung von Straßennutzungsgebühren entstehen. Hier gilt es, die Anonymität der Nutzenden bestmöglich zu wahren.
- Die „Empfehlung zu Datenschutz und Elektronik-Abfall“ befasst sich mit den Gefahren für die Privatsphäre, die durch unsachgemäße Entsorgung oder Weitergabe von Telekommunikationsendgeräten (Handys und Personal Digital Assistants – PDA) entstehen können, wenn diese Geräte zum Zeitpunkt der Weitergabe oder Entsorgung noch personenbezogene Daten enthalten (z. B. in Adressbüchern, gespeicherten SMS oder Anruflisten)[184].
- Ein weiteres Arbeitspapier behandelt die Risiken bei der Wiederverwendung von E-Mail-Konten und ähnlichen Diensten der Informationsgesellschaft, z. B. nach Beendigung des Dienstleistungsvertrages oder dem Tod der Betroffenen[185].

183 Vgl. Dokumentenband 2009, S.137
184 Vgl. Dokumentenband 2009, S. 150
185 Vgl. Dokumentenband 2009, S. 153

# 14. Informationsfreiheit

## 14.1 Informationsfreiheit in Deutschland

Das **Bundesverfassungsgericht** hat entschieden, dass Abgeordneten ein umfassendes Informationsrecht gegenüber der Regierung zusteht, das sich bereits aus allgemeinen Verfassungsgrundsätzen herleitet.[186] Es befand, dass die Bundesregierung auch bei Kleinen Anfragen von Abgeordneten die Verweigerung von Auskünften ausführlich begründen muss. Im konkreten Fall ging es um Abgeordnete der Fraktion Bündnis 90/Die Grünen, die vom Bundesnachrichtendienst überwacht worden waren. Die Regierung wollte hierzu keine Einzelheiten mitteilen – zu Unrecht. Das Gericht hat damit die Kontrollrechte der Parlamentarier (nicht nur im Hinblick auf die Geheimdienste) gestärkt.

Beim Informationsfreiheitsgesetz des Bundes (Bundes-IFG) konnte ein Rückschritt abgewendet werden: Im Entwurf für ein **Zahlungsdiensteumsetzungsgesetz** war eine Änderung des Bundes-IFG versteckt, mit der auf Vorschlag des Bundesrates[187] eine Bereichsausnahme für Behörden der Finanz-, Wertpapier- und Versicherungsaufsicht eingefügt werden sollte. Eine solche pauschale Ausnahme hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland abgelehnt.[188] Denn es kann nicht angehen, dass gerade bei den Aufsichtsbehörden, deren Tätigkeit durch die globale Finanz- und Bankenkrise in die öffentliche Kritik geraten ist, die Transparenz noch weiter eingeschränkt wird. Der Bundestag ist dem Vorschlag des Bundesrates erfreulicherweise nicht gefolgt. So konnte eine Aushöhlung des Informationsanspruchs der Bürgerinnen und Bürger gegenüber Behörden verhindert werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat sich auch dafür ausgesprochen, dass Beschäftigte, die Missstände und Rechtsverstöße in Behörden oder Unternehmen aufdecken (sog. **Whistleblower**), gesetzlich

186 Beschluss vom 1. Juli 2009 – 2 BvE 5/06

187 BR-Drs. 827/08

188 Entschließung vom 26. Januar 2009: Keine weitere Einschränkung der Transparenz bei Finanzaufsichtsbehörden, Dokumentenband 2009, S. 159

geschützt werden.[189] Denn Hinweisgeberinnen und -geber sorgen für mehr Transparenz im Beschäftigungsumfeld. Sie sollten deshalb keine Repressalien am Arbeitsplatz befürchten müssen. Umgekehrt müssen die Datenschutzrechte der Belasteten (wie Auskunft und Berichtigung) berücksichtigt werden. Schließlich hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland gefordert, Hindernisse beim Informationszugang abzubauen[190] und die in verschiedenen Gesetzen verstreuten Informationszugangsrechte zu konsolidieren. [191]

Als Folge der Europäischen Transparenzinitiative[192] sind nun auch in Deutschland die Empfänger von **EU-Agrarsubventionen** im Internet gelistet[193]. Von den Bundesländern hat sich am längsten Bayern gegen die Veröffentlichung gewehrt und sich dabei auf den Persönlichkeitsschutz der Subventionierten berufen. Dieser Widerstand wurde schließlich aufgegeben, nicht zuletzt nachdem mehrere Obergerichte entschieden hatten, dass das Transparenzinteresse an der Veröffentlichung der Subventionsempfängerinnen und -empfänger höher zu bewerten ist als das Geheimhaltungsinteresse der Betroffenen.[194]

Es gibt wenig **Neues aus den Bundesländern.** Erfreulich ist, dass der Datenschutzbeauftragte in Hamburg jetzt auch die Aufgaben des Informationsfreiheitsbeauftragten wahrnimmt. Diese sinnvolle Aufgabenbündelung ist nach den Landtagswahlen in Thüringen Teil der Koalitionsvereinbarung, sodass im Jahr 2010 mit der Umsetzung gerechnet werden kann. Dann gibt es nur noch in Rheinland-Pfalz ein IFG ohne Informationsfreiheitsbeauftragten. In Hessen und Niedersachsen waren die parlamentarischen Anhörungen zu IFG-Entwürfen leider nicht zielführend. Dort ist also in absehbarer Zeit ebenso wenig mit Informationsfreiheitsgesetzen zu rechnen wie in Baden-Württemberg, Bayern und Sachsen.

189 Entschließung vom 24. Juni 2009: Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern, Dokumentenband 2009, S. 161

190 Entschließung vom 24. Juni 2009: Informationszugang für Bürgerinnen und Bürger verbessern, Dokumentenband 2009, S. 160

191 Entschließung vom 16. Dezember 2009: Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen, Dokumentenband 2009, S. 162

192 Zuletzt JB 2008, 15.1.

193 http://www.agrar-fischerei-zahlungen.de

194 Vgl. nur OVG Münster, Beschlüsse vom 24. April 2009 – 16 B 485/09, vom 27. April 2009 – 16 B 539/09, vom 28. April 2009 – 16 B 566/09

## 14.2 Informationsfreiheit in Berlin

### 14.2.1 Allgemeine Entwicklungen

Der **Berliner Verfassungsgerichtshof** hat entschieden, dass der Senat ein Volksbegehren wegen eines vermeintlichen Verstoßes gegen höherrangiges Recht nicht als unzulässig ablehnen darf.[195] Mit dem Volksbegehren „Schluss mit den Geheimverträgen – Wir Berliner wollen unser Wasser zurück" wollte die **Bürgerinitiative „Berliner Wassertisch"** eine vorbehaltlose Offenlegung der Verträge mit privatrechtlichen und öffentlich-rechtlichen Wasserversorgungsunternehmen erreichen[196]. Eine materiell-rechtliche Aussage zum IFG trifft das Gericht zwar nicht. Allerdings ist es der Meinung, dass die öffentliche Daseinsvorsorge zwar mit den Mitteln des Privatrechts (vertraglich) geregelt werden, aber nicht dem öffentlichen Recht entzogen werden könne. Das bedeutet, dass solche Verträge grundsätzlich auch dem IFG unterliegen und nicht von vornherein und in Gänze geheim gehalten werden dürfen. Das Gericht hat auch hervorgehoben, dass dem Senat kein Recht auf „Präventivkontrolle" zusteht. Allein der Verfassungsgerichtshof habe die Kompetenz zu prüfen, ob ein durch Volksbegehren zustande gekommenes Gesetz gegen höherrangiges Recht verstößt und verfassungswidrig ist, wie es der Senat zur Begründung seiner Ablehnung u. a.unter Berufung auf das „Recht der Unternehmen auf informationelle Selbstbestimmung" befunden hatte.

Die pauschale **Geheimhaltung von Verträgen,** die das Land Berlin mit Privaten schließt, ist auch in anderen Verwaltungsbereichen verbreitet. Umso erfreulicher ist, dass der Unterausschuss „Datenschutz und Informationsfreiheit" auf unseren Vorschlag einen Beschluss für mehr Transparenz gefasst hat. Der Senat wird aufgefordert, mit einem Schreiben an die öffentlichen Stellen des Landes Berlin darauf hinzuwirken, dass die öffentliche Hand - insbesondere im Bereich der Grundversorgung - künftig keine pauschale Vereinbarung mit einem Vertragspartner über die Geheimhaltung des gesamten Vertrages schließt und stattdessen im Vertrag auf das Berliner Informationsfreiheitsgesetz hinweist, nach

195 Urteil vom 6. Oktober 2009 – VerfGH 63/08
196 JB 2008, 15.2.1

dem auf Antrag eine (u. U. nur teilweise) Offenlegung des Vertrages in Betracht kommen kann.

Zu begrüßen ist die **Bundesratsinitiative Berlins**[197] **zur Änderung des Verbraucherinformationsgesetzes (VIG)**[198]. Basierend auf den Erfahrungen mit dem VIG, aber auch mit dem Umweltinformationsgesetz soll der Anspruch auf Zugang zu Verbraucherinformationen genauer ausgestaltet und insgesamt gestärkt werden. Die informationspflichtigen Stellen sollen zur aktiven Verbreitung von Verbraucherinformationen verpflichtet werden, wobei Inhalt und Art im Gesetz vorgegeben sind. Darüber hinaus sollen die Kostenregelungen vereinfacht werden.

Daneben gibt es weitere Initiativen für mehr Transparenz. So hat die Senatsverwaltung für Integration, Arbeit und Soziales eine Datenbank ins Internet gestellt, mit der über die **Verteilung von Zuwendungsmitteln** für Projekte in den Politikfeldern Arbeit, Soziales, Integration und Antidiskriminierung informiert wird. Neben der Höhe und dem Zweck der Zuwendungen sind die Namen und Anschriften der Empfängerinnen und Empfänger für die im Vorjahr ausgereichten Beträge von mehr als 5.000 Euro abrufbar.[199]

Auf Anregung und mit Unterstützung des Senats haben die Vereinigungen des sog. Dritten Sektors eine **Transparenzcharta der gemeinnützigen Organisationen** formuliert, mit der sie in einer Art Selbstverpflichtung ihre Arbeit nachvollziehbarer und durchschaubarer machen wollen. Damit soll um mehr Vertrauen geworben werden, das als zentrale Voraussetzung für eine aktive Beteiligung der Bürgerinnen und Bürger an der Gestaltung des städtischen Lebens verstanden wird.

Um mehr Vertrauen muss auch im Bereich des Sponsorings geworben werden. Zwar erstellt der Senat bereits regelmäßig einen **Sponsoringbericht** für die öffentliche Verwaltung in Berlin[200]. Die Berichtspflicht muss jedoch erweitert werden auf Fälle, in denen nicht die öffentliche Stelle direkt Empfängerin

197 BR-Drs. 652/09
198 JB 2008, 15.1
199 JB 2007, 13.2
200 JB 2007, 13.2

der Zuwendung ist, sondern eine private Einrichtung, die das Geld im Auftrag der öffentlichen Stelle projektbezogen einsetzen soll (wie z. B. beim alljährlichen Hoffest des Regierenden Bürgermeisters). Zu begrüßen ist deshalb der Antrag[201] der Fraktion Bündnis 90/Die Grünen, denn die öffentliche Hand darf sich nicht durch eine „Flucht ins Privatrecht" ihrer Transparenzpflichten entledigen.

## 14.2.2 Einzelfälle



**Dienstwagen im Urlaub**

Anlässlich der sog. Dienstwagenaffäre der früheren Bundesgesundheitsministerin Ulla Schmidt fragte ein Abgeordneter den Senat u. a., welchen Beschäftigten der Landesverwaltung eine private Nutzung von Dienstfahrzeugen gestattet sei und welche Senatsmitglieder die Dienstwagen auch zu Privatfahrten, ggf. Urlaubsfahrten nutzen.[202] Die Senatsverwaltung für Inneres und Sport hat uns um Stellungnahme zum Umfang der Offenbarung personenbezogener Daten gebeten.

Nach Art. 45 Abs. 2 Verfassung von Berlin hat jeder Abgeordnete das Recht, Einsicht in Akten und sonstige amtliche Unterlagen der Verwaltung zu nehmen. Die Einsichtnahme darf nur abgelehnt werden, soweit überwiegende private Interessen an der Geheimhaltung dies zwingend erforderlich machen. Der Abgeordnete hat mit der Kleinen Anfrage allerdings nicht von seinem Einsichts-, sondern nur von seinem Auskunftsrecht Gebrauch gemacht. Sein Auskunftsanspruch musste deshalb mindestens im selben Umfang erfüllt werden wie ein Einsichtsanspruch. Welche überwiegenden privaten Interessen der Betroffenen die Geheimhaltung zwingend (!) erforderten, war angesichts der öffentlichen Debatte um den Ausgangsfall nicht ersichtlich. Deshalb bestand ein umfassender personenbezogener Auskunftsanspruch des Abgeordneten.[203] Dass das Informationsrecht von Abgeordneten gegenüber der Regierung ein umfassendes ist, hatte kurz zuvor das Bundesverfassungsgericht entschieden.[204]

201 Abgh-Drs. 16/2840: Sponsoringbericht des Senats: Berichtspflicht erweitern

202 Kleine Anfrage des Abgeordneten Dr. Sebastian Kluckert (FDP) vom 28. Juli 2009 und Antwort: Machen auch Berliner Dienstwagen Urlaub in Spanien?, Abgh-Drs. 16/13 621

203 Betr. Ziff. 1, 5 sowie 6-9 der Kleinen Anfrage

204 Vgl. Fn. 186

Konkrete Fälle der (in Berlin unzulässigen) Privatnutzung im Urlaub hätten personenbezogen zwar dem Abgeordneten mitgeteilt, nicht jedoch in die zur Veröffentlichung vorgesehene Fassung der Antwort des Senats aufgenommen werden dürfen. Hier hätten nur anonymisierte Aussagen getroffen werden dürfen, weil sonst der Allgemeinheit personenbezogene Informationen zugänglich geworden wären, deren Offenbarung vom IFG nicht gedeckt wäre.

Nach diesem Gesetz hätten auch „Nichtparlamentarier" wie interessierte Bürgerinnen und Bürger oder die Presse entsprechende personenbezogene Informationsansprüche geltend machen können. Nach § 6 Abs. 2 Satz 1 Nr. 1 a) IFG stehen der Offenbarung personenbezogener Daten schutzwürdige Belange der Betroffenen in der Regel nicht entgegen, soweit sich aus einer Akte ergibt, dass die Betroffenen an einem Verwaltungsverfahren oder einem sonstigen Verfahren beteiligt sind. In diesem Fall müssen die Tatsache der Beteiligung sowie Namen und Funktionsbezeichnung offenbart werden. Von einer Verfahrensbeteiligung im Sinne des Regelbeispiels war (hypothetisch) auszugehen, weil einigen Funktionsträgern die Nutzung personengebundener Dienstfahrzeuge nach den hierfür geltenden Regelungen der Senatsverwaltung für Inneres und Sport eingeräumt wurde[205]. Deshalb hätte auch nach IFG ein Anspruch auf Benennung all derjenigen Personen bestanden, die an dem Nutzungsverfahren (sei es zu privaten oder dienstlichen Zwecken) überhaupt beteiligt waren, und auf Offenbarung der Tatsache der Privatnutzung. Dagegen wäre die Offenbarung der Privatnutzung des Dienstwagens zu Urlaubsfahrten durch bestimmte Funktionsträger vom IFG nicht gedeckt und nach § 6 Abs. 1 Satz 1 Berliner Datenschutzgesetz unzulässig gewesen, weil die Privatnutzung der Dienstwagen zu Urlaubsfahrten gerade nicht gestattet und damit nicht als Teil des Nutzungsverfahrens anzusehen ist.

Die Informationsrechte von Abgeordneten gegenüber der Verwaltung sind aufgrund der Verfassung von Berlin umfassender als die von „Nichtparlamentariern" nach IFG. Auch diese erhalten jedoch personenbezogene Informationen auf der Grundlage der in § 6 Abs. 2 IFG genannten Regelbeispiele.

205 Interne Regelungen der Senatsverwaltung für Inneres und Sport zur Nutzung personengebundener Dienstkraftfahrzeuge vom 14. Juni 2007

**Informationsweiterverwendung nach Informationszugang**

Für den Aufbau eines deutschlandweiten Flutmodells benötigte ein international tätiges Unternehmen, das sich mit der Entwicklung von Katastrophen-Management-Modellen befasst, riesige Datenmengen mit Messpegeln der Berliner Oberflächengewässer. Die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz fragte uns, wie die Gebühren nach IFG angesichts der Unmengen an Daten zu berechnen sind.

Wir haben mitgeteilt, dass der Zugang zu den Informationen nach § 18 a IFG zu bewerten ist, der auf das Umweltinformationsgesetz des Bundes verweist. Deshalb galt für die begehrten Umweltinformationen nicht das Verbot der gewerblichen Nutzung nach § 13 Abs. 7 IFG. Auf die Verwendung der Informationen war das Informationsweiterverwendungsgesetz (IWG) anzuwenden unter der Voraussetzung, dass eine Entgelterzielungsabsicht des Interessenten bestand (§ 2 Nr. 3 IWG). In diesem Fall haben wir empfohlen, eine Vereinbarung nach § 4 Abs. 2, 3 IWG zu schließen, entweder anstelle oder zusätzlich zu der Gebührenerhebung, wenn schon die Bereitstellung der Informationen nach IFG Kosten verursacht hat.

Es ist zu unterscheiden zwischen dem Zugang zu Informationen nach dem Informationsfreiheitsgesetz und der Verwendung von Informationen nach dem Informationsweiterverwendungsgesetz. Für die Verwendung kann eine Entgeltvereinbarung getroffen werden.

# 15. Was die Menschen von unserer Tätigkeit haben

Ein Bürger beschwerte sich darüber, dass er als Erbe keine Einsicht in die Unterlagen (Bankbelege im Umfang von neun Ordnern) der Betreuungsstelle im Bezirksamt Mitte über die Amtspflegschaft seiner Mutter erhielt. Später wurde vom Bezirksamt **Akteneinsicht** nach IFG zugebilligt, hierfür aber eine Gebühr von rund 100 Euro in Aussicht gestellt. Wir haben dem Bezirksamt mitgeteilt, dass das IFG mit der Gebührenfolge nicht maßgeblich ist, da für den Erben der Betreuten dieselben Rechte gelten wie für die Betreute selbst (nach Sozialgesetzbuch – SGB X). Deshalb durfte für die Akteneinsicht keine Gebühr erhoben werden. Allerdings haben wir auch mitgeteilt, dass eine zusätzliche Erläuterung der Bankbelege nicht erfolgen muss, weil der Vorgang seit Monaten abgeschlossen war und über mehrere Jahre zurückreichte. Insofern blieb dem Bürger nur die gerichtliche Überprüfung, soweit er die Richtigkeit der Zahlungsabläufe in Frage stellte.

Ein Bürger beschwerte sich darüber, dass die Berliner Wasserbetriebe (BWB) die Auskunft darüber verweigerten, von welcher Firma die angeschafften 70 Kanalschachtgeruchsfilter stammen. Die BWB beriefen sich im Hinblick auf eine mögliche Vergabeüberprüfung durch den Antragsteller auf **schutzwürdige Betriebs- oder Geschäftsgeheimnisse** der ausgewählten Firma. Wir haben die BWB davon überzeugt, dass die bloße Offenbarung eines Firmennamens kein solches Geheimnis darstellt. Daraufhin wurde dem Bürger der Name der Firma mitgeteilt.

Ein Bürger beschwerte sich darüber, dass ihm die **Akteneinsicht beim Jobcenter** Mitte verweigert wurde. Er war an dem Errichtungsvertrag der ARGE sowie an der Geschäftsordnung interessiert. Das Jobcenter hatte die Akteneinsicht unter Hinweis auf laufende gerichtliche Verfahren verweigert. Wir haben das Jobcenter davon überzeugt, dass **allgemeine Informationen über die Organisation und Abläufe** eines Jobcenters jedermann offenbart werden müssen. Daran änderten die anhängigen Klagen nichts. So konnten wir dazu beitragen, dass ein langjähriger Rechtsstreit teilweise beigelegt wurde.

Ein Jobcenter hat sich an den Arbeitgeber eines Leistungsempfängers gewandt, um eine Arbeitsbescheinigung und die Abrechnungen für zwei Monate anzufordern, ohne zuvor den Betroffenen darüber zu informieren oder die Unterlagen von diesem selbst zu verlangen. Das verstößt gegen das **Gebot der Direkterhebung beim Betroffenen**. Wir haben das Jobcenter zur Löschung der erhobenen Daten aufgefordert. Es hat den Datenschutzverstoß eingesehen und die Unterlagen aus der Akte des Betroffenen entfernt und vernichtet.

Ein Journalist hat uns darauf aufmerksam gemacht, dass bei einem **Jobcenter** wiederholt Post vor den überfüllten Briefkästen gelegen hat. Bei einer Ortsprüfung haben wir festgestellt, dass die Briefkästen so klein waren, dass insbesondere größere Umschläge nicht vollständig in den Briefkasten eingeworfen werden konnten. Auch schien das **Fassungsvermögen der Briefkästen** im Hinblick auf die Anzahl der zu erwartenden Postsendungen nicht auszureichen. Dadurch war nur ein unzureichender Schutz vor dem Zugriff unbefugter Dritter gewährleistet. Das Jobcenter hat dem Mangel abgeholfen und für die Anbringung eines größeren Briefkastens gesorgt, der den datenschutzrechtlichen Vorgaben entspricht.

Ein Bezirksamt hatte mit Änderung des Zahlungssystems für Sozialleistungen nach dem SGB XII auch die **Absenderkennzeichnung bei den Überweisungen** geändert, sodass auf der Überweisung zusätzlich das Kürzel „Soz“ verwendet wurde. Durch die Nutzung dieses Zusatzes war auch für Außenstehende ersichtlich, dass es sich bei dem Geldeingang um Sozialhilfe handelt. Es bestand die Gefahr, dass das kontoführende Geldinstitut erst auf diesem Weg vom **Bezug der Sozialhilfe** erfahren hätte. Wir haben das Bezirksamt davon überzeugt, auf das Kürzel „Soz“ zu verzichten und eine neutrale Absenderkennzeichnung zu verwenden.

Ein Bürger hat uns gefragt, inwieweit er verpflichtet ist, bei einem Antrag auf **Umzugskostenübernahme** eine vom Jobcenter geforderte **namentliche Liste der Umzugshelferinnen und -helfer** einzureichen. Wir haben das Jobcenter darauf hingewiesen, dass die Namen der Helfenden für die Bewilligung des Antrags auf Umzugskostenübernahme nicht erforderlich und daher unzulässig sind. Das Jobcenter hat das eingesehen und mitgeteilt, dass diese Daten künftig bei der Bearbeitung solcher Anträge nicht mehr erhoben werden.

Das **Berlin-Ticket S „berlinpass“** enthält ein Lichtbild der oder des Berechtigten sowie die komplette Wohnanschrift (Straße, Hausnummer, Postleitzahl). Das Ticket gilt zusammen mit dem entsprechenden Wertabschnitt als Fahrausweis für die öffentlichen Verkehrsmittel in Berlin. Beide Belege sind bei Kontrollen vorzulegen. Wir haben die für die Ausgestaltung des „berlinpass“ bzw. des Berlin-Ticket S zuständige Senatsverwaltung für Integration, Arbeit und Soziales darauf hingewiesen, dass eine eindeutige **Identifikation bereits durch das Lichtbild** verbunden mit dem Namen sowie der Ausweisnummer möglich ist. Die Senatsverwaltung ist dem gefolgt und verzichtet künftig auf Geburtsdatum und die Adresse auf dem Pass. Die Umsetzung wird bei der Nachbestellung von Passformularen erfolgen.

Eine Schule hat die Eltern und deren Kinder zu einem informellen Gespräch über die **Lernsituation in der Klasse** eingeladen. Dabei wurde – für die Betroffenen unerwartet – von der Schulleitung und den Lehrkräften im Beisein der anderen Eltern das Fehlverhalten einzelner Schüler erörtert. Wir haben die Schule darüber informiert, dass es sich bei einer derartigen **Offenbarung von personenbezogenen Schülerdaten** im Beisein von Dritten (anderen Eltern) um eine unzulässige Übermittlung von personenbezogenen Daten der betroffenen Schüler handelt. Wir haben empfohlen, von den Betroffenen künftig im Vorfeld derartiger informeller Gespräche eine Einwilligung in die Datenweitergabe einzuholen bzw., wenn diese nicht vorliegt, die Datenweitergabe künftig zu unterlassen.

Ein Vater informierte uns darüber, dass seiner Tochter von der Schule eine Liste mit den Ergebnissen der **Bundesjugendspiele 2008** übergeben wurde. Die Ergebnisliste enthielt, sortiert nach Klassen, Angaben mit den Namen und Vornamen der Schülerinnen und Schüler, die erreichte Punktzahl und die Angabe, ob eine Ehren- oder Siegerurkunde verliehen worden ist. Wir haben der Schule mitgeteilt, dass es sich bei diesen Angaben um personenbezogene Daten handelt, deren Übermittlung an Stellen außerhalb des öffentlichen Bereichs (die Eltern anderer Schüler) grundsätzlich nur mit Einwilligung der Betroffenen zulässig ist. Die Schulleitung teilte uns mit, dass die Liste versehentlich im Klassenraum in die Altpapierablage gelangt sei. Dieses Altpapier sei als Bastel- und Schmierpapier benutzt worden. Auf diesem Wege sei eines der Blätter mit den Daten der Bundesjugendspiele in die Hände der Schülerin gelangt. Die zuständige Klassenlehrerin hat sich bei dem Vater dafür entschuldigt.

Ehegatten oder eingetragene Lebenspartner haben als berücksichtigungsfähige Angehörige grundsätzlich einen **Beihilfeanspruch**, wenn ihr Einkommen im zweiten Kalenderjahr vor Beantragung der Beihilfe 17.000 Euro nicht übersteigt. Das Einkommen muss durch **Vorlage des Einkommensteuerbescheides** nach § 4 Abs. 1 Beihilfeverordnung jährlich nachgewiesen werden. Dabei wird jedoch nur vermerkt, dass der jeweilige Steuerbescheid vorlag und die Einkommensgrenze nicht überschritten wurde. Eine Speicherung des Betrages der Einkünfte erfolgt nicht. Der Steuerbescheid wird nach Prüfung zurückgesandt. Eine Aufnahme dieser Daten in die Personalakte der oder des Betroffenen findet nicht statt. Da die Kopie des Steuerbescheids jedoch auch Daten enthält, die für die Prüfung eines Beihilfeanspruchs Angehöriger nicht relevant sind, können diese selbstverständlich geschwärzt werden. Wir haben das Landesverwaltungsamt gebeten, einen entsprechenden Hinweis in das Merkblatt aufzunehmen.

Eine Beamtin beschwerte sich darüber, dass ein **ärztliches Gutachten** zur Feststellung ihrer Dienstunfähigkeit von dem Gutachter vollständig an die Personalstelle ihrer Dienstbehörde übermittelt worden war. Das 49-seitige Gutachten enthielt ausführliche und zum Teil sehr intime Informationen zur Biographie der Petentin, die für die bevorstehende Personalentscheidung nicht relevant waren. Der Dienstbehörde wurden nicht nur die maßgebenden Befunde, d. h. das Ergebnis der Untersuchung, mitgeteilt, sondern eine vollständige medizinische Dokumentation einschließlich einer umfassenden Anamnese vorgelegt. Das war unzulässig. Wir konnten erreichen, dass das Gutachten aus der Personalakte entfernt wird.

Die gesetzlichen Krankenkassen dürfen zur Sicherstellung einer wirtschaftlichen **Versorgung mit Hilfsmitteln** Verträge auch mit einzelnen Anbietern abschließen. Die Versorgung der Versicherten erfolgt dann ausschließlich durch diesen Vertragspartner. Die **AOK Berlin** hat für die Versorgung mit Schlafapnoe-Therapiegeräten einen solchen Vertrag geschlossen. Um die Auslieferung dieser Hilfsmittel zu beschleunigen, hat sie **Adressdaten** der betroffenen Versicherten an das Vertragsunternehmen weitergeben, ohne vorab deren Einwilligung einzuholen. Wir haben deshalb gegenüber der AOK einen Datenschutzverstoß festgestellt.

Im Rahmen der Bearbeitung einer Bürgerbeschwerde wurde uns von einer Klinik der Charité das dort verwendete Formular für eine **Schweigepflicht-**

**entbindungserklärung** vorgelegt. Es genügte nicht den datenschutzrechtlichen Anforderungen. Für die Patientinnen und Patienten war aus der Formulierung der Einwilligungsklausel nicht hinreichend deutlich erkennbar, dass Behandlungsdaten an ein privates Unternehmen zur Abrechnung ärztlicher Leistungen übermittelt werden sollten. Wir konnten erreichen, dass das Formular geändert wird.

Ein Patient beschwerte sich über das Schreiben eines Arztes der Charité, in dem dieser sich für das entgegengebrachte Vertrauen bei der Behandlung im Krankenhaus bedankte und mitteilte, dass er nunmehr in einer **Gemeinschaftspraxis** als niedergelassener Arzt tätig sei. Der Arzt war nicht berechtigt, die aus der **Patientenkartei der Klinik** stammenden Adressdaten für sein Informationsschreiben zu verwenden. Wir haben den Datenschutzverstoß mit einem Verwarnungsgeld geahndet.

Ein **Pflegedienst** begehrte Einsicht in ein an die AOK Berlin gerichtetes Beschwerdeschreiben, das Anlass für eine Qualitätsprüfung in einer Einrichtung des Pflegedienstes durch den Medizinischen Dienst der Krankenversicherung war. Mit der Gewährung der **Akteneinsicht** wäre allerdings auch der Name des Informanten offengelegt worden. Dieser unterfällt unabhängig davon, ob Vertraulichkeit ausdrücklich gefordert oder zugesichert worden ist, dem von der Pflegekasse zu beachtenden **Sozialdatenschutz**. Danach bestand keine Übermittlungsbefugnis. Auch ein überwiegendes Interesse der Pflegeeinrichtung, die **Identität des Informanten** festzustellen, lag nicht vor. Das wäre nur dann der Fall, wenn ausreichende Anhaltspunkte dafür bestehen, dass der Informant wider besseres Wissen und in der vorgefassten Absicht, den Ruf der Pflegeeinrichtung zu schädigen, gehandelt haben könnte. Die AOK hat die Akteneinsicht entsprechend unserem Rat abgelehnt.

Ein Kunde wurde von seiner Bank darüber informiert, dass sein Konto in einer anderen Filiale geführt wird, weil eine Auswertung seiner **Bargeldabhebungen** ergeben hat, dass er häufiger in seiner neuen Filiale Geld abhebt. Die **Auswertung der Kontobewegungsdaten** durch die Bank erfolgte ohne Zustimmung des Kunden und war deshalb rechtswidrig. Die Bank hat uns zugesagt, künftig ähnliche Auswertungen nur noch mit Einwilligung der Betroffenen vorzunehmen.

Eine Bürgerin beschwerte sich über ihre Bank, die mitgeteilt hatte, sie werde die monatlichen **Kreditkartenabrechnungen per E-Mail** zuleiten, sofern dem nicht widersprochen wird. Wir konnten durchsetzen, dass die Bank nur dann die Abrechnungen per E-Mail versendet, wenn die Kundin oder der Kunde diesem Verfahren ausdrücklich zustimmt.

Eine Bürgerin erhielt ein **Werbeschreiben** einer ihr nicht bekannten Bank, in dem ihr ein Kredit angeboten wurde. Die Bank hatte ihr schon vorab eine Kontonummer zugeteilt. Diese war identisch mit der Kontonummer einer Bank, mit der die Bürgerin ein Jahr zuvor die Vertragsbeziehung beendet hatte. Unsere Ermittlungen ergaben, dass die werbende Bank die ehemalige Bank der Betroffenen übernommen hatte und die **Daten der ehemaligen Kundinnen und Kunden für eine Mailingaktion** nutzte. Wir haben die Bank darauf hingewiesen, dass Bankverbindungsdaten von ehemaligen Kundinnen und Kunden aus dem operativen Geschäft zu entfernen sind und nicht für Werbezwecke verwendet werden dürfen. Die Bürgerin wird künftig von der Bank nicht mehr beworben.

Ein ehemaliger Kunde eines insolventen Fitness-Studios erhielt ein **Werbeschreiben** von einem anderen Fitness-Studio. Dieses hatte die **Kundendaten** von einem Unbekannten für zwei Eiweißdosen gekauft. Die Daten enthielten neben Namen und Anschrift auch die Bankverbindung des Betroffenen. Wir haben beim Fitness-Studio durchgesetzt, dass die illegal erworbenen Daten vernichtet wurden.

Im **Versicherungsvermittlerregister** war auf der Webseite www.vermittlerregister.info die Angabe der betrieblichen Anschrift der jeweiligen Versicherungsmaklerin oder des jeweiligen Versicherungsmaklers vorgesehen. Bei Gleichheit von betrieblicher und privater Anschrift bestand für die betroffenen Makler mit der **Maklerregistrierung** im Vermittlerregister die Gefahr, permanent postalisch mit Werbung behelligt zu werden. So versuchten Versicherungsunternehmen und Maklerpools die dort registrierten Makler abzuwerben oder sie mit ihren neuesten Produkten zu bewerben. Wir haben die IHK Berlin gebeten, auf der entsprechenden Webseite folgende Nutzungsbeschränkung einzufügen: „Die Nutzung dieser Daten zu werblichen Zwecken ist untersagt." Der Betreiber der Webseite teilte uns mit, dass er unserer Empfehlung folgen und den Satz auf der Startseite des Vermittlerregisters aufnehmen wird.

Eine Kundin wurde von einem Beerdigungsinstitut mit Hilfe von Mustern darüber informiert, wie **Todesanzeigen** formuliert werden können. Als Muster verwandte das Institut die Todesanzeigen der letzten Monate. Die Kundin wollte verhindern, dass auch die Todesanzeige für ihre Mutter als Muster verwendet wird. Wir konnten beim Beerdigungsinstitut durchsetzen, dass Anzeigenmuster künftig keine **Echtdaten** mehr enthalten.

Ein Nutzer eines Angebots, bei dem man eigene Homepages im Internet veröffentlichen kann, beschwerte sich darüber, dass der Anbieter seinen Namen, seine Post- und E-Mail-Adresse mitsamt der IP-Adresse, unter der er das Angebot gebucht hatte, im Internet veröffentlicht hat – und zwar auch zur Indexierung durch externe Suchmaschinen. Der Anbieter berief sich auf die presserechtliche **Impressumspflicht**. Wir haben ihn darauf hingewiesen, dass hier das Telemediengesetz und nicht das Presserecht gilt. Eine Veröffentlichung von Namen, Post- und E-Mail-Adresse der Nutzenden ohne ihre Einwilligung ist nur zulässig, soweit diese einer Impressumspflicht nach § 5 TMG unterliegen. Das ist nicht bei allen Homepages der Fall (insbesondere nicht bei privaten). Erst recht ist eine **Veröffentlichung der IP-Adresse, u**nter der eine Nutzerin oder ein Nutzer eine Homepage bei dem Anbieter eingerichtet hat, ohne Einwilligung unzulässig. Darüber hinaus wurden Angaben zu Geschlecht und Geburtstag erhoben, die für die Erbringung des Dienstes nicht erforderlich sind. Wir haben dem Anbieter empfohlen, den Nutzenden hinsichtlich der Indexierung durch Suchmaschinen ein Wahlrecht einzuräumen. Im Verlauf des Schriftwechsels stellte sich heraus, dass der Anbieter auch von Nutzenden der Webseite seiner Kundschaft Nutzungsdaten (insbesondere dynamische IP-Adressen) dauerhaft speicherte - auch hier ohne Rechtsgrundlage. Nach längerem Schriftwechsel hat der Anbieter allen unseren Forderungen entsprochen.

Ein Nutzer einer Online-Partnerschaftsvermittlung beschwerte sich darüber, dass der Anbieter Angaben zu seinem persönlichen Profil (einschließlich vollem Namen und Wohnort) allgemein suchfähig für **externe Suchmaschinen** ins Internet gestellt hat. Zu diesem Zeitpunkt enthielten die Allgemeinen Geschäftsbedingungen nur einen vagen Hinweis, dass bestimmte Daten des Profils für die Erfassung durch externe Suchmaschinen freigegeben würden. Aufgrund unserer Intervention hat das Unternehmen die Datenschutzerklärung dahingehend ergänzt, dass ausdrücklich auf die Art der veröffentlichten Daten sowie darauf hingewiesen wird, dass diese Funktion durch die Nutzen-

den deaktiviert werden kann. Im Laufe des Schriftwechsels stellte sich heraus, dass der Anbieter IP-Adressen von Nutzerinnen und Nutzern auch nach Beendigung des Nutzungsvorgangs dauerhaft speicherte. Wir haben dem Anbieter mitgeteilt, dass es hierfür keine Rechtsgrundlage gibt, mit Ausnahme einer kurzfristigen Speicherung von Nutzungsdaten ausschließlich zu Zwecken der Gewährleistung der Datensicherheit. Der Anbieter hat daraufhin seine Speicherungspraxis geändert.

# 16. Aus der Dienststelle

## 16.1 Entwicklungen

Der Stellvertreter des Berliner Beauftragten für Datenschutz und Informationsfreiheit für den Bereich Recht, Dr. Thomas Petri, wurde am 27. Mai zum neuen Bayerischen Landesbeauftragten für den Datenschutz gewählt. Sein Weggang und die deutlich gestiegenen Anforderungen an die Datenschutzaufsicht insbesondere im Bereich der Privatwirtschaft wurden zum Anlass für eine Neuorganisation vor allem des juristischen Bereichs der Dienststelle genommen. Nachdem das Abgeordnetenhaus dankenswerterweise mit dem Haushaltsplan 2010/2011 zwei dringend benötigte zusätzliche Planstellen des höheren Dienstes bewilligt hatte, konnte der stark angewachsene Bereich Recht aufgeteilt werden, sodass sowohl den zunehmenden Kontrollerfordernissen in der Wirtschaft als auch in der Berliner Verwaltung in Zukunft besser Rechnung getragen werden kann. Damit wird eine Struktur wiedereingeführt, die bereits bis 1998 Bestand hatte, als der juristische Bereich zusammengelegt wurde. Die jetzt gewählte Organisation sieht vor, dass dem Leiter des neuen Bereichs Recht I eine eigens gebildete Sanktionsstelle zugeordnet wird, in der sowohl Bußgeldverfahren als auch Verwaltungszwangsmaßnahmen nach dem Bundesdatenschutzgesetz bearbeitet werden. Die Bürgereingaben werden weiterhin in einem BürgerOffice behandelt, das dem Leiter des Bereichs Recht II zugeordnet ist.

Die Zahl der Eingaben ist erneut deutlich gestiegen[206]. Auch die Zahl der eingeleiteten Bußgeldverfahren nahm stark zu. Es wurden 19 Bußgeldbescheide und Verwarnungen über eine Gesamthöhe von 1,146 Millionen Euro verhängt. In sechs Fällen wurden Einsprüche eingelegt, über die in zwei Fällen noch nicht entschieden ist.

206 Vgl. Tabelle nächste Seite

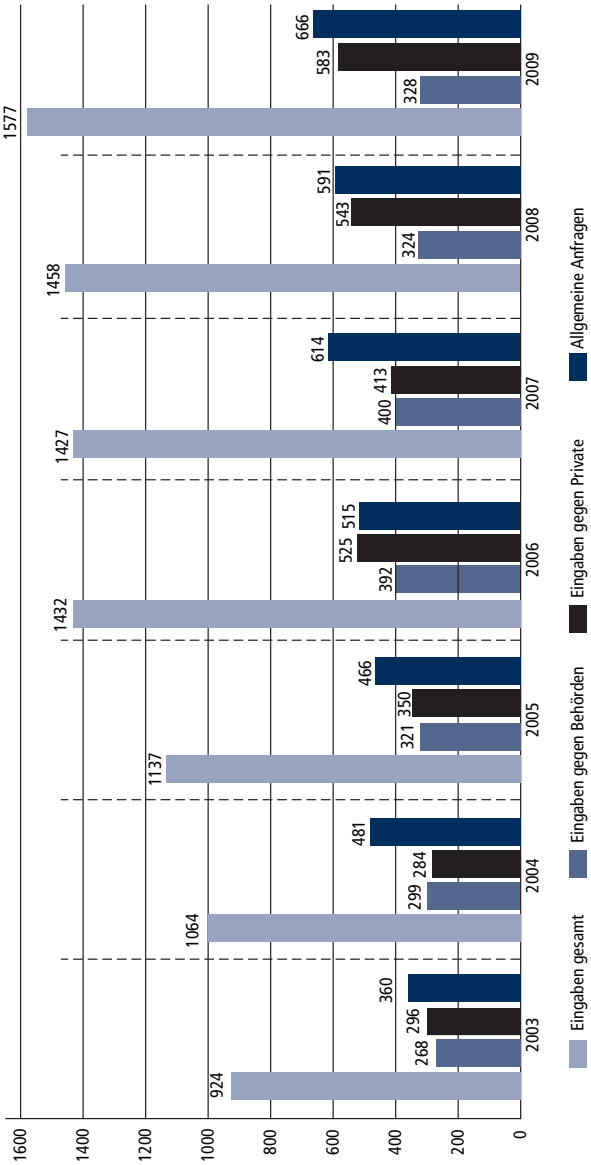


Tabelle 1: Anzahl der Bürgereingaben im Jahresvergleich 2003–2009

## 16.2 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 2007 abschließend beraten und daneben zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit erörtert. Auf Empfehlung des Unterausschusses hat das Abgeordnetenhaus am 25. Juni eine Reihe von Beschlüssen gefasst, in denen der Senat aufgefordert wird, für ein datenschutzgerechtes Vorgehen der Verwaltung zu sorgen oder bestimmte Prüfungen vorzunehmen[207].

## 16.3 Zusammenarbeit mit anderen Stellen

2009 hatte der Berliner Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz in der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** inne, die am 26./27. März und 8./9. Oktober in Berlin tagte. Die Konferenz hat zahlreiche Entschließungen gefasst[208]. Für 2010 hat der Landesbeauftragte für den Datenschutz Baden-Württemberg den Konferenzvorsitz übernommen.

Die im **„Düsseldorfer Kreis“** kooperierenden Aufsichtsbehörden für den **Datenschutz in der Privatwirtschaft** haben unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern am 23./24. April in Schwerin und am 26./27. November in Stralsund getagt. Auch sie haben Beschlüsse zum Datenschutz gefasst, die so unterschiedliche Themen wie das Screening von Beschäftigten anhand sog. Terrorlisten, die Übermittlung von Passagierdaten auf Vorrat an britische Behörden und die datenschutzkonforme Ausgestaltung von Analyseverfahren bei Internetangeboten (z. B. Google Analytics) betrafen[209].

207 Vgl. Anhang 1
208 Vgl. Dokumentenband 2009, S. 11 ff.
209 Vgl. a.a.O., S. 24 ff.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 23./24. Juni in Magdeburg unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Sachsen-Anhalt und am 16. Dezember in Hamburg unter dem Vorsitz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Sie hat Entschließungen zur Transparenz bei der Finanzaufsicht, zum Schutz von Whistleblowern und zur bürgerfreundlichen Regelung des Informationszugangs gefasst[210]. Im ersten Halbjahr 2010 hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz dieser Konferenz übernommen.

Berlin vertritt die Bundesländer im Auftrag der Konferenz der Datenschutzbeauftragten sowie der Aufsichtsbehörden in der **Arbeitsgruppe nach Artikel 29 Europäische Datenschutzrichtlinie**, seit diese Arbeitsgruppe 1996 ihre Arbeit aufgenommen hat. Sie hat erneut mehrere Stellungnahmen zu zentralen Datenschutzfragen abgegeben, die die vorprozessuale Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery), die Verwendung von Standardvertragsklauseln beim Datenexport, den Schutz personenbezogener Daten von Kindern und die Nutzung sozialer Online-Netzwerke betreffen[211]. Auf Einladung der spanischen Datenschutzbehörde fand die **31. Internationale Konferenz der Datenschutzbeauftragten** vom 4.–6. November in Madrid statt. Die Teilnehmenden fassten einen grundlegenden Beschluss zur Erarbeitung international verbindlicher Datenschutzstandards, der an frühere Initiativen der Datenschutzbeauftragten anknüpft.

Die **Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group")** tagte unter unserem Vorsitz am 12./13. März in Sofia und am 7./8. September in Berlin. Die Gruppe verabschiedete Arbeitspapiere zum Datenschutz in Mautsystemen („Sofia Memorandum"), zum Elektronik-Abfall und zum Problem verwaister E-Mail-Konten[212].

Die **Internationale Konferenz der Informationsfreiheitsbeauftragten** fand vom 27.–30. September auf Einladung des norwegischen parlamentarischen Ombudsmanns in Oslo statt.

210 Vgl. a.a.O., S. 160
211 Vgl. a.a.O., S. 35
212 Vgl. a.a.O., S. 137

## 16.4 Öffentlichkeitsarbeit

In diesem Jahr konnte die Dienststelle ihr 30-jähriges Bestehen feiern. Aus diesem Anlass fand am 29. Oktober ein Festakt im Abgeordnetenhaus zu „30 Jahren Datenschutz und 10 Jahren Informationsfreiheit in Berlin“ statt. Unter den zahlreichen Gästen waren auch der erste Berliner Datenschutzbeauftragte, Dr. Hans-Joachim Kerkau, und sein Nachfolger, Prof. Dr. Dr. Hansjürgen Garstka. Den Festvortrag zum Thema „Prävention – Herausforderung und Grenze des Datenschutzes“ hielt der langjährige Hessische Datenschutzbeauftragte Prof. Dr. Dr. h. c. mult. Spiros Simitis.

Der 3. Europäische Datenschutztag fand am 28. Januar statt unter dem Motto „Der ideale Angestellte, der genormte Arbeitnehmer: Wie viel darf mein Arbeitgeber über mich wissen?“. Das Thema hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits 2008 aufgrund der zahlreihen Überwachungsskandale im privatwirtschaftlichen Bereich gewählt.

Daneben beteiligten wir uns wieder an mehreren öffentlichen Veranstaltungen:

- Tag der offenen Tür des Landtages Brandenburg am 4. Juli
- 5. Jugendverbraucherschutztag im Freizeit- und Erholungszentrum Wuhlheide am 23. September
- Jugendmesse YOU am 9./10. Oktober
- 9. Berliner Jugendforum im Abgeordnetenhaus am 14. November.

Auch an mehreren Diskussionen in Berliner Schulen nahmen wir teil, z. B. in der John-F.-Kennedy-Gesamtschule zum Thema „60 Jahre Grundgesetz“.

Berlin, den 31. März 2010

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

# Anhang

**Anhang 1:**
Beschlüsse des Abgeordnetenhauses vom 25. Juni 2009

**Anhang 2:**
Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 25. Juni 2009 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2007

**Anhang 3:**
Auszug aus dem Geschäftsverteilungsplan

**Stichwortverzeichnis**

# Beschlüsse des Abgeordnetenhauses vom 25. Juni 2009

## Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2007

**1a) Aktuelle IT-Projekte des Landes, hier: Erneuerung der IT-Verfahren der Berliner Steuerverwaltung – EOSS (1.2.3, Drs. S. 15 f)**

**b) Aktuelle IT-Projekte des Landes, hier: Online-Bewerbungen und -Einstellungen für Berliner Lehrkräfte (BEO) und für Vertretungslehrkräfte (BEO V) (1.2.3, Drs. S. 16 ff)**

Der Senat wird aufgefordert, dafür zu sorgen, dass die sich aus § 24 Abs. 3 Satz 3 BlnDSG ergebende Pflicht zur Unterrichtung des Berliner Beauftragten für Datenschutz und Informationsfreiheit über neue Automationsvorhaben und über wesentliche Änderungen automatisierter Datenverarbeitungen so rechtzeitig wahrgenommen wird, dass er noch vor ihrer Einführung Gelegenheit zur Stellungnahme erhält.

**2. Zuverlässigkeitsüberprüfungen bei der Deutschen Bundesbank (3.1.7, Drs. S. 75 ff)**

Der Senat wird aufgefordert, bei der nächsten Senatsvorlage zur Änderung des ASOG eine klarstellende Regelung für Zuverlässigkeitsüberprüfungen und Akkreditierungsverfahren bei Großereignissen (wie Fußballweltmeisterschaft, Leichtathletikweltmeisterschaft, Staatsbesuchen) oder von Personen, die als Lieferanten oder Dienstleister Zutritt zu sicherheitsempfindlichen Einrichtungen benötigen, vorzusehen.

### 3. Automatisierte Erteilung von Melderegisterauskünften (4.1.3, Drs. S. 86 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass die im Informations- und Melderegister enthaltenen Daten, für die keine gesetzliche Speicherungsbefugnis besteht, unverzüglich gelöscht werden.

### 4. Schwärzungen im Mietvertrag (7.2.3, Drs. S. 120 ff)

Der Senat wird aufgefordert, darauf hinzuwirken, dass alle Berliner Jobcenter bei der Prüfung von Leistungen für Unterkunft und Heizung nur die hierfür erforderlichen Daten erheben. Die Betroffenen dürfen nicht erforderliche Daten bei Vorlage des Mietvertrages schwärzen, worauf sie hinzuweisen sind.

### 5. Überprüfung von Meldedaten durch Schulämter bei Anmeldung zur Einschulung (8.3.2, Drs. S. 158 ff)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die Schulbehörden bei der Anmeldung zur Einschulung grundsätzlich die im Melderegister erfassten Daten für die Entscheidung über die Aufnahme eines Schulkindes an einer Grundschule zugrunde legen. Nur bei konkreten Anhaltspunkten dafür, dass die Meldedaten nicht den tatsächlichen Wohnverhältnissen des Kindes entsprechen, sind die erforderlichen Ermittlungen von der Meldebehörde in eigener Zuständigkeit und nicht von der Schulbehörde durchzuführen.

### 6. Informationsfreiheit im Land Berlin, hier: Allgemein zugängliche Aktenverzeichnisse nach § 17 Abs. 4 IFG (13.2, Drs. S. 217 f)

Der Senat wird aufgefordert, mit einem Schreiben an die öffentlichen Stellen des Landes Berlin darauf hinzuwirken, dass die nach § 17 Abs. 4 IFG bestehende Pflicht, Aktenverzeichnisse zu führen und diese allgemein zugänglich zu machen, überall umgesetzt wird. Dies soll pro-aktiv durch Veröffentlichung im Internet geschehen.

### 7. Informationsfreiheit im Land Berlin, hier: Einzelfälle (13.2.1 – 13.2.8, Drs. S. 218 ff)

Der Senat wird aufgefordert, mit einem Schreiben an die öffentlichen Stellen des Landes Berlin darauf hinzuweisen, dass die in § 13 Abs. 5 IFG genannte Urheberrechtsklausel nur die Frage der (urheberrechtlich relevanten) Verwertung von zuvor erlangten Informationen betrifft und nicht von vornherein den Informationszugang ausschließt.

### 8. Öffentlichkeitsarbeit – Nutzung elektronischer E-Mail-Verteiler (14.4, Drs. S. 228 f)

Der Senat wird aufgefordert, den Berliner Beauftragten für Datenschutz und Informationsfreiheit dadurch zu unterstützen, dass dessen Informationsmaterial (z. B. Einladungen zu Veranstaltungen) bei Bedarf über die elektronischen Verteiler der Verwaltungen verbreitet wird.

### 9. Auswertedatenbank „Polizeilicher Staatsschutz“ (3.1.6, Drs. S. 72 ff)

„Der Senat wird aufgefordert, darauf hinzuwirken, dass die Polizei von den gesetzlich vorgesehenen Höchstprüffristen für in Auswertedatenbanken gespeicherte Personen nur in den Fällen Gebrauch macht, in denen dies nach konkreter Prüfung im Einzelfall unter strenger Wahrung des Verhältnismäßigkeitsgrundsatzes jeweils erforderlich ist.“

### 10. Datenerhebung vor Erteilung einer Niederlassungserlaubnis (4.1.5, Drs. S. 89 ff)

„Der Senat wird aufgefordert, dafür zu sorgen, dass die Ausländerbehörde zur Prüfung des aufenthaltsrechtlichen Status eines Antragstellers nur Unterlagen anfordert, die für die Beurteilung tatsächlich erforderlich sind. Das schließt die Anforderung von Unterlagen aus, die er im Rahmen seiner Mitwirkungspflicht nicht beschaffen muss.“

# Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 25. Juni 2009 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2007

**Herr Präsident,**
**sehr geehrte Damen und Herren,**

Ihnen liegen heute die Beschlussempfehlungen des Ausschusses für Inneres, Sicherheit und Ordnung vor, die der Unterausschuss „Datenschutz und Informationsfreiheit" vorbereitet hat. Dessen Mitglieder haben parteiübergreifend Position zu Themen aus dem **Jahresbericht 2007** bezogen, zu denen Meinungsunterschiede mit dem Senat bestanden. Erneut hat sich gezeigt, wie wichtig der parlamentarische Rückhalt für die Arbeit des Beauftragten für Datenschutz und Informationsfreiheit ist. Ich danke deshalb allen Abgeordneten für ihre Unterstützung, die in diesen Beschlussempfehlungen zum Ausdruck kommt.

Sie betreffen mehrere Situationen, in denen wir vom Senat eine frühere Beteiligung bei IT-Projekten erwarten. Aber auch die bisher unzureichend legitimierte Zuverlässigkeitsüberprüfung bei Großereignissen wie der Leichtathletik-WM, der Umgang mit Meldedaten oder die nach dem Informationsfreiheitsgesetz vorgeschriebene Veröffentlichung von Aktenverzeichnissen sind Gegenstand dieser Empfehlungen.

Erlauben Sie mir aus aktuellem Anlass eine Bemerkung zum Verhältnis zwischen dem Datenschutz und ehrenamtlicher Tätigkeit, denn dieses wurde bis vor kurzem kontrovers im Verbund öffentlicher Bibliotheken Berlins diskutiert. In zwei Bezirken sind **Ehrenamtliche in öffentlichen Bibliotheken** tätig. So begrüßenswert es sein mag, dass Bibliotheken, die sonst von der Schließung bedroht wären, dank ehrenamtlichem Engagement weiter betrieben werden können, so klar ist aber auch, dass dies nur im Einklang mit den Bestimmungen des Datenschutzrechts möglich ist.

Bibliotheken unterscheiden sich insoweit nicht von anderen öffentlichen Stellen wie Gesundheitsämtern oder Jobcentern. Wer sie als Bürger aufsucht, kann darauf vertrauen, dass er seine Daten nur fest angestellten Dienstkräften des Landes oder der Bezirke offenbart. Es besteht deshalb Einvernehmen mit dem Bibliotheksverbund, dass ehrenamtlich in Bibliotheken Tätige keinen berlinweiten Zugriff auf Daten über Nutzer und ihre Lesegewohnheiten erhalten dürfen. Bis zur Umstellung der Software, die erst im nächsten Jahr möglich ist, muss dies in den betroffenen Bibliotheken organisatorisch sichergestellt werden. Das kann, wie offenbar jetzt geplant, z. B. dadurch erfolgen, dass den ehrenamtlichen Mitarbeitern hauptamtliche zur Seite gestellt werden, denen der Zugriff auf die Nutzerkonten vorbehalten ist.

Als ich vor einem Jahr an dieser Stelle angesichts der Datenskandale beim Lebensmittel-Discounter Lidl und bei der Deutschen Telekom davon sprach, dass der Datenschutz in aller Munde sei, war noch nicht bekannt, dass die **Deutsche Bahn** ihre Mitarbeiter und Außenstehende über Jahre systematisch mehrfach heimlich ausgespäht hat. Zur Korruptionsbekämpfung und Aufklärung von Geheimnisverrat schien diesem Unternehmen nahezu jedes Mittel recht zu sein. Zeitweise entstand der Eindruck, dass das Unternehmen sich einer unabhängigen Aufklärung dieser Vorgänge durch die zuständige Aufsichtsbehörde, den Berliner Beauftragten für Datenschutz und Informationsfreiheit, entziehen wolle.

Mittlerweile – nach grundlegenden Veränderungen im Unternehmensvorstand – bin ich zuversichtlicher, dass wir **unsere Aufgabe der unabhängigen Datenschutzkontrolle** auch bei diesem Konzern, dem größten Arbeitgeber in Berlin – wenn nicht in der Bundesrepublik, ungehindert erfüllen können. Dabei müssen wir nicht nur Rechtsverstöße in der Vergangenheit ahnden, sondern vor allem den Konzern zu einer grundlegenden Änderung seiner internen Abläufe hin zu einer datenschutzgerechten Unternehmenskultur bewegen.

Daneben hat der Aufsichtsrat der Deutschen Bahn zwei Anwaltskanzleien und ein Wirtschaftsprüfungsunternehmen als Sonderermittler beauftragt, die für ihre Untersuchungen Personal im doppelten Umfang des gesamten Personals meiner Dienststelle eingesetzt haben. Die unabhängige Datenschutzkontrolle ist aber nach dem Gesetz primär Aufgabe meiner Behörde. Dieser Aufgabe kann sie nur nachkommen, wenn ihr **Personal** bei den kommenden Haushaltsbe-

ratungen angemessen verstärkt wird, denn die Deutsche Bahn ist – da bin ich mir sicher - nur die Spitze des Eisbergs. Ich bitte Sie insoweit schon jetzt um Ihre Unterstützung.

Auch der Bundesgesetzgeber ist aufgerufen, durch die baldige Verabschiedung eines Arbeitnehmerdatenschutzgesetzes dafür zu sorgen, dass Unternehmen ihre Beschäftigten nicht zu „informationellem Freiwild" machen können. Ich erwarte, dass der Senat nach der Bundestagswahl hierzu **Initiativen im Bundesrat** ergreift, und bitte Sie, auch dieses Anliegen zu unterstützen.

*Vielen Dank für Ihre Aufmerksamkeit.*

# Auszug aus dem Geschäftsverteilungsplan

## Stand: 31. Dezember 2009

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,**<br>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<br>AG: Internationaler und europäischer Datenschutz, Abgeordnetenhaus, Bezirksverordnetenversammlungen, Informationsfreiheit |
| Zentrale Aufgaben | |
| App. 211 | AG: Telekommunikation, Tele- und Mediendienste, Rundfunk |
| App. 210 | 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 AV, Rechnungsstelle, Beschaffungswesen, IPV, Dienstreisen im Bereich Recht |
| **BEREICH RECHT** | |
| App. 111 | **Volker Brozio**, Bereichsleiter (kommissarisch), AG: Senatskanzlei (außer Kultur), Rechnungshof, Parteien |
| App. 302 | Sekretariat |
| **BürgerOffice** | |
| App. 111 | Leitung; Öffentlichkeitsarbeit<br>AG: Finanzen, Schule |
| App. 112 | AG: Inneres, Sport, Integration (Ausländerrecht) |
| 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, öffentliche Verkehrsunternehmen |
| App. 212 | Stellvertretender Pressesprecher<br>AG: Gesundheit, eGovernment |

| | |
|---|---|
| App. 318 | AG: Jugend |
| App. 315 | AG: Soziales |
| App. 300 | Justiz |
| App. 304 | AG: Stadtentwicklung, Kultur, Umwelt, Presserecht, Rundfunkgebühren |
| **BEREICH INFORMATIK** | |
| App. 400 | Dipl.-Informatiker **Hanns-Wilhelm Heibey**, Bereichsleiter, Vertreter des BlnBDI<br><br>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,<br>Erstellung und Pflege von Verteilerlisten |
| App. 408 | Q: Berliner Landesnetz, Telekommunikationssysteme<br>R: Inneres (außer Standesämter)<br>I: Systemkoordination |
| App. 405 | Q: Beratung der behördlichen und betrieblichen Datenschutzbeauftragten, Organisation des Datenschutzes, Unterrichtung nach § 24 Abs. 3 Satz 3 BlnDSG, nichtautomatisierte Datenverarbeitung, Führung des Registers nach §§ 4d, 4e BDSG<br>R: Verfassungsorgane, Senatskanzlei, Justiz, Finanzen, Wirtschaft<br>I: Behördlicher Datenschutzbeauftragter |
| App. 404 | Q: Datenschutz und IT-Sicherheit im Internet<br>R: Schule, Bildung, Wissenschaft, Forschung |
| App. 411 | Q: Informationstechnik im Gesundheitswesen, Kryptographie, Anonymisierung, Pseudonymisierung, Normung<br>R: Gesundheitswesen |

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

# Stichwortverzeichnis

## A



## B

## C / D



## E



## F / G



## H

## I



## J / K



## L



## M

## N / O



## P



## Q / R



## S

## T



## U / V



## W



## Z

## Veröffentlichungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit

**Tätigkeitsberichte:** Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über seine Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. 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

Intelligente Stromnetze – Smart Grids • Auslegungsprobleme beim novellierten Bundesdatenschutzgesetz • Videoüberwachung an Schulen • Zugriffsregelungen in Krankenhausinformationssystemen • Datenerhebung für den Europäischen Sozialfonds • Private Meldedatenpools zur Adressermittlung • Datenschutz und Virtualisierung • Kfz-Kennzeichenscanning • Den Datensündern auf der Spur – Entwicklung der Bußgeldpraxis • Berliner Kinderschutzgesetz datenschutzrechtlich tragbar • Versorgungsforschung der Krankenkassen – noch eine zentrale Datenbank? • Elektronische Gesundheitskarte • Lehramtsanwärter auf Herz und Nieren geprüft • Forschung mit Friedhofsdaten • Fragebogen im Betriebspraktikum • Was wäre die Schule ohne Hausaufgaben? • Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) • Cold Calls und kein Ende • Was Programme so ausplaudern • Behördliche Datenschutzbeauftragte • Das Recht am eigenen Bild • Informationsfreiheit in Berlin