Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2011

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung alle zwei Jahre einen Bericht über ihre Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz, § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 22. März 2010 vorgelegten Tätigkeitsbericht 2008/2009 an und deckt den Zeitraum vom 1. Januar 2010 bis zum 31. Dezember 2011 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter

http://www.lda.brandenburg.de

abgerufen werden.

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Fax: 033203 356-49

E-Mail: Poststelle@LDA.Brandenburg.de
Internet: http://www.lda.brandenburg.de

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Druckerei Pietsch, Kloster Lehnin

Inhaltsverzeichnis

Anlagen

Einleitung

Unser derzeitiges Datenschutzrecht ist zu einer Zeit entstanden, als die moderne Datenverarbeitung und das Internet noch in ihren Kinderschuhen steckten. Von weltweit tätigen Unternehmen oder so genannten sozialen Netzen war keine Rede, als das Brandenburgische Datenschutzgesetz, das Bundesdatenschutzgesetz oder die Europäische Datenschutzrichtlinie verabschiedet wurden. In der Zwischenzeit haben Globalisierung und technologische Entwicklung unseren Alltag rasant verändert. Kaum jemand kann oder will sich den daraus unzweifelhaft entstandenen Vorteilen verschließen: Digitale Kartendienste, Mobilfunk oder die Pflege sozialer Kontakte im Internet sind für viele eine Selbstverständlichkeit geworden. In den beiden zurückliegenden Jahren führte die Öffentlichkeit aber auch eine teilweise recht intensive Diskussion über den Datenschutz bei der Nutzung solcher Dienste. Die Risiken der Technologien rückten allmählich ins Bewusstsein: Bildaufnahmen im Internet, Ortungstechnik oder die kinderleichte Erstellung von Persönlichkeitsprofilen.

Ziel der Datenschutzbeauftragten des Bundes und der Länder ist es, das Recht auf informationelle Selbstbestimmung angesichts der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung zu gewährleisten. Ihr gemeinsames Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ weist auf die Unzulänglichkeiten der bestehenden Datenschutzregelungen hin und skizziert die wesentlichen Empfehlungen der Datenschutzbeauftragten zur Weiterentwicklung der gesetzlichen Grundlagen in der Bundesrepublik Deutschland. Die Notwendigkeit für eine solche Anpassung wird auch auf der Ebene der Europäischen Union gesehen. So hat die Europäische Kommission für den 25. Januar 2012 einen Entwurf zur Neuordnung des Datenschutzrechts angekündigt und signalisiert, dabei nicht nur den wichtigen Ansatz der Technikneutralität der Regelungen, sondern auch die grenzüberschreitende Datenverarbeitung zu berücksichtigen. Die Diskussion dieses umfassenden Entwurfs eines gemeinschaftlichen Rechtsrahmens wird zum Zeitpunkt der Veröffentlichung meines Tätigkeitsberichts gerade in vollem Gange sein.

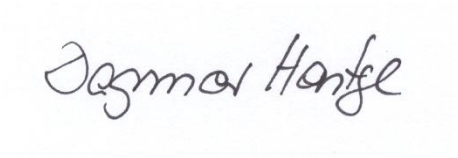
Flankiert wird die Debatte von wegweisenden gerichtlichen Entscheidungen: So hat das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung den Schutz des Einzelnen deutlich gestärkt. Der Europäische Gerichtshof entschied für die unabhängige Kontrolle des Datenschutzes auch in Brandenburg. Durch die Zusammenführung der Datenschutzaufsicht bei der Landesbeauftragten bin ich nunmehr auch für die Aufsicht über den nichtöffentlichen Bereich zuständig. Zahlreiche Beiträge meines Tätigkeitsberichts zeigen, wie wichtig hier eine effektive Kontrolle ist. Im Berichtszeitraum habe ich mich unter anderem mit intelligenten Stromzählern, der Datenverarbeitung

durch Auskunfteien, dem Scoring und dem Schutz von Gesundheitsdaten in privaten Arztpraxen beschäftigt. Aber auch Datenschutzverstöße öffentlicher Stellen zeigen, dass dort teilweise noch Überzeugungsarbeit zu leisten ist. So habe ich die Einführung umfangreicher Verfahren zur Datenverarbeitung auf Landesebene begleitet. Meine Behörde hatte praktische Fragen beispielsweise des Sozialdatenschutzes ebenso zu bearbeiten wie solche zur Einführung des neuen Personalausweises. Zwei Themen haben mich in den beiden zurückliegenden Jahren besonders beschäftigt: die Videoüberwachung und der Zensus 2011.

Auch die Informationsfreiheit war im Berichtszeitraum aktueller denn je. Dass der gesellschaftliche Bedarf an Transparenz zugenommen hat, war den kontroversen Debatten um die Enthüllungsplattform WikiLeaks deutlich zu entnehmen – auch wenn man die Plattform selbst durchaus kritisch bewerten mag. Die rechtlichen Grundlagen der Informationsfreiheit werden auf der Ebene der Europäischen Union, im Bund und in zahlreichen Ländern evaluiert und novelliert – eine Entwicklung, der sich das Land Brandenburg bislang leider verschließt.

Mein 16. Tätigkeitsbericht informiert über diese Entwicklungen sowie über zahlreiche Einzelfälle, die in den Jahren 2010 und 2011 zu bearbeiten waren. Ihnen, liebe Leserinnen und Leser, wünsche ich eine interessante Lektüre.

Kleinmachnow, den 6. März 2012



Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Videoüberwachung

1.1.1 Rechtliche Aspekte

Wenn Privatpersonen oder Unternehmen öffentlich zugängliche Räume per Video überwachen wollen, stellt sich die Frage, welche Grundrechte schwerer wiegen: der Anspruch der Überwachten, in Ruhe gelassen zu werden, oder das Recht, das Eigentum oder den Betrieb zu schützen?

Bereits in der Vergangenheit haben wir uns wiederholt zum Einsatz von Videoüberwachung durch staatliche Stellen im öffentlichen Raum geäußert. Rechtsgrundlage hierfür ist § 33c Brandenburgisches Datenschutzgesetz. Mit Übertragung der Aufsichtsbefugnisse auch für den nicht-öffentlichen Bereich ist die Landesbeauftragte nunmehr auch für die Kontrolle der Videoüberwachung durch private Stellen zuständig. Sowohl von Unternehmen als auch von Privatpersonen werden vielfältige Gründe vorgetragen, um den Einsatz von Kameras zu rechtfertigen.

Aufnahmen von Personen können in deren Persönlichkeitsrechte – insbesondere in deren Recht auf informationelle Selbstbestimmung und in das Recht am eigenen Bild – eingreifen. Umgekehrt kann sich auch derjenige, der das Bildmaterial anfertigt, auf eigene Rechte berufen. Er macht beispielsweise geltend, sein Eigentum oder seine persönliche Sphäre vor Übergriffen schützen zu wollen. Anders als öffentliche Stellen können Private sich somit darauf stützen, mit den Aufnahmen ihre eigenen Grundrechte wahrzunehmen. Die Ausübung der Grundrechte der einen Seite kann also gleichzeitig einen Eingriff in die Grundrechte der anderen Seite darstellen. Für die Entscheidung darüber, ob und in welchem Umfang die Videoüberwachung erlaubt ist, bedarf es einer Abwägung zwischen den beteiligten Rechtsgütern. Das Ergebnis hängt von den speziellen örtlichen, zeitlichen und persönlichen Umständen in jedem Einzelfall ab.

Grundsätzlich steht es jedem in seiner eigenen Privatsphäre frei, Videoüberwachungsanlagen zu installieren. Eine Kamera, die z. B. nur das eigene Grundstück oder die eigene Wohnung erfasst, ohne deren räumliche Grenzen zu überschreiten, ist daher in aller Regel aus datenschutzrechtlicher

Sicht unproblematisch. Selbstverständlich darf aber auch in diesen Fällen keine heimliche Aufzeichnung von Besuchern erfolgen.

Datenschutzrechtlich sind vor allem solche Videoaufnahmen relevant, die nicht nur den eigenen privaten Raum erfassen, sondern auch geeignet sind, in die Rechte Dritter einzugreifen. Dies ist beispielsweise der Fall, wenn Kameras im Rahmen der Überwachung des eigenen Grundstücks auch allgemein zugängliche Örtlichkeiten miterfassen (z. B. Straßen oder Fußwege) oder eigene, für die Öffentlichkeit zugänglich gemachte Räume beobachtet werden sollen (z. B. Geschäfte, Schwimmbäder oder Arztpraxen). Dabei spielt es keine Rolle, ob die Überwachung in Form permanenter Aufzeichnungen oder durch videotechnisch unterstützte, bloße Beobachtung erfolgt.

§ 6b Bundesdatenschutzgesetz (BDSG) regelt die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch nicht-öffentliche Stellen.

Der Anwendungsbereich des § 6b BDSG ist bereits dann eröffnet, wenn eine Videoanlage installiert wird, die technisch in der Lage ist, Bilder aufzuzeichnen oder auch nur zu beobachten, auch wenn dies von dem Verantwortlichen nur im Einzelfall vorgesehen ist.

Dagegen werden reine Attrappen nicht vom Anwendungsbereich des § 6b BDSG erfasst, da sie von vornherein technisch nicht in der Lage sind, Beobachtungen oder Aufzeichnungen vorzunehmen und der reinen Abschreckung dienen sollen. Weil durch die Verwendung von Attrappen der Eindruck entsteht, dass ein bestimmtes Areal überwacht wird, geht von diesen trotz nicht vorhandener technischer Fähigkeit zur Beobachtung oder Aufzeichnung ein (im Regelfall auch gewollter) Druck aus, sich in einer bestimmten Art und Weise zu verhalten bzw. bestimmte Handlungen zu unterlassen. Ein solcher Druck wird als Eingriff in die Rechtssphäre der Betroffenen gewertet. Zwar kann man dagegen zivilrechtliche Unterlassungsansprüche wegen eines Verstoßes gegen das allgemeine Persönlichkeitsrecht geltend machen. Ein Verstoß gegen das Bundesdatenschutzgesetz liegt jedoch nicht vor, da eine Verarbeitung von Daten oder Bildern nicht stattfindet.

Öffentlich zugängliche Räume sind solche innerhalb oder außerhalb von Gebäuden, die frei oder nach allgemeinen erfüllbaren Voraussetzungen, wie beispielsweise dem Lösen einer Eintrittskarte, betreten werden können. Im Gegensatz dazu sind Räumlichkeiten, die nur einem ganz bestimmten Personenkreis offen stehen sollen, in diesem Sinne nicht öffentlich. Dies gilt z. B. für umzäunte oder mit Hinweisschildern versehene Areale wie Werksgelände. Die Bewertung, ob ein Raum öffentlich zugänglich ist oder nicht, hängt immer auch vom Einzelfall ab: Ein Klub, der nur Mitgliedern Zutritt gewährt, wird in

diesem Sinne als nicht öffentlich zugänglich einzustufen sein, wohingegen eine Arztpraxis mit freien Sprechstunden für jedermann als öffentlich zugänglich betrachtet werden kann.

Die Installation einer Videoüberwachung in öffentlich zugänglichen Räumen ist nur zur Wahrung des Hausrechts oder bei Vorliegen eines berechtigten Interesses erlaubt. Letzteres kann für ein Kaufhaus darin liegen, Diebstähle zu verhindern oder für einen Hauseigentümer, das Beschmieren oder Beschädigen der Fassade zu vermeiden. Der Zweck muss vor Installation der betreffenden Anlage schriftlich festgelegt und nachprüfbar dokumentiert werden.

Darüber hinaus muss die Anlage auch erforderlich sein, um das (Überwachungs-) Ziel zu erreichen. Im Einzelfall müssen weniger einschneidende Mittel wie etwa regelmäßige Kontrollgänge durch Bewachungspersonal auf ihre Tauglichkeit geprüft werden. Zugleich muss in diesem Zusammenhang darüber befunden werden, ob ein punktueller Einsatz der Technik zur Erreichung des Ziels ausreicht. Er ist einer flächendeckenden Kameraüberwachung stets vorzuziehen. Zu erwägen ist auch eine zeitliche Begrenzung des Technikeinsatzes. In vielen Fällen reicht es aus, eine Überwachung nur in den Nachtzeiten vorzunehmen, da in der belebteren Tageszeit aufgrund des höheren Publikumsaufkommens kaum damit zu rechnen ist, das eine gut einsehbare Eingangstür aufgebrochen wird.

Schließlich kann eine Videoüberwachung sogar unzulässig sein, obwohl ein berechtigtes Interesse für ihren Einsatz vorliegt und ein weniger einschneidendes Mittel nicht existiert. Dies trifft immer dann zu, wenn die schutzwürdigen Interessen der (aufgenommenen) Betroffenen das Interesse an der Überwachung überwiegen. Das ist der Fall, wenn sensitive Daten z. B. aus dem Gesundheitsbereich erhoben werden oder sogar die Intimsphäre verletzt wird. Aus dem letztgenannten Grund dürfen weder Toiletten noch Umkleidekabinen überwacht werden.

Die Videoüberwachung öffentlich zugänglicher Räume ist Unternehmen oder Privatpersonen nur unter den engen Voraussetzungen des § 6b BDSG gestattet. Insbesondere muss sie für den beabsichtigten Zweck erforderlich sein. Schutzwürdige Interessen der Betroffenen dürfen nicht überwiegen. In jedem Einzelfall sind die Grundrechte aller Beteiligten gegeneinander abzuwägen.

1.1.2 Technisch-organisatorische Aspekte

Öffentliche und nicht-öffentliche Stellen dürfen unter bestimmten Voraussetzungen öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen überwachen. Die einschlägigen Rechtsgrundlagen finden sich in § 33c Brandenburgisches Datenschutzgesetz (BbgDSG) bzw. § 6b Bundesdatenschutzgesetz (BDSG). Eine datenschutzkonforme Installation der Anlage sowie ihr datenschutzkonformer Betrieb erfordern immer auch angemessene technische und organisatorische Maßnahmen.

Die Auswahl der technischen und organisatorischen Maßnahmen richtet sich nach den jeweils im Einzelfall zu betrachtenden Risiken für das Recht auf informationelle Selbstbestimmung der Beobachteten. Sie müssen für den Schutzbedarf der verarbeiteten personenbezogenen Daten sowie den Schutzzweck angemessen sein und dem aktuellen Stand der Technik entsprechen. Darüber hinaus sind die vor Ort gültigen Rahmenbedingungen zu beachten. Obwohl in der Regel keine Videoüberwachungsmaßnahme der anderen gleicht und für jede Installation die Angemessenheit und Wirksamkeit der getroffenen Maßnahmen überprüft werden muss, gibt es grundlegende Anforderungen, die für jede Videoüberwachung Gültigkeit haben und Ausgangspunkt für weitere Überlegungen sein sollten.

Im Vorfeld jeder Videoüberwachungsmaßnahme muss die Überwachungsart festgelegt werden – diese Entscheidung hat erhebliche Auswirkungen auf die Auswahl und Ausgestaltung der erforderlichen technischen und organisatorischen Maßnahmen. Werden die zu installierenden Kameras lediglich zur Beobachtung eingesetzt (d. h. ohne eine Aufzeichnung), sind die Anforderungen an die technischen und organisatorischen Maßnahmen wegen der geringeren Eingriffstiefe in die Persönlichkeitsrechte der Betroffenen weniger hoch. Werden die erfassten Daten für eine mögliche Weiterverarbeitung gespeichert, sind zusätzliche Maßnahmen erforderlich.

Auch die Wahl der Überwachungstechnik hat Einfluss auf die Bewertung der Risiken für die schutzwürdigen Interessen Betroffener. Bisher wurden meist analoge Kameras verwendet, die ihre Bilder über ein Koaxialkabel an einen Monitor übertragen und in der Regel eigenständig arbeiten. Zunehmend sind jedoch Kameras im Einsatz, die eine direkte Einbindung in ein Rechnernetz ermöglichen (z. B. über eine IP-Netzschnittstelle). Bei derartigen Kameras werden die Bildinformationen in einem Signalprozessor oder direkt im Bildsensor digitalisiert und anschließend als Datenpakete über das IP-Netz an eine zentrale Stelle (meist einen Videoserver) übertragen. Netzkameras verwenden überwiegend Bildsensoren mit einer hohen Auflösung, die auch ein digitales Vergrößern ermöglichen. Eingebunden in ein bestehendes IP-

Netz und ausgestattet mit zusätzlichen Eigenschaften, wie z. B. einem Schwenk-Neigekopf in alle Richtungen und Motor-Zoom-Objektiven, können sie zu perfekten, ferngesteuerten Überwachungsinstrumenten werden.

Durch die Umsetzung technischer und organisatorischer Maßnahmen gem. § 10 BbgDSG bzw. § 9 BDSG und dessen Anlage 1 muss die jeweilige verantwortliche Daten verarbeitende Stelle gewährleisten, dass bei einer Videoüberwachung u. a. die Vertraulichkeit, Integrität, Authentizität, Revisionsfähigkeit und Transparenz der Verarbeitung personenbezogener Daten der Betroffenen gesichert werden. Der Einsatz von Netzkameras in IP-Netzen bedarf aufgrund des erhöhten Gefährdungspotenzials dieser Technik und der Vernetzung mit anderen Komponenten in der Regel besonderer Maßnahmen, erst recht bei einem Anschluss einer solchen Anlage an das Internet. Die verantwortliche Stelle muss in jedem Fall, z. B. für die Verschlüsselung der Kommunikation zwischen Kameras und Videoserver, die rechentechnische Abschottung des gesamten Netzes, die strikte Sicherung des Zugangs zu einzelnen Komponenten und den Schutz gegen unberechtigten Zutritt zu relevanten Betriebsräumen sorgen. Eine detaillierte Risikoanalyse hilft hier, die Gefährdungslage zu erkennen und zu bewerten. Sie bietet die Möglichkeit, speziell auf die Risiken abgestimmte Maßnahmen zu identifizieren und umzusetzen. Bei umfangreicheren Installationen müssen diese Überlegungen in einem umfassenden IT-Sicherheitskonzept münden.

Vielfach haben wir im Zuge unserer Aufsichts- und Kontrolltätigkeit festgestellt, dass der technisch mögliche Erfassungsbereich einer Kamera weit über den Bereich hinausgeht, der für die Erreichung des mit der Videoüberwachung angestrebten Zwecks erforderlich ist. Die Beobachtung oder gar Aufzeichnung von Videosequenzen dieser Bereiche ist nicht erforderlich und widerspricht dem Prinzip der Datenvermeidung und Datensparsamkeit. Werden sogar der Öffentlichkeit gewidmete Straßen, Wege oder Plätze auf solche Weise überwacht, ist dies rechtswidrig. Die verantwortliche Stelle muss daher sicherstellen, dass derartige Bereiche ausgeblendet werden. Dazu dienen mechanische Vorrichtungen zum Abdecken von Bereichen des Objektivs der Kamera oder auch das softwareseitige Verpixeln (Privacy Zone Masking) von Ausschnitten der aufgenommenen Bilder bzw. Videos.

Jede Videoüberwachung unterliegt einer strengen Zweckbindung, die vor Inbetriebnahme eindeutig festgelegt werden muss. Werden in der Überwachungsphase mit der Anlage keine Ereignisse registriert, die eine weitere Auswertung der Bilder bzw. Videos erforderlich machen, entfällt die Erforderlichkeit der Datenverarbeitung. Diese Daten sind dann unverzüglich automatisiert zu löschen. In der Regel sind Speicherfristen von 48 Stunden ausreichend. Im Ereignisfall, der zur Auswertung führen soll, kann eine manuelle Sperre aktiviert werden, die das Löschen von Beweismaterial verhindert.

Von erheblicher Bedeutung für den Datenschutz und die Datensicherheit eines Videoüberwachungssystems ist auch die revisionssichere Protokollierung der administrativen Tätigkeiten. Mindestens jede Veränderung am System (z. B. des Erfassungsbereichs), jede Authentisierung von Nutzern sowie jede Einsicht und Auswertung der gespeicherten Videosequenzen müssen protokolliert werden. Für eine datenschutzkonforme Gestaltung müssen die Art und Weise sowie der Umfang der Auswertung unter Beachtung der engen Zweckbindung der Protokolldaten vorab festgelegt werden. Ratsam ist die Beteiligung des behördlichen bzw. betrieblichen Datenschutzbeauftragten. Dieser sollte im Rahmen des Vier-Augen-Prinzips ohnehin zur Sichtung der Protokolldaten hinzugezogen werden. Darüber hinaus ist er auch für die Erstellung der Vorabkontrolle gem. § 10a BbgDSG bzw. § 4d Abs. 5 BDSG verantwortlich. Diese wird erforderlich, da mit der Videoüberwachung in der Regel besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden sind.

Zur Herstellung von Transparenz gehört es auch, den Umstand der Videoüberwachung öffentlich zugänglicher Räume gem. § 33c Abs. 2 BbgDSG bzw. § 6b Abs. 2 BDSG durch geeignete Maßnahmen kenntlich zu machen. Wir empfehlen die Nutzung des einheitlichen Piktogramms gemäß DIN 33450. Ferner muss für den Betroffenen zweifelsfrei identifizierbar sein, wer für die Videoüberwachung verantwortlich ist.

Der Einsatz von Videoüberwachungssystemen kann besondere Risiken für das Recht auf informationelle Selbstbestimmung mit sich bringen. Daher müssen umfangreiche technische und organisatorische Maßnahmen getroffen werden, die einen datenschutzkonformen Betrieb ermöglichen.

1.1.3 Einzelfälle

1.1.3.1 Videoüberwachung in einem Schnellrestaurant

Ein Petent beschwerte sich, dass er bei einem Besuch eines Schnellrestaurants gefilmt und die Videoaufzeichnung seiner Meinung nach unrechtmäßig ausgewertet wurde. Außerdem habe ein Hinweisschild auf die Videoüberwachung gefehlt.

Die Beschwerde haben wir zum Anlass genommen, das als Franchiseunternehmen geführte Restaurant hinsichtlich der Videoüberwachung vor Ort zu kontrollieren. Im Vorfeld der Kontrolle wurde uns ein Videoüberwachungskonzept des Franchisegebers zur Verfügung gestellt, das bereits von der zuständigen Datenschutzaufsicht geprüft worden war. An dieses Konzept hatten sich alle Franchisenehmer zu halten. Seine Umsetzung war gleichfalls Gegenstand unserer Kontrolle.

Die Prüfung vor Ort brachte datenschutzrechtliche Mängel zutage. So haben zwei Videokameras unerlaubter weise Teile des Gastraums überwacht. Nach unserem Hinweis wurde der Einstellwinkel der Kameras umgehend verändert. Grundsätzlich nicht zu bemängeln war die Videoüberwachung des Kassenbereichs.

Das Unternehmen speicherte die Videoaufzeichnungen erheblich zu lange – insgesamt sieben Tage. Es hielt sich damit nicht einmal an ihr eigenes Videoüberwachungskonzept. Empfohlen haben wir eine Speicherdauer von 48 Stunden. Diese Zeit genügt für die Erreichung des Beobachtungszwecks und damit zur Feststellung von Diebstählen, Sachbeschädigungen und Aufklärung von Sachverhalten hinsichtlich der Wahrnehmung des Hausrechts, da das Restaurant täglich geöffnet ist.

Der Petent hatte durch sein Verhalten während des Besuchs der Gaststätte Anlass zur Auswertung der Videoaufzeichnung gegeben – mit der Folge, dass ihm Hausverbot erteilt wurde. Hiergegen hatten wir keine datenschutzrechtlichen Bedenken.

Die Beschwerde des Petenten über das Fehlen der Piktogramme stellte sich als unbegründet heraus. Alle Ein- und Ausgangstüren waren mit genormten Hinweisschildern versehen.

Das Unternehmen war während der Vor-Ort-Prüfung nicht in der Lage, uns für den Betrieb der Videoüberwachungsanlage das Verfahrensverzeichnis, den Wartungsvertrag und die Unterlagen zur Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten vorzulegen. Nach schriftlicher Aufforderung wurde uns zunächst ein Teil der angeforderten Dokumente zugesandt.

Soweit erforderlich, sind Videoüberwachungsmaßnahmen auch in Gaststätten zulässig, wenn nicht Teile des Gastraums überwacht werden. Eine Auswertung der Aufnahmen für den festgelegten Beobachtungszweck ist möglich.

1.1.3.2 Videoüberwachung im Ruheraum einer Therme

Den Ruheraum einer Therme suchen die Gäste normalerweise auf, um sich zu entspannen. Entdecken sie aber zufällig eine Videokamera, ist es mit der Erholung häufig nicht mehr so weit her. Ist eine solche Beobachtung im Ruheraum überhaupt zulässig?

Der Gast einer Therme hatte sich darauf gefreut, den Tag mit einem ungestörten Aufenthalt im Ruheraum ausklingen zu lassen. In der Ecke des Raumes fiel ihm jedoch ein halbrunder Gegenstand auf, den er für eine Kamera

hielt. An keiner Stelle des Bades fand er jedoch ein entsprechendes Hinweisschild. Beim Blick durch das Fenster der Beckenaufsicht bestätigte sich sein Verdacht: Ein Monitor zeigte deutlich die Liegen im Ruheraum. Jeder, der wollte, konnte die Übertragung sehen.

Wir nahmen die Beschwerde des Badegastes zum Anlass, die Videoüberwachung in der Therme zu überprüfen. Es stellte sich heraus, dass innerhalb des Gebäudes sechzehn Kameras installiert waren, die neben dem Ruheraum auch den Eingangsbereich sowie die Wertschließfächer überwachten. Als Grund für die Beobachtung des Ruheraums wurde uns erklärt, dass sich dort zuvor ein Badebereich für Kinder befunden habe. Die Erforderlichkeit der fortgeführten Videoüberwachung in dem nunmehr als Ruheraum genutzten Abschnitt legte der Betreiber jedoch nicht dar. Es bestand zudem keine sinnvolle Möglichkeit, die Kamera so auszurichten, dass die Badegäste nicht mehr im Blickfeld sind. Wir forderten deshalb, die Kameras abzubauen.

Die Erforderlichkeit der Videoüberwachung der Eingänge und Wertschließfächer stand aus unserer Sicht zwar nicht infrage, wir machten den Betreiber der Therme aber auf die Verpflichtung aufmerksam, sie mit den entsprechenden Hinweisschildern zu kennzeichnen. Es war außerdem zu verhindern, dass Unbefugte weiterhin ohne Schwierigkeiten die Monitore der Beckenaufsicht einsehen können. Um dies zu erreichen, haben wir empfohlen, die Bildschirme im Aufsichtsraum so umzustellen, dass sie den Blicken Neugieriger verborgen bleiben. Unseren Forderungen ist der Betreiber nachgekommen.

Die Videoüberwachung von Ruheräumen in einer Therme ist nicht erforderlich. Das schutzwürdige Interesse der Gäste gebietet den Abbau der Kameras.

1.1.3.3 Überwachung eines öffentlich zugänglichen Privatwegs?

Unmittelbar neben einem großen Einkaufszentrum verläuft ein privater Gehweg, der von Kunden und Anwohnern häufig genutzt wird. Als der Betreiber an seinem Gebäude Kameras anbrachte, die auch den Weg im Blick hatten, beschwerten sich Passanten. Darf der Eigentümer auf seinem eigenen Weg die Videoüberwachung nach Belieben einsetzen?

Der Betreiber des Einkaufszentrums begründete das Erfordernis zur Videoüberwachung mit den in der Vergangenheit aufgetretenen Schäden durch Vandalismus und Diebstahl. Seine Versicherung sei nicht mehr bereit, ohne entsprechende Maßnahmen weiterhin für die Schäden aufzukommen. Außerdem sollte die Überwachung die zunehmende, illegale Abfallentsorgung am Rande des Gehwegs eindämmen. Auf die Videoüberwachung werde

zudem mit entsprechenden Schildern hingewiesen, die auch den Verantwortlichen für die Überwachung eindeutig benennen.

Als wir die Videoüberwachung vor Ort kontrollierten, stellte sich heraus, dass die Videoüberwachung 24 Stunden täglich ohne Unterbrechung erfolgte. Zwar machten die Kameras die Aufnahmen der gegenüberliegenden Wohnhäuser automatisch unkenntlich, zeigten von den Fußgängern, die den Privatweg nutzten, aber deutliche Bilder. Dieser öffentlich zugängliche Weg wurde von den Kameras über eine Entfernung mehrerer Meter von der Außenwand des Gebäudes erfasst.

Die Videoüberwachung öffentlich zugänglicher Räume ist ausschließlich in einem engen Abstand zwischen dem Gebäude und dem Gehweg zulässig. Da der Betreiber nicht bereit war, die Reichweite der Kameras entsprechend einzuschränken, blieben nur zwei Alternativen: Entweder wird auf die Videoüberwachung verzichtet oder der Privatweg für die Nutzung durch die Öffentlichkeit gesperrt. Der Betreiber entschied sich für die letztgenannte Variante und stellte am Beginn und Ende des Gehwegs Hinweisschilder auf, die dessen öffentliche Nutzung untersagen.

Die Überwachung eines öffentlich zugänglichen Weges durch private Grundstückseigentümer ist nur mit Einschränkungen zulässig. Die Eigentümer können Kameras auf öffentlich zugänglichen Privatgrundstücken nur dann uneingeschränkt einsetzen, wenn sie die Öffentlichkeit erkennbar von der Nutzung ausschließen.

1.1.3.4 Unzulässige Videoüberwachung in Werbefilm dokumentiert

Eine Familie beschwerte sich bei uns, dass die Zufahrt zu ihrem Wohngrundstück sowie das davor liegende öffentliche Straßenland durch eine Videoanlage überwacht werden. Ein frei im Internet zugänglicher Verkaufsfilm eines Immobilienmaklers hatte dies dokumentiert.

Nach einer ersten Sichtung des Films wandten wir uns an den Betreiber der Videoüberwachung. Dies war offensichtlich der Eigentümer des Grundstücks auf der gegenüberliegenden Straßenseite. Er bestätigte, dass er beabsichtigte, sein Grundstück und das darauf befindliche Wohnhaus zu verkaufen und hierfür einen Immobilienmakler mit der Vermarktung – auch im Internet – beauftragt hatte. Sowohl im Verkaufstext als auch in dem zugehörigen Video wurde mit der Überwachung des Carports und der dort untergestellten Kraftfahrzeuge geworben. Das Video enthielt auch beispielhaft Bilder der Überwachungskamera.

Obwohl bei jedem Aufruf der fraglichen Internetseite die gleiche Filmsequenz gezeigt wurde und darauf keine Personen zu sehen waren, dokumentierte das Video jedoch, dass eine Beobachtung der Zufahrt zum Grundstück der Petenten und der davor liegenden Straße über die installierte Videoanlage möglich war. Wir forderten den Betreiber deshalb auf, den Einstellwinkel der Kamera so zu verändern, dass nur das eigene Grundstück erfasst wird. Er kam dieser Aufforderung nach.

Werden Videoüberwachungsanlagen zur Wahrnehmung des Hausrechts eingesetzt, sind die Kameras so einzustellen, dass kein öffentliches Straßenland erfasst oder Persönlichkeitsrechte der Nachbarn verletzt werden.

1.1.3.5 Abmahnung eines Falschparkers wegen Videoüberwachung?

Ein Autofahrer stellte sein Fahrzeug auf dem Kundenparkplatz eines Getränkemarktes ab. Einige Wochen später erhielt er eine gebührenpflichtige Abmahnung durch einen Rechtsanwalt. Dieser warf ihm vor, in der fraglichen Zeit gar nicht Kunde des Marktes gewesen zu sein. Die Abmahnung, so beschwerte sich der Autofahrer, sei durch eine unzulässige Videoüberwachung auf dem Kundenparkplatz erst möglich geworden.

Grund für die Annahme einer unzulässigen Videoüberwachung war der Hinweis des Rechtsanwalts auf ein vorhandenes Beweisfoto. Das von uns zur Stellungnahme aufgeforderte Unternehmen teilte zwar mit, dass eine Videokamera betrieben werde. Diese sei jedoch ausschließlich auf den Eingangsbereich zum Ladengeschäft gerichtet; eine Überwachung des unternehmenseigenen Parkplatzes bzw. eine dadurch mögliche Erfassung der Kfz-Kennzeichen per Video erfolge nicht. Das Unternehmen habe die Kameras im Übrigen erst nach mehreren bewaffneten Raubüberfällen auf Anraten der Polizei installiert. Das vom Rechtsanwalt erwähnte Beweisfoto sei vielmehr von einem beauftragten Unternehmen gefertigt worden. Unter anderem überwache dieses die Einhaltung der Parkplatzregelungen, um das widerrechtliche Abstellen von Fahrzeugen auf dem Kundenparkplatz einzudämmen.

Unsere Kontrolle vor Ort ergab, dass die Videoüberwachung des Ladengeschäfts datenschutzrechtlich nicht zu beanstanden war. Die von dem Unternehmen geschilderten Umstände trafen zu: Der Kundenparkplatz war eindeutig als solcher ausgewiesen und die Bedingungen zum Abstellen von Fahrzeugen klar erkennbar. Die vermutete Videoüberwachung des Parkplatzes fand nicht statt.

Die Abmahnung wegen Falschparkens basierte nicht auf einer Videoüberwachung. Aus datenschutzrechtlicher Sicht waren die Abmahngebühren, die der Autofahrer zu tragen hatte, nicht zu beanstanden.

1.1.3.6 Videoüberwachung öffentlichen Straßenraums durch eine Privatperson?

Um Sachbeschädigungen an seinem Auto auf die Spur zu kommen und die Attraktivität seiner Homepage zu steigern, beobachtete eine Privatperson mit drei Videokameras das öffentliche Straßenland und stellte die Bilder live ins Internet. Passanten fühlten sich dadurch beobachtet.

Es bedurfte mehrerer deutlicher Hinweise auf die Rechtslage, der Einleitung eines Ordnungswidrigkeitenverfahrens sowie zweier Vor-Ort-Kontrollen, um die unzulässige Videoüberwachung zu unterbinden. Der Bundes- als auch der Landesgesetzgeber haben der Videoüberwachung klare Grenzen gesetzt. Erlaubt ist die Überwachung nur dann, wenn die Voraussetzungen des § 6b Bundesdatenschutzgesetz, § 33c Brandenburgisches Datenschutzgesetz oder § 31 Brandenburgisches Polizeigesetz vorliegen.

Der Betreiber der Videokameras hatte eine öffentlich zugängliche Straße unzulässigerweise beobachtet. Dieses Recht wird ausschließlich der Polizei eingeräumt. Sie kann öffentlich zugängliche Straßen und Plätze mittels Bildübertragung offen beobachten, wenn und solange aufgrund von Lageerkenntnissen Tatsachen die Annahme rechtfertigen, dass an diesen Orten vermehrt Straftaten drohen. Die polizeilichen Befugnisse darf sich ein Bürger nicht zu eigen machen, um selbsttätig Sachbeschädigungen aufzuklären.

Die Liveübertragung der Kamerabilder ins Internet zur Steigerung der Attraktivität der eigenen Homepage war erst recht kein Argument für die Videoüberwachung.

Wir haben letztendlich durchgesetzt, dass der Bürger zwei der Kameras deaktivierte und die dritte in ihrem Einstellwinkel so veränderte, dass eine Beobachtung des öffentlichen Straßenlandes nicht mehr erfolgen konnte.

Öffentlich zugängliche Straßen und Plätze darf grundsätzlich nur die Polizei per Video überwachen. Privatpersonen dürfen sich deren Befugnisse nicht zu eigen machen.

1.1.3.7 Videoüberwachung von Müllcontainern in einer Wohnanlage

Eine Gemeindeverwaltung informierte uns, dass die Müllcontainer in einer Wohnanlage mit einer Videoanlage überwacht werden. Es war zu befürchteten, dass hierbei auch private Bereiche der Bewohner einbezogen sowie Passanten betroffen waren.

In seiner Stellungnahme teilte uns das mit der Verwaltung der Wohnanlage beauftragte Unternehmen mit, dass es in der Vergangenheit wiederholt und in erheblichem Ausmaß zu illegalen Müllentsorgungen – insbesondere von Sperrmüll – neben den Containern gekommen war und belegte dies mit zahlreichen Fotos. Der Versand von Rundschreiben sowie die direkte Ansprache der Bewohner führten zu keiner Verbesserung der Situation. Daraufhin fasste die Wohnungseigentümergemeinschaft den Beschluss, die Müllcontainer durch eine Videoanlage zu überwachen, um die illegale Entsorgung zu verhindern bzw. deren Verursacher nachträglich anhand der Aufzeichnungen ermitteln zu können.

Die Wohnungsverwaltung setzte diesen Beschluss um. Sie informierte uns, dass lediglich die Müllcontainer von der Videoüberwachung erfasst und Privatbereiche wie Wohnungsfenster oder Hauseingänge durch Schwärzung ausgeblendet werden. Die Auswertung der Videoaufzeichnungen erfolgt nur im Bedarfsfall, ansonsten werden sie automatisch überschrieben. Der Zutritt zu dem Betriebsraum ist nur dem Hausmeister möglich. Ein Passwortschutz soll unberechtigte Zugriffe verhindern. Durch ein Piktogramm wird auf die Überwachung hingewiesen.

Bei einer Vor-Ort-Kontrolle haben wir die Konfiguration der Anlage geprüft. Im Ergebnis forderten wir, die Speicherdauer der Videoaufzeichnungen auf 48 Stunden zu begrenzen (außer an Wochenenden und Feiertagen), die Videoüberwachung auf die Zeit zwischen 19 und 7 Uhr einzuschränken und den Einstellwinkel der Videokamera so zu verändern, dass nur ein geringerer Ausschnitt des Gehwegs erfasst wird. Unter den genannten Voraussetzungen kann die Videoüberwachung – zunächst befristet für 6 Monate – erfolgen. Dann ist zu prüfen, ob die Maßnahme weiter erforderlich ist.

Die Wohnungsverwaltung sagte die Umsetzung der Forderungen zu.

Zur Verhinderung bzw. Aufdeckung illegaler Müllentsorgungen in einer Wohnanlage kann unter bestimmten Voraussetzungen eine Videoüberwachung erforderlich sein. Wird im Ergebnis einer verpflichtenden Abwägung festgestellt, dass die schutzwürdigen Interessen der Bewohner überwiegen, darf die Maßnahme nicht durchgeführt werden.

1.2 Zensus 2011

Im Berichtszeitraum wurden die Vorbereitungen zum Zensus 2011 abgeschlossen und die sogenannte moderne Volkszählung weitgehend durchgeführt. Bereits in den vergangenen Tätigkeitsberichten[1] haben wir über die umfangreichen Vorbereitungsmaßnahmen berichtet.

1.2.1 Zensusausführungsgesetz

Die Europäische Union schrieb in ihrer Verordnung[2] vor, dass für das Jahr 2011 gemeinschaftsweite Volks- und Wohnungszählungen durchzuführen sind. In Deutschland ist dazu am 16. Juli 2009 das Zensusgesetz 2011 in Kraft getreten, welches die Rahmenbedingungen festlegt, unter denen die Volkszählung in Deutschland 2011 stattfindet. Dieses Bundesgesetz bedurfte landesrechtlicher Ausführungsgesetze. Mit der Verabschiedung des Brandenburgischen Zensusausführungsgesetzes[3] im September 2010 wurde die letzte rechtliche Voraussetzung für die Durchführung des Zensus im Land geschaffen.

Bei dem Gesetzgebungsverfahren wurde unsere Behörde von Anfang an vom zuständigen Ministerium des Innern eingebunden. Gesetzentwürfe und begleitende Konzepte für die Errichtung von Erhebungsstellen in Brandenburg wurden uns rechtzeitig und umfassend zur Verfügung gestellt. Auch in einer regelmäßig tagenden Arbeitsgruppe zur Vorbereitung des Zensus 2011 wirkten wir mit. Datenschutzrechtliche Probleme konnten so frühzeitig erkannt und behoben werden.

1.2.2 Begleitung der Vorbereitungen und der Durchführung des Zensus

Im April 2010 wurde unter Leitung des Amtes für Statistik Berlin-Brandenburg (AfSBB) die „AG Zensus 2011 – Erhebungsstellen Brandenburg“ ins Leben gerufen, die sich aus Vertretern des Ministeriums des Innern, des Städte- und Gemeindebundes, des Landkreistages, der Landkreise und kreisfreien Städte sowie unserer Behörde zusammensetzte und monatlich tagte.

In dieser AG wurden unter anderem eine Musterdienstanweisung für die Erhebungsstellen und eine Vorlage für den „Maßnahmenkatalog zum Sicherheitskonzept für die Erhebungsstellen“ erarbeitet.

---

1 vgl. Tätigkeitsbericht 2006/2007, A 5.3.4 und Tätigkeitsbericht 2008/2009, A 4.5.1

2 Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen (ABl. EU Nr. L 218, S. 14)

3 Gesetz zur Ausführung des Zensusgesetzes 2011 im Land Brandenburg vom 22. September 2010 (GVBl. I 2010, Nr. 29)

Auch eine technische Lösung für die Anbindung der Erhebungsstellen an das Amt für Statistik musste gefunden werden: Diese war so zu gestalten, dass die Abschottung zur Verwaltung gewährleistet war. Das AfSBB entschied sich für eine datenschutzfreundliche Lösung, bei der für die Zensusbearbeitung eigene, vom Amt bereitgestellte Clients und Router genutzt wurden, die über eine verschlüsselte Verbindung mit den zentralen Servern des Zensus-DV-Verfahrens kommunizierten.

Mit der Bestellung der Erhebungsstellenleitungen im Oktober 2010 wurde die Arbeitsgemeinschaft aufgelöst. Sie ging nahtlos in eine ebenso regelmäßig tagende Beratungsrunde der Erhebungsstellenleitungen über. Auch an diesen Beratungen nahm unsere Behörde teil.

1.2.3 Kontrollen von Erhebungsstellen

Vor dem Beginn der Erhebungen zum Stichtag 9. Mai 2011 prüfte unsere Behörde fünf der 30 Erhebungsstellen im Land Brandenburg. Dabei ging es insbesondere um die räumliche und personelle Trennung der Erhebungsstellen von der Verwaltung und die Anpassung der Musterdienstanweisung sowie des Maßnahmenkataloges zum IT-Sicherheitskonzept an die örtlichen Gegebenheiten.

Die räumlichen Bedingungen waren bei den kontrollierten Erhebungsstellen sehr unterschiedlich. Unabhängig davon, ob diese angemietete Objekte oder freie Kapazitäten der eigenen Verwaltungen nutzten, wurden die Vorgaben in allen Fällen umgesetzt.

Bei den Anpassungen der Musterdienstanweisungen an die jeweilige Verwaltungsstruktur und die örtlichen Gegebenheiten gab es nur wenige Mängel; die Vervollständigung des Maßnahmenkataloges zur IT-Sicherheit musste jedoch in den meisten Fällen angemahnt werden. Weiterhin kritisierten wir, dass das Verfahrensverzeichnis nach § 8 Brandenburgisches Datenschutzgesetz noch nicht vorlag. Dieser Umstand war darauf zurückzuführen, dass hierfür das AfSBB Vorarbeiten leisten musste, die im Zusammenhang mit dem gesamten IT-Sicherheitskonzept standen. Die Muster für die Verfahrensverzeichnisse für den Bereich der Erhebungsstellen wurden deshalb im Nachgang durch das AfSBB erstellt und anschließend an lokale Gegebenheiten angepasst.

Während der Erhebungsphase prüfte unsere Behörde vier weitere Erhebungsstellen ohne vorherige Ankündigung. Schwerpunkte hierbei waren die Abschottung der Erhebungsstellen, die Lagerung ausgefüllter Fragebögen und die Übergabe der Unterlagen an den Kurierdienst. Mängel konnten nicht festgestellt werden. Wir planen weitere Prüfungen in der Phase der Auflösung der Erhebungsstellen.

1.2.4 Kontrolle der IT-Sicherheit im Amt für Statistik Berlin-Brandenburg

Das Amt für Statistik Berlin-Brandenburg (AfSBB) ist eine gemeinsame Anstalt der Bundesländer Berlin und Brandenburg. Die Kontrolle der IT-Sicherheit durch unsere Behörde erfolgte deshalb in Kooperation mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit. Sie fand am Standort für das Projekt Zensus 2011 in Berlin statt. Im Vorfeld wurde uns dazu – leider erst nach längeren Diskussionen – durch das AfSBB das IT-Sicherheitskonzept übergeben, welches Voraussetzung für eine derartige Prüfung ist.

Positiv hervorzuheben ist, dass bei der Erstellung des Konzepts die Vorgehensweise nach IT-Grundschutz und die Standards 100-2 und 100-3 des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) konsequent eingehalten wurden. Auch die Auswahl von Sicherheitsmaßnahmen folgte grundsätzlich den Empfehlungen des BSI in den Grundschutzkatalogen. Damit wurde den IT-Sicherheitsleitlinien der beiden beteiligten Länder Rechnung getragen. Das Konzept berücksichtigte den hohen Schutzbedarf der verarbeiteten personenbezogenen Daten. Dementsprechend wurden auch sogenannte Zusatzmaßnahmen der Grundschutzkataloge im Konzept aufgenommen sowie ergänzende, selbst abgeleitete Sicherheitsmaßnahmen definiert, um den Gefährdungen bei der Verarbeitung von personenbezogenen Daten mit hohem Schutzbedarf zu begegnen.

Das vorgelegte IT-Sicherheitskonzept erwies sich als grundsätzlich geeignet, die mit der Verarbeitung personenbezogener Daten im Zensus-Projekt verbundenen Risiken zu beherrschen. Zu einigen wenigen Punkten haben wir das AfSBB jedoch zur Nachbesserung aufgefordert. Hierbei handelte es sich z. B. um die Begründung der Entbehrlichkeit von einzelnen Grundschutzbausteinen oder von Sicherheitsmaßnahmen oder die Ergänzung der noch unvollständigen Dokumentation des Umsetzungsstatus von IT-Sicherheitsmaßnahmen und des Realisierungsplanes.

Im Verlauf der Vor-Ort-Kontrolle in dem eigens für den Zensus 2011 angemieteten Objekt prüften wir auch die Abarbeitung der Fragebögen vom Post- bzw. Kuriereingang über die elektronische Beleglesung bis zu ihrer Lagerung. Datenschutzrechtliche oder IT-sicherheitstechnische Mängel wurden dabei nicht festgestellt.

1.2.5 Eingaben

Erfreulicherweise gab es zum Zensus 2011 neben allgemeinen Anfragen nur wenige Eingaben, denen wir nachgehen mussten. Dies dürfte darauf zurückzuführen sein, dass bei der Haushaltebefragung auf Stichprobenbasis im Land Brandenburg nur etwa 12% der Bevölkerung einbezogen wurden, der Fragenkatalog verhältnismäßig kurz war und es zum Zensus eine umfangreiche, den Datenschutz berücksichtigende Öffentlichkeitsarbeit durch das AfSBB und das Statistische Bundesamt gab.

Die meisten Anfragen gingen zum Thema Auskunftspflicht ein. Beschwerden gab es, weil bei der postalischen Befragung der Zugangscode für den Online-Fragebogen in manchen Fällen im Anschriftenfenster des Briefumschlages sichtbar war. Dies kam daher, dass die Umschläge für mehrere Fragebögen ausgelegt waren und bei der Versendung von nur einem Bogen dieser verrutschen konnte. Bei Folgebefragungen wurde in diesen Fällen ein Deckblatt in den Umschlag eingelegt.

Die ca. 4.300 freiwilligen Erhebungsbeauftragten (Interviewer) in Brandenburg haben sich – soweit uns bekannt – größtenteils datenschutzgerecht verhalten. Selten kam es vor, dass Erhebungsbeauftragte darauf drängten, den Fragebogen gemeinsam mit den Bürgern auszufüllen, um die höhere Aufwandsentschädigung zu erhalten. Weitere Alternativen (allerdings mit geringerer Aufwandsentschädigung für die Erhebungsbeauftragten) waren, den Fragebogen selbst auszufüllen und ihn per Post an das AfSBB zu senden oder online zu antworten – darauf wurde bereits in den Ankündigungsschreiben hingewiesen. In den Fällen, in denen es zu Vorkommnissen kam, wurde der Sachverhalt von der Erhebungsstellenleitung mit den Erhebungsbeauftragten ausgewertet.

Bei dem Projektteil der Gebäude- und Wohnungszählung kam es vor, dass Personen angeschrieben wurden, die keine Eigentümer eines Gebäudes oder einer Wohnung waren. Dies resultierte daher, dass die Anschriften aus verschiedenen Registern generiert wurden, in denen offensichtlich falsche oder veraltete Angaben gespeichert waren. Die betroffenen Personen mussten den Fragebogen trotzdem beantworten, da bei ihnen sonst automatisch das Mahnverfahren eingeleitet worden wäre. Sie hatten in diesen Fällen anzukreuzen, dass sie nicht der Eigentümer sind – somit war die Befragung für sie abgeschlossen. Die betroffenen Personen können sich selbstverständlich im AfSBB erkundigen, woher die fehlerhaften Daten stammten. Das AfSBB darf allerdings wegen des Rückspielverbotes von Daten aus statistischen Erhebungen diese Fehler nicht in den Registern der Verwaltung korrigieren lassen.

Bundesweit wurde das Problem aufgeworfen, dass bei der Online-Beantwortung der Fragebögen über eine SSL-verschlüsselte Verbindung die Seriennummer und der Fingerabdruck des SSL-Zertifikats des zentralen Zensus-Servers nicht überprüft werden konnten.

Das Statistische Bundesamt hat daraufhin die Angaben zur Überprüfung des Sicherheitszertifikates auf der Zensus-Webseite veröffentlicht. Dies war allerdings nur die zweitbeste Lösung, da diese Webseite Ziel eines Angriffs und damit einer Manipulation hätte werden können. Eine bessere Lösung wäre gewesen, die Informationen zum Zertifikat des Servers auf die Fragebögen zu drucken.

Der Zensus 2011 verlief bisher ohne größere datenschutzrechtliche Probleme. Durch die gut funktionierende Zusammenarbeit aller Verantwortlichen gelang es, Schwierigkeiten bereits im Vorfeld auszuräumen. Wir werden das Projekt bis zur Auflösung der Erhebungsstellen und der Vernichtung der Unterlagen weiter kritisch begleiten.

2 Entwicklungen des Datenschutzrechts

2.1 Unabhängige Aufsichtsbehörden – Datenschutz aus einer Hand

Der Europäische Gerichtshof hat in einem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland entschieden, dass die Einordnung von Datenschutzaufsichtsbehörden in die reguläre staatliche Verwaltung dem Unabhängigkeitsgebot der Datenschutzrichtlinie widerspricht. Hintergrund des Verfahrens war die Tatsache, dass einige Länder die Datenschutzaufsicht über nicht-öffentliche Stellen sowie öffentlich-rechtliche Wettbewerbsunternehmen in ihre Ministerialverwaltungen eingegliedert hatten. Auch in Brandenburg wurde die Aufsicht über den nicht-öffentlichen Bereich bis Mitte 2010 vom Ministerium des Innern ausgeübt.

Artikel 28 Abs. 1, Unterabsatz 2 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr fordert, dass die Aufsicht ihre Aufgaben in „völliger Unabhängigkeit“ wahrnimmt. Der Gerichtshof hat in seinem Urteil vom 9. März 2010[4] festgestellt, dass dies nur der Fall ist, wenn die Datenschutzkontrolle im nicht-öffentlichen Bereich ohne jede mittelbare oder unmittelbare Einflussnahme erfüllt wird. Bereits die Gefahr einer politischen Einflussnahme auf die

4 Rechtssache C-518/07

Kontrollstellen genügte dem Europäischen Gerichtshof, um deren Unabhängigkeit infrage zu stellen. Damit stellt das Urteil klar, dass sich die Forderung nach Unabhängigkeit nicht nur auf die notwendige Distanz zu den kontrollierten Stellen, sondern auch zur staatlichen Organisation bezieht.

Die Entscheidung des Europäischen Gerichtshofs musste durch die betroffenen Länder der Bundesrepublik Deutschland zügig umgesetzt werden. Zum Zeitpunkt des Urteils hatten die Regierungsfraktionen im Landtag Brandenburg bereits einen Gesetzentwurf eingebracht. Danach sollte die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich aus dem Ministerium des Innern ausgegliedert und der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zugewiesen werden. Angesichts der Forderungen des Gerichtshofs wurde der Gesetzentwurf auf Vorschlag des Ausschusses für Inneres unverzüglich angepasst: Die ursprünglich vorgesehene Rechtsaufsicht über die Landesbeauftragte bei der Ausübung der Datenschutzkontrolle im nicht-öffentlichen Bereich wurde gestrichen und das Gesetz am 6. Mai 2010 vom Landtag verabschiedet.[5] Mit seinem In-Kraft-Treten zum 1. Juni 2010 wurde die Datenschutzaufsicht in meiner Behörde zusammengeführt. Ich berate und kontrolliere seither sowohl die öffentlichen Stellen des Landes als auch die Unternehmen mit Sitz in Brandenburg. Außerdem wurde mir zusätzlich die Aufgabe der Durchführung von Ordnungswidrigkeitenverfahren im Falle entsprechender Verstöße gegen die Datenschutzgesetze übertragen.

Mein Vorschlag, die Dienststelle als oberste Landesbehörde einzurichten, fand leider keinen Eingang in das Gesetz. Ich hielt dies für erforderlich, um die völlige Unabhängigkeit auch im Personal- und Haushaltswesen umzusetzen.

Die Vorgaben des Europäischen Gerichtshofs werden inzwischen auch von allen übrigen Ländern eingehalten: In Schleswig-Holstein und im Saarland wird die Datenschutzkontrolle von Anstalten des öffentlichen Rechts ausgeübt. In Hessen, Berlin, Niedersachsen und Rheinland-Pfalz sind die Dienststellen der Datenschutzbeauftragten oberste Landesbehörden oder haben eine entsprechende Stellung, während der Freistaat Bayern ein zusätzliches Landesamt für die Datenschutzaufsicht über nicht-öffentliche Stellen eingerichtet hat. Die verbleibenden Länder haben ihre Aufsichtsbehörden bei den Landtagen eingerichtet, die Freie Hansestadt Bremen bei der Senatorin für Finanzen.

[5] Viertes Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 25. Mai 2010 (GVBl. I Nr. 21)

2.2 Modernisierung des deutschen Datenschutzrechts

Das auf dem Volkszählungsurteil des Bundesverfassungsgerichts basierende Bundesdatenschutzgesetz in seiner aktuellen Fassung stammt noch aus dem Jahre 1990; das ursprüngliche Brandenburgische Datenschutzgesetz aus dem Jahre 1992. Weder der umfassende Einsatz moderner Informationstechnik, noch die heute weitverbreitete Nutzung des Internets standen damals auf der Agenda. Von Web 2.0 war ebenso wenig die Rede wie von sozialen Netzwerken oder der fortschreitenden Globalisierung. Inzwischen ist aber weithin deutlich geworden, dass das Datenschutzrecht zur Beherrschung der Risiken dieser Entwicklungen für das Recht des Einzelnen auf informationelle Selbstbestimmung nur unzureichende Instrumente bereithält. Die letzten Novellierungen des Brandenburgischen Datenschutzgesetzes sowie des Bundesdatenschutzgesetzes haben zwar punktuelle Verbesserungen mit sich gebracht, eine umfassende Überarbeitung konnte damit aber nicht erreicht werden. Die Anpassung des Datenschutzrechts an die rasanten technischen und gesellschaftlichen Entwicklungen der letzten Jahre ist deshalb weiterhin dringend erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich ausführlich mit der Frage beschäftigt, wie ein modernes Datenschutzgesetz für das 21. Jahrhundert aussehen soll. Im Frühjahr 2010 stellten sie das Ergebnis in Form eines Eckpunktepapiers der Öffentlichkeit vor.[6] Besonders wichtig sind mir folgende Punkte:

- Weniger ist mehr – diese Devise gilt vor allem für die zahlreichen spezialgesetzlichen Grundlagen zum Datenschutz. In den vergangenen zwanzig Jahren sind sowohl im Landes- als auch im Bundesrecht derart viele bereichsspezifische Rechtsgrundlagen für die Datenverarbeitung entstanden, dass Verwaltungen, Unternehmen und Bürger sich nur schwer zurechtfinden. Abgesehen von den sicher auch weiterhin erforderlichen, speziellen Regelungen z. B. auf den Gebieten der öffentlichen Sicherheit und des Sozialrechts sollte künftig der Blick in die allgemeinen Datenschutzgesetze ausreichen, um die Rechtslage zu erkennen. Die Mehrzahl der bereichsspezifischen Datenschutzregelungen gehört daher ebenso auf den Prüfstand wie unverständliche Formulierungen.

- Um einen datenschutzrechtlichen Mindeststandard zu gewährleisten, sollten das Brandenburgische und das Bundesdatenschutzgesetz verbindliche datenschutzrechtliche Grundprinzipien enthalten. Beispielsweise dürfen der bereits normierte Grundsatz der Zweckbindung für die

[6] Das Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ ist auf der Website der LDA (http://www.lda.brandenburg.de) verfügbar.

Verwendung personenbezogener Daten oder das noch zu regelnde Verbot der Profilbildung nicht durch gegenläufige Bestimmungen infrage gestellt werden. Verstöße gegen solche Mindeststandards sollten mit angemessenen Sanktionen bewehrt sein.

- Ein technikneutraler Ansatz sollte sicherstellen, dass die Regelungen sich nicht mehr auf konkrete Verfahren und Anwendungen beziehen, sondern vielmehr für technologische Entwicklungen offen sind. Dies betrifft sowohl die zu kontrollierenden Datenverarbeitungen als auch die technisch-organisatorischen Maßnahmen, die zum Schutz des Rechts auf informationelle Selbstbestimmung und zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu ergreifen sind.

- Die Transparenz für die Betroffenen sollte bei der Modernisierung des Datenschutzrechts eine hohe Priorität haben; die Wahrnehmung von Auskunftsrechten muss erleichtert werden. In der aktuellen Diskussion über soziale Netzwerke wird deutlich, dass die Nutzer sich nur für oder gegen eine bestimmte Anwendung oder ein Verhalten entscheiden können, wenn sie wissen, wie der Anbieter mit ihren Daten umgeht. Vertrauen allein genügt nicht. Dies gilt vor allem für weltweit tätige Unternehmen, die unterschiedlichen, einzelstaatlichen Transparenzpflichten unterliegen.

Gerade die zuletzt beschriebenen Anforderungen an einen internationalen Datenschutz machen deutlich, dass nationale oder gar Landesgesetzgeber allein mit der Modernisierung des Datenschutzrechts noch keine zufriedenstellenden Ergebnisse werden erzielen können. Europarechtliche Regelungen sollten an dieser Stelle einen Rahmen setzen.

Jeder, der sich für die Modernisierung des Datenschutzrechts interessiert, ist herzlich eingeladen, sich auf der Grundlage des Eckpunktepapiers der Datenschutzbeauftragten an der Diskussion zu beteiligen.

2.3 Regelung des Datenschutzes durch die Europäische Union

Bereits im Jahre 2009 begann die Europäische Kommission mit der Überprüfung der mittlerweile über 15 Jahre alten EU-Datenschutzrichtlinie 95/46/EG und weiteren, ergänzenden Rechtsinstrumenten zur Gewährleistung des Rechts auf Datenschutz und den freien Datenverkehr. Neben der Überarbeitung der EU-Datenschutzrichtlinie und ihrer Modernisierung entsprechend den Herausforderungen neuer Technologien und der Globalisierung sollten klare und konsequente Datenschutzbestimmungen geschaffen, das Recht

des Einzelnen gestärkt und gleichzeitig der bürokratische Aufwand reduziert werden, um einen freien Datenverkehr im EU-Binnenmarkt zu gewährleisten.

Im Mai 2009 lud die Kommission zunächst zu einer Expertenkonferenz als Auftaktveranstaltung ein. Im Anschluss daran führte sie bis Ende 2009 eine öffentliche Konsultation durch. Außerdem wurden mehrere Studien in Auftrag gegeben. Ergebnis dieses Vorgehens war das am 4. November 2010 vorgelegte Gesamtkonzept für den Datenschutz in der Europäischen Union[7], das folgende Kernziele verfolgt:

- Stärkung der Rechte des Einzelnen, insbes. durch die Beschränkung der Sammlung und Nutzung personenbezogener Daten auf das absolut erforderliche Mindestmaß, klare und transparente Informationen und das „Recht auf Vergessen“,

- Stärkung des Binnenmarkts durch Verringerung des Verwaltungsaufwands für die Unternehmen und Gewährleistung gleicher Rahmenbedingungen,

- Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden, ggf. ihre Einbeziehung unter Berücksichtigung der Besonderheiten und Erfordernisse dieses Bereichs,

- Gewährleistung eines hohen Schutzniveaus bei aus der EU übermittelten Daten, u. a. die Verbesserung und Erleichterung des internationalen Datentransfers, das Anstreben desselben Schutzniveaus bei der Zusammenarbeit mit Drittstaaten und das weltweite Einsetzen für hohe Datenschutzstandards und die

- wirksamere Durchsetzung der Vorschriften, speziell die Stärkung und weitere Harmonisierung der Aufgaben und Befugnisse der Datenschutzbehörden und die bessere Zusammenarbeit und Abstimmung mit Blick auf eine konsequentere Anwendung der Datenschutzbestimmungen im gesamten Binnenmarkt.

Dieses Gesamtkonzept wurde von der Europäischen Kommission erneut zur Diskussion gestellt. Im Rahmen des Konsultationsverfahrens nahmen unter anderem der Bundesrat, die Bundesregierung sowie die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu Stellung. Sie begrüßten durchgehend das Vorhaben der Modernisierung und umfassenden Sicherstellung des Datenschutzes auf EU-Ebene.

---

7 KOM(2010) 609 endg.

Die Kommission hat angekündigt, ihren Vorschlag am 25. Januar 2012 zu veröffentlichen.

3 Technisch-organisatorische Entwicklungen

3.1 Cloud Computing

Cloud Computing[8] – die netzwerkgestützte Auslagerung der Informationsverarbeitung – wird von Privatanwendern, Behörden und Unternehmen zunehmend genutzt. Durch die „in der Wolke" lokalisierten Dienste soll eine schnelle, flexible, dynamisch anpassbare und bedarfsgerechte Bereitstellung von Ressourcen ermöglicht werden. Kosten werden vom Cloud-Anbieter nur nach der tatsächlichen Nutzung der Ressourcen in Rechnung gestellt. Die für das Cloud Computing erforderlichen technischen Rahmenbedingungen sind zwar weitestgehend geschaffen, allerdings treten bei der Berücksichtigung der datenschutzrechtlichen Vorgaben nach wie vor Schwierigkeiten auf.

Insbesondere große Unternehmen wie Amazon, Google oder Microsoft bieten das Cloud Computing in unterschiedlichen Betriebsmodellen an: Bei dem Modell Infrastructure as a Service (IaaS) werden nur Basisdienste wie Speicher- oder Netzdienste bereitgestellt, Platform as a Service (PaaS) bietet darüber hinaus auch Funktionen von Betriebssystemen, Datenbanken oder Umgebungen zur Softwareentwicklung, während beim Modell Software as a Service (SaaS) die komplette Anwendungssoftware „in der Wolke" angeboten wird. Bekannte Beispiele für das letztgenannte Modell sind Google Apps oder Microsoft Office Web Apps bzw. Office 365. In kurzen Zeitabständen drängen immer neue Cloud-Dienste auf den Markt. So hat die Firma Apple Ende 2011 ihren Dienst iCloud für den Massenmarkt der iPhones, iPads und iPods freigeschaltet.

Die Angebote der Cloud-Dienstleister sind bisher nur in Ausnahmefällen datenschutzkonform. Als besonders problematisch hat sich die Verlagerung der Informationsverarbeitung in die sogenannte Public Cloud erwiesen, bei der mehrere Cloud-Nutzer gemeinsam dieselben Ressourcen öffentlicher Cloud-Angebote verwenden. Die gesetzlichen Anforderungen an die Datenverarbeitung der Unternehmen und Behörden bezüglich Datenschutz und IT-Sicherheit, zu denen neben dem Trennungsgebot, der Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit auch die Kontrollierbarkeit,

[8] vgl. Tätigkeitsbericht 2008/2009, A 2.2

Transparenz und Beeinflussbarkeit gehören, sind hier nur sehr schwer oder gar nicht zu erfüllen.

Wer Cloud-Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten anbietet oder nutzt, sollte zur datenschutzkonformen Gestaltung des Verfahrens mindestens auf die Einhaltung folgender Punkte achten:

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender entscheiden können, ob Cloud Computing überhaupt infrage kommt und in der Lage sind, einen geeigneten Cloud-Anbieter auszuwählen,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ muss,

- die Umsetzung von abgestimmten IT-Sicherheitsmaßnahmen auf Seiten von Cloud-Anbietern und Cloud-Anwendern,

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüforganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Eine Arbeitsgruppe der Arbeitskreise „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe[9] zur datenschutzgerechten Ausgestaltung und Nutzung von Cloud-Diensten erarbeitet. Diese richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technik fördern. Die Orientierungshilfe wird von einer Entschließung[10] der Konferenz, in der die wesentlichen Anforderungen zusammengefasst sind, begleitet.

9 siehe http://www.lda.brandenburg.de

10 siehe Anlage 1.1.3: Entschließung „Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing“ vom 28./29. September 2011

Cloud-Anwender dürfen Cloud-Dienste nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Daten verarbeitende Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben. Die Verantwortung für die eigene Datenverarbeitung kann nicht auf den Cloud-Anbieter übertragen werden.

3.2 Datenschutzkonforme Reichweitenanalyse mit Google Analytics

Bereits in unserem letzten Tätigkeitsbericht[11] hatten wir uns kritisch mit sogenannten Tracking Tools zur Reichweitenanalyse von Internetangeboten befasst. Das am weitesten verbreitete Werkzeug Google Analytics kann nun datenschutzkonform eingesetzt werden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im Berichtszeitraum in umfangreichen Gesprächen mit der Firma Google Änderungen für einen gesetzeskonformen Einsatz von Google Analytics erreicht. Diese umfassen sowohl die internen Verarbeitungsprozesse bei Google als auch die Schutzmöglichkeiten für die Besucher einer Webseite, auf der Google Analytics eingesetzt wird (Einstellungen im Webbrowser). Ergänzend ist der Webseitenbetreiber verpflichtet, mindestens folgende Maßnahmen umzusetzen:

- Es muss ein schriftlicher Vertrag zur Auftragsdatenverarbeitung mit der Firma Google abgeschlossen werden. Hierzu wurde eine mit den Datenschutzaufsichtsbehörden abgestimmte Vorlage[12] erarbeitet.

- Die Nutzer müssen auf der Webseite in einer Datenschutzerklärung über die Verarbeitung ihrer personenbezogenen Daten im Rahmen von Google Analytics aufgeklärt und auf die Widerspruchsmöglichkeiten gegen die Erfassung durch das Werkzeug hingewiesen werden. Für gängige Webbrowser stellt Google Erweiterungen[13] (Plugins) zur Verhinderung der Erfassung (Opt-Out) bereit.

- Durch eine entsprechende Einstellung im Quelltext der Webseite muss Google zur Kürzung der IP-Adressen der Webseitennutzer veranlasst werden. Hierzu ist auf jeder Webseite mit Einbindung von Google Analy-

11 vgl. Tätigkeitsbericht 2008/2009, A 2.3

12 siehe http://www.google.de/intl/de/analytics/tos.pdf

13 siehe http://tools.google.com/dlpage/gaoptout?hl=de

tics der Tracking Code um den Aufruf einer Anonymisierungsfunktion zu ergänzen.[14]

- Die durch frühere Versionen von Google Analytics erfassten Altdaten wurden unzulässig erhoben und müssen gelöscht werden. Dazu hat der Webseitenbetreiber sein bestehendes Google Analytics-Profil zu schließen und anschließend ein neues zu eröffnen.

Webseitenbetreiber, die die Nutzung ihrer Webangebote mit Google Analytics auswerten möchten, handeln nur dann datenschutzkonform, wenn sie die vorgegebenen und auf die geänderte Version des Produkts abgestimmten Maßnahmen implementieren.

3.3 Smart Meter – Der gläserne Kunde?

Smart Meter, Smart Grid, Smart Home – Intelligenter Zähler, Intelligentes Stromnetz, Intelligentes Haus – das sind Begriffe, die uns künftig begleiten werden. Welche Möglichkeiten bieten sich und welche Risiken sind mit dem Einsatz dieser neuen Techniken, insbesondere von Smart Metern, verbunden?

Entsprechend den Vorgaben in Artikel 13 Absatz 1 der EU-Richtlinie über Endenergieeffizienz und Energiedienstleistungen[15] haben die Mitgliedstaaten, soweit es technisch machbar und finanziell vertretbar ist, sicherzustellen, dass die Endkunden in den Bereichen Strom, Erdgas, Fernheizung und/oder -kühlung und Warmbrauchwasser individuelle Zähler nutzen, die den tatsächlichen Energieverbrauch des Kunden und die tatsächliche Nutzungszeit widerspiegeln. Ziel ist es letztendlich, Energie zu sparen. Der Einsatz der neuen Zähler muss im Vergleich zu potenziellen Energieeinsparungen angemessen sein.

In Deutschland wurde die genannte EU-Richtlinie im Rahmen der Novellierung mehrerer Gesetze umgesetzt – u. a. mit Änderungen des Energiewirtschaftsgesetzes (EnWG).[16] Ergänzend sollen eine Reihe technischer Richtlinien, die zurzeit erarbeitet werden, Einzelheiten zur Nutzung der Smart Meter regeln. Bereits seit dem 1. Januar 2010 sind in Neubauten und bei Renovierungsmaßnahmen individuelle Zähler einzubauen. Darüber hinaus müssen

14 http://code.google.com/intl/de/apis/analytics/docs/gaJS/gaJSApi_gat.html#_gat._anonymizeIp

15 Richtlinie 2006/32/EG des europäischen Parlaments und des Rates vom 5. April 2006 über Endenergieeffizienz und Energiedienstleistungen und zur Aufhebung der Richtlinie 93/76/EWG des Rates (ABl. EU Nr. L 114 S. 64)

16 Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), zuletzt durch Artikel 2 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1690)

Energieversorgungsunternehmen seit dem 30. Dezember 2010 tageszeit- oder lastvariable Tarife anbieten.

Generell lässt sich feststellen, dass mit Hilfe von intelligenten Stromzählern und der damit verbundenen, potenziell sekundengenauen Erfassung des Verbrauchs eines Kunden Verhaltensprofile – und zwar auch ohne direkte Messung des Stromverbrauchs am Einzelgerät – gebildet werden können. Dies ergibt sich daraus, dass jedes Haushaltsgerät (wie z. B. Backofen, Spülmaschine und Kühlschrank) eine eigene, charakteristische Lastprofilkurve aufweist. Selbst wenn die Messungen beispielsweise nur im Viertelstundentakt erfolgen, lässt sich anhand der typischen Lastprofile eindeutig erkennen, welches Gerät der Kunde wann eingeschaltet hat. Dies erlaubt Rückschlüsse auf die Lebensgewohnheiten der Haushaltsmitglieder. Weitere Gefährdungen der Privatsphäre bestehen durch langfristige Aufzeichnungen, Verknüpfungsmöglichkeiten der Profile mit anderen Daten sowie das Auslesen der Daten per Fernzugriff. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb in einer Entschließung[17] frühzeitig u. a. eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch intelligente Zähler erhobenen Verbrauchsinformationen gefordert.

Durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde ein Schutzprofil für die Kommunikationseinheit (Gateway) von intelligenten Messsystemen entwickelt, welches Sicherheits- und Datenschutzanforderungen festschreibt. Hierzu gehören u. a.

- die Möglichkeit, über sogenannte Berechtigungsprofile festzulegen, wem, wann und wie oft welche Verbrauchsdaten – ggf. in kumulierter Form – übermittelt werden,

- die Pflicht, Verbrauchsdaten ausschließlich verschlüsselt und digital signiert an Berechtigte zu übertragen,

- die Festlegung, dass jede Kommunikation vom Gateway initiiert werden muss (mit Ausnahme kryptografisch gesicherter Administrationsanfragen),

- die Darstellung des Energieverbrauchs beim Endnutzer über eine lokale Schnittstelle (z. B. Display oder Web-Browser im Heimnetzwerk) ohne die Notwendigkeit der Datenübertragung an Dritte sowie die Protokollie-

[17] siehe Anlage 1.4.2: Entschließung „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs“ vom 3./4. November 2010

rung des Auslesens von Verbrauchsdaten zur Herstellung der Transparenz.

Positiv geprüfte Produkte, die das Schutzprofil erfüllen, sollen ein Zertifikat erhalten. Gemäß § 21e Abs. 4 EnWG dürfen nur zertifizierte Produkte als Messsysteme eingesetzt werden.

Im Land Brandenburg gibt es bereits einige Pilotprojekte zum Smart Metering. Beispielsweise hat die Stadt Forst (Lausitz) als Teil des Forster Energieeffizienzprogramms am 1. Oktober 2010 ein zweijähriges Pilotprojekt gestartet. Als Netzbetreiber fungiert hier die Netzgesellschaft Forst (Lausitz) mbH & Co. KG. Ziel ist es, bei ca. 1600 Haushalten die Zählertechnik, die Verbrauchserfassung mittels Fernauslesung, die Kommunikationsstruktur sowie die Datenübermittlung unter realen Bedingungen zu testen. Bereits vor Beginn des Projektes ist die Netzgesellschaft auf unsere Behörde zugekommen und hat um ein Informationsgespräch gebeten. Darüber hinaus waren wir beim Energiedienstleister E.ON edis AG im Rahmen eines Smart Metering Workshops mit verschiedenen Vertretern der Wirtschaft und anwesenden Stadtwerken beratend tätig.

Neben Smart Metern werden künftig auch Smart Grids und Smart Home an Bedeutung gewinnen. Bei Smart Grids handelt es sich um intelligente Stromnetze mit einem zwischen Netzkomponenten, Verbrauchern, Speichern und Erzeugern abgestimmten Netzmanagement. Unter Smart Home versteht man im Allgemeinen eine intelligente und integrierte Haussteuerung von Anlagen und Geräten mit dem Ziel eines effizienten Ressourcenverbrauchs.

Die Landesbeauftragte ist gern bereit, verantwortliche Daten verarbeitende Stellen bei der Nutzung dieser neuen Techniken unterstützend zu beraten.

Der Einsatz von Smart Metern darf nicht ohne Beachtung des Datenschutzes und der IT-Sicherheit erfolgen. Beim Umgang mit den personenbezogenen Daten sollten Energieversorgungsunternehmen ein Vertrauensverhältnis zu ihren Kunden aufbauen. Die Bildung von Verhaltensprofilen muss durch technische Maßnahmen wie Pseudonymisierung, verschlüsselte und digital signierte Datenübertragung sowie Kumulation der Messwerte verhindert werden.

3.4 IPv6 – nur ein neues Protokoll für das Internet?

Die Protokollsammlung TCP/IP beschreibt die grundlegenden Mechanismen des Datenaustausches im Internet. Das Internet Protokoll IP (als Bestandteil dieser Sammlung) dient dabei u. a. zur eindeutigen Adressierung der miteinander über das Internet kommunizierenden Endgeräte. Die Version 4 dieses Protokolls (IPv4) ist seit Langem im Einsatz und wird in den kommenden Jahren durch die Version 6 (IPv6) abgelöst werden. Im Zuge der Umstellung sind auch datenschutzrechtliche Aspekte zu beachten.

Bei der Nutzung von IPv4 werden Endgeräte im Internet durch Adressen mit einer Länge von 32 bit identifiziert. Bereits seit einigen Jahren ist abzusehen, dass aufgrund der rasanten Verbreitung des Internets der Vorrat an IPv4-Adressen zur Neige geht. Auf der technischen Ebene existieren deshalb Lösungen, diesen Engpass zu überwinden. So werden insbesondere bei der Vermittlung von Internetzugängen für Privatanwender IPv4-Adressen in der Regel nur dynamisch – und damit temporär – einem Nutzer zugewiesen. Darüber hinaus können durch Verwendung der sogenannten Network Address Translation (NAT) ganze Netze von Rechnern über eine einzige, gemeinsame, öffentliche IPv4-Adresse an das Internet angeschlossen werden. Beides verursacht jedoch bei Internet Providern bzw. Netzbetreibern zusätzlichen Aufwand.

Die Nutzung von IPv6 bietet einen Ausweg aus der Adressknappheit. Durch das neue Protokoll vervierfacht sich die Länge der IP-Adressen auf 128 bit. Die ersten 64 bit dieser Adressen (der sogenannte Präfix) werden dabei durch den Internet Provider oder Netzwerkadministrator zugeteilt, die restlichen 64 bit (der sogenannte Interface Identifier) durch das jeweils genutzte Endgerät bzw. den Nutzer selbst festgelegt. Rein rechnerisch wäre es möglich, weltweit jedem noch so kleinen Endgerät seine eigene IPv6-Adresse dauerhaft zuzuweisen.

Der Einsatz von IPv6 kann mit einer Reihe von Vorteilen für die Kommunikation im Internet verbunden sein. So lässt sich z. B. eine echte Ende-zu-Ende-Kommunikation (und damit auch eine Ende-zu-Ende-Sicherheit) zwischen Kommunikationspartnern realisieren. Dienste können direkt und ohne vermittelnde Portale (wie heute z. B. bei sozialen Netzwerken) nach dem Peer-to-Peer-Prinzip bereitgestellt werden. Eigenschaften von IPv6 sind auch ein vereinfachter, flexibler Aufbau des Protokollkopfes, eine verbesserte, performante Wegewahl im Internet (Routing), eine automatische Adresskonfiguration und der Verzicht auf NAT sowie auf Netzwerke mit privaten, nichtöffentlichen Adressen.

Aus datenschutzrechtlicher Sicht erhöhen jedoch dauerhaft zugewiesene, statische IP-Adressen das Risiko der Identifizierbarkeit von Nutzern und der Nachverfolgbarkeit ihrer Aktivitäten im Internet. Anbieter können u. U. leichter als bisher individuelle Profile zum Nutzungsverhalten erstellen oder diese webseitenübergreifend zusammenführen. Zu beachten ist dabei, dass sich das Risiko der Identifikation von Nutzern und der Profilbildung bereits aus beiden Teilen einer IPv6-Adresse allein (d. h. sowohl aus dem Präfix als auch aus dem Interface Identifier) ergeben kann.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit einer Entschließung[18] an Anbieter von Internetzugängen und Internetdiensten sowie an Hersteller von Hard- und Softwarelösungen im Kontext von IPv6 gewandt. Sie fordern, dass bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit gewährleistet werden müssen. Insbesondere sollten Produkte und Dienstleistungen datenschutzfreundlich gestaltet (privacy by design) bzw. mit datenschutzfreundlichen Voreinstellungen versehen werden (privacy by default). Weiterhin fordern die Datenschutzbeauftragten u. a., dass

- Zugangsanbieter ihren Kunden statische und dynamische IPv6-Adressen ohne Aufpreis zuweisen sollten und auf Wunsch des Kunden statische Adressen gewechselt werden können,

- Hersteller die sogenannten Privacy Extensions unterstützen und standardmäßig einschalten sollten, um die Wiedererkennung von Nutzern anhand des Interface Identifiers einer IPv6-Adresse zu erschweren,

- Inhalteanbieter zur Reichweitenmessung ihrer Webangebote nur die ersten 4 Bytes einer IPv6-Adresse nutzen, da diese für die Geolokalisierung ausreichen,

- Hard- und Softwarehersteller verstärkt an der Pflege und Weiterentwicklung ihrer Produkte arbeiten, um deren Reifegrad für die Nutzung des IPv6-Protokolls zu verbessern.

Es ist zu erwarten, dass das Internet Protokoll IPv6 in naher Zukunft in größerem Maßstab auch bei der Anbindung von Privatanwendern an das Internet zum Einsatz kommt. Dabei ist darauf zu achten, dass die Umstellung auf das neue Protokoll auch zu einer Verbesserung der IT-Sicherheit und des Datenschutzes für die Internetnutzer führt.

[18] siehe Anlage 1.1.5: Entschließung „Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!“ vom 28./29. September 2011

3.5 Elektronisches Grundbuch – Testbetrieb mit Echtdaten

Unter Federführung des Freistaates Bayern soll für alle Bundesländer ein bundeseinheitliches Datenbankgrundbuchsystem entwickelt werden. Als datenschutzrechtliches Problem erweist sich dabei die beabsichtige Übermittlung von Echtdaten aus Grundbüchern an ein privates Unternehmen und deren Nutzung im Rahmen der Entwicklung und des Tests eines Migrationsprogrammes.

Das private Unternehmen soll u. a. damit beauftragt werden, eine Software zur Digitalisierung und strukturierten Speicherung von derzeit nur in Papierform oder als gescannte Grafik vorliegenden Grundbuchblättern zu entwickeln. Um die Qualität dieser Software zu gewährleisten, muss auf einen repräsentativen Bestand an Echtdaten aus Grundbüchern zurückgegriffen werden. Nur so kann gesichert werden, dass z. B. unterschiedliche Papierformate, handschriftliche Anmerkungen oder altdeutsche Schrift korrekt erkannt, digitalisiert und gespeichert werden.

Da auch brandenburgische Grundbuchämter von der Lieferung ausgewählter Echtdaten aus Grundbüchern betroffen sein werden, stellt sich die Frage nach der Rechtsgrundlage für eine solche Übermittlung. Die Grundbuchordnung[19] enthält keine diesbezüglichen Regelungen. Auch nach dem Brandenburgischen Datenschutzgesetz ist eine Weitergabe nicht zulässig, da die Voraussetzungen für die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs nicht erfüllt sind. Es verbietet zudem die Nutzung von personenbezogenen Echtdaten zu Test- und Prüfungszwecken.

Insofern bestand aus unserer Sicht die Notwendigkeit, eine explizite Rechtsgrundlage für die Übermittlung der Echtdaten aus Grundbüchern zu schaffen, die sinnvollerweise bundesweit einheitlich sein sollte. Diese Auffassung, die auch die Datenschutzbeauftragten anderer Bundesländer vertraten, teilten wir dem in Brandenburg zuständigen Ministerium für Justiz mit.

Mittlerweile wurde auf Initiative des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz der Entwurf für eine diesbezügliche Ergänzung der Grundbuchordnung erarbeitet, der sich gegenwärtig in der Abstimmung befindet.

[19] Grundbuchordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1114), zuletzt geändert am 11. August 2009 (BGBl. I S. 2713)

Die Übermittlung personenbezogener Echtdaten aus Grundbüchern an eine nicht-öffentliche Stelle zur Entwicklung eines Migrationsprogramms für das bundesweit einheitliche elektronische Datenbankgrundbuch bedarf einer Rechtsgrundlage. Mit der beabsichtigten Ergänzung der Grundbuchordnung soll eine solche geschaffen werden.

3.6 Löschen von Datenträgern durch Überschreiben

Das datenschutzgerechte Löschen und Entsorgen von Datenträgern haben wir bereits mehrfach in unseren Tätigkeitsberichten thematisiert.[20] Dass die damit verbundenen Probleme nichts von ihrer Aktualität eingebüßt haben, zeigen die häufigen Nachfragen von verantwortlichen Daten verarbeitenden Stellen an unsere Behörde.

Sollen noch intakte Datenträger (wie Festplatten, Flash-Speichermedien oder wiederbeschreibbare DVDs) einer neuen Nutzung innerhalb der Daten verarbeitenden Stelle zugeführt oder verkauft, vermietet, zurückgegeben bzw. ausgesondert werden, sind sie zuvor durch das Überschreiben mit Zufallsdaten oder mit wechselnden Datenmustern zu löschen. Hierzu können grundsätzlich folgende Empfehlungen gegeben werden:

- Daten jeder Art sollten mindestens einmal überschrieben werden. Bei sensitiven Daten oder Datenträgern, die ein spezielles Aufzeichnungsverfahren verwenden, kann ein mehrfaches Überschreiben erforderlich sein.

- Es ist zu berücksichtigen, dass Kopien der zu löschenden Daten an verschiedenen Stellen auf demselben oder auf anderen Datenträgern liegen können (z. B. in temporären oder Auslagerungsdateien, Sicherungskopien o. ä.). Insofern ist das komplette Löschen der fraglichen Datenträger dem selektiven Löschen einzelner Dateien vorzuziehen.

- Manche Datenträger (z. B. moderne Festplatten) zeichnen sich dadurch aus, dass ausgewählte Bereiche für bestimmte Zwecke reserviert und nicht durch Überschreibsoftware erreicht werden können. Diese Bereiche sind vor dem Überschreiben zu identifizieren und aufzulösen.

- Auch defekte Bereiche (bad blocks) und die interne Umorganisation von Sektoren (reallocated sectors) können das vollständige Überschreiben des kompletten Datenträgers verhindern. Das durch verbleibende Datenreste entstehende Risiko ist im Einzelfall zu bewerten. Ggf. muss der Datenträger physisch vernichtet werden (z. B. durch mechanische, thermi-

[20] zuletzt vgl. Tätigkeitsbericht 2004/2005, A 2.11

sche oder magnetische Zerstörung). Gleiches gilt auch für nicht mehr intakte Datenträger.

- Es existieren frei verfügbare Softwarewerkzeuge, die sich grundsätzlich für das Löschen von Datenträgern durch das ein- oder mehrfache Überschreiben eignen. Für bestimmte Arten von Festplatten mit Hardwarebesonderheiten kann es erforderlich sein, herstellerspezifische Software zum Überschreiben einzusetzen.

- Bei Datenträgern mit Halbleiterspeicher (Flash-Speichermedien, USB-Sticks, Hybridfestplatten) erschweren interne Mechanismen wie Wear Leveling oder Defekt Management das Löschen durch Überschreiben. Es wird empfohlen, den Datenträger durch Beschreiben mit einer (einzigen) Datei in der Größe des Speichermediums zu überschreiben.

- Verantwortliche sollten sich zumindest stichprobenartig durch das anschließende Auslesen von ausgewählten Bereichen des Datenträgers davon überzeugen, dass das Überschreiben mit Zufallszahlen oder mit definierten wechselnden Datenmustern wie beabsichtigt vollzogen wurde.

Unabhängig von der Frage des sicheren Löschens von Daten empfehlen wir, sensitive Daten von Beginn an nur verschlüsselt auf Datenträgern zu speichern. Es gibt kostenfreie Werkzeuge, die eine transparente verschlüsselte Speicherung bei nur geringen Einbußen der Rechnerleistung unterstützen. Diese schützt (falls Verschlüsselungsalgorithmus und Schlüssel geeignet gewählt wurden) auch die Vertraulichkeit der Daten bei einem Verlust oder Diebstahl des Datenträgers.

Jede Daten verarbeitende Stelle hat bei der Entsorgung von Datenträgern die Datenschutzanforderungen zu beachten. Wenn Datenträger weiter genutzt werden sollen und sie deshalb nicht physisch vernichtet werden, sind sie irreversibel zu überschreiben. Die dabei verwendeten Methoden und Werkzeuge müssen sich nach dem Schutzbedarf der gespeicherten Daten sowie dem jeweils aktuellen Stand der Technik richten.

3.7 Online-Banking – iTAN, mTAN, ChipTAN, HBCI

Viele Menschen wickeln ihre Bankgeschäfte über das Internet mit dem eigenen PC und zunehmend auch mit Smartphones ab. Gleichzeitig ist die Zahl der Betrugsfälle beim Online-Banking in den letzten Jahren stark angestiegen. Hierbei werden persönliche Identifikations- bzw. Transaktionsnummern (PINs bzw. TANs) von Kriminellen ausgespäht und missbraucht, indem sie eigene Überweisungen von dem Konto des

Opfers durchführen. Die von den Banken angebotenen Verfahren zum Online-Banking sind unterschiedlich sicher.

Das erste PIN/TAN-Verfahren der Banken, bei dem Nutzer beliebige TANs eines TAN-Blocks verwenden konnten, hat sich schnell als unsicher erwiesen, weil Kriminelle über imitierte Banken-Webseiten relativ einfach in den Besitz gültiger PINs und TANs gelangen konnten. Die Geldinstitute wechselten daher zum bekannten iTAN-Verfahren (indizierte TAN), bei dem sie nummerierte TAN-Listen an die Benutzer verschicken. Das Online-Banking-Verfahren fragt hierbei für Überweisungen nach einer bestimmten, durch eine Nummer bezeichneten TAN auf der Liste. Nur mit dieser TAN kann die Überweisung autorisiert werden. Selbst wenn ein Angreifer in den Besitz dieser TAN gelangen sollte, kann er sie also nicht für eine andere Überweisung verwenden, sodass dieses Verfahren lange Zeit als sicher galt.

Inzwischen haben sich Betrüger über die weite Verbreitung von Banking-Trojanern wie ZeuS und SpyEye wieder die Möglichkeit geschaffen, trotz iTAN-Verfahren Konten leerzuräumen. Ein Banking-Trojaner (eigentlich: Trojanisches Pferd) ist eine Schadsoftware, die über Sicherheitslücken auf den Rechner eines Bankkunden eingeschleust wird, sich dort in die Kommunikation im Webbrowser einklinkt und während eines Banking-Vorgangs heimlich Überweisungsdaten manipuliert. Das Opfer merkt davon nichts, weil der Trojaner ihm immer die legitimen Überweisungsdaten präsentiert, während er im Hintergrund mit der eingegebenen iTAN eine illegale Transaktion anstößt.

Da das iTAN-Verfahren also nicht mehr sicher ist, sind von vielen Banken verbesserte Verfahren wie mTAN/smsTAN und ChipTAN eingeführt worden. Beim mTAN-Verfahren (mobile TAN) wird eine SMS mit der TAN und den auf dem PC eingegebenen Überweisungsdaten an den Kunden geschickt. Der Sicherheitsgewinn dieses Verfahrens liegt in der Unabhängigkeit des Übertragungskanals der SMS vom PC, auf dem das Homebanking durchgeführt wird. Allerdings sind mittlerweile auch die Banking-Trojaner an das Verfahren angepasst worden und können im Online-Banking-Dialog die Handynummer des Opfers abfragen, um über eine als Sicherheitsupdate getarnte SMS das Handy mit einer mobilen Version der Schadsoftware zu infizieren. Danach können die Betrüger wieder die TANs mitlesen. Umso wichtiger ist es, das mTAN-Verfahren nicht zusammen mit dem Mobile Banking auf demselben Smartphone zu nutzen, da ein Schädling auf diesem Smartphone sowohl Zugriff auf die per SMS übersandten TANs als auch auf die Transaktionsdaten des Mobile-Banking-Dialogs hätte. Die meisten Mobile-Banking-Applikationen für Smartphones lassen daher die Nutzung von mTANs nicht zu.

Das ChipTAN-Verfahren arbeitet mit einem Kartenleser inklusive TAN-Generator, in den der Anwender seine Bankkarte einsteckt, einen Startcode und die Überweisungsdaten eingibt. Danach wird von der Bankkarte die erforderliche TAN berechnet und im Display angezeigt. Diese TAN ist nur für wenige Minuten und nur für die eingegebenen Überweisungsdaten gültig, sodass sie nicht missbraucht werden kann. Zur Vereinfachung der aufwendigen und fehleranfälligen Eingabe von Transaktionsdaten auf dem TAN-Generator gibt es inzwischen auch ChipTAN-Geräte mit optischen Sensoren, die die Überweisungsdaten mittels optischer Übertragung vom Bildschirm des Rechners übernehmen können. Dazu wird im Online-Banking-Dialog auf dem PC aus den Transaktionsdaten und dem Startcode ein flackerndes Schwarz-weiß-Muster erzeugt, dass durch Heranhalten des ChipTAN-Gerätes über die Sensoren eingelesen wird. Die Fototransistoren rechnen das eingelesene Muster wieder in die alphanumerischen Transaktionsdaten um, aus denen danach die TAN erzeugt werden kann. Wichtig ist, dass ein Anwender immer sorgfältig die Überweisungsdaten im ChipTAN-Gerät auf Korrektheit kontrolliert, damit ihm nicht von Angreifern falsche Daten untergeschoben werden können.

Als sicherste Methode für das Homebanking gilt das von einigen Banken schon lange eingeführte HBCI-Verfahren. HBCI steht für Homebanking Computer Interface. Der Dialog mit dem Bankserver erfolgt hierbei nicht wie bei den anderen beschriebenen Verfahren über eine Webschnittstelle, sondern über ein gesondertes Protokoll. Für Homebanking per HBCI benötigt man ein Kartenlesegerät, in das die Bankkarte mit einem Signaturschlüssel gesteckt wird. Für die Legitimation von Transaktionsdaten werden jetzt keine TANs mehr verwendet, sondern die Datensätze werden mit dem Signaturschlüssel digital signiert, nachdem der Benutzer seine PIN auf der Zehnertastatur des Kartenlesergerätes eingegeben hat. Da der Signiervorgang im Chip der Karte erfolgt und der Signaturschlüssel nicht aus dem Chip auslesbar ist, können keine falschen Signaturen für manipulierte Transaktionsdaten erzeugt werden. Die hohe Sicherheit des HBCI-Verfahrens ist aber nur gewährleistet, wenn man einen Kartenleser mit Tastatur verwendet und die PIN nicht auf der PC-Tastatur eingibt, sonst könnte Schadsoftware die PIN mitlesen und missbrauchen.

Das iTAN-Verfahren ist grundsätzlich nicht mehr zu empfehlen. Das mTAN-Verfahren ist sicherer als iTAN, allerdings sind auch dafür bereits Schädlinge im Umlauf. Es darf nicht auf Smartphones eingesetzt werden. ChipTAN und HBCI sind bei Beachtung der notwendigen Sicherheitsvorkehrungen sichere Homebanking-Verfahren.

3.8 Vom schleichenden Tod der qualifizierten elektronischen Signatur

Im Rahmen von E-Government-Projekten besteht die Tendenz, zur rechtsverbindlichen Sicherung der Authentizität und Integrität von Dokumenten statt der qualifizierten elektronischen Signatur (QES) Verfahren einzusetzen, die weniger sicher sind und nur zur Authentisierung von Personen dienen. Bei der elektronischen Steuererklärung ELSTER wird dieser Trend fortgeführt, indem ein sogenanntes „anderes sicheres Verfahren" zur Authentisierung der Datenübermittler quasi als Standardverfahren gesetzlich festgeschrieben wird.

Die Abgabenordnung sieht bei einer Steuererklärung die Schriftform vor, d. h., sie ist von den Steuerpflichtigen zu unterschreiben. Die Schriftform kann durch die elektronische Form ersetzt werden. Dazu ist die Signatur des Dokumentes mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz erforderlich. Soll eine Steuererklärung in elektronischer Form abgegeben werden, muss sie also vom Grundsatz her qualifiziert elektronisch signiert werden. Der Gesetzgeber hat nun vorgesehen, für Steuererklärungen neben der qualifizierten elektronischen Signatur bis zum 31. Dezember 2011 „auch ein anderes sicheres Verfahren" zuzulassen, das „die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt" (§ 87a Abs. 6 Abgabenordnung). Nach der derzeitigen Fassung der Abgabenordnung ist also für die elektronische Form der Steuererklärung als Regelfall die qualifizierte elektronische Signatur und als alternative Möglichkeit das „andere sichere Verfahren" vorgesehen. Faktisch ist aber die Nutzung der QES bisher überhaupt nicht möglich, weil die Finanzbehörden dafür keinen Zugang eröffnet haben. Die einzig mögliche elektronische Form ist derzeit das ELSTER-Verfahren, in welchem jedoch keine Sicherung der Authentizität und Integrität von Dokumenten erfolgt, sondern lediglich der Datenübermittler als Person authentisiert wird.

Im ELSTER-Verfahren können Steuerpflichtige ihre Steuererklärung über ein Internetportal in elektronischer Form bei den Finanzbehörden einreichen. Gemäß dem gesetzlichen Auftrag fand nun eine Evaluierung des Verfahrens statt, die eine positive Bilanz der Verwendung des ELSTER-Verfahrens zieht. Der Evaluierungsbericht enthält nach unserem Dafürhalten allerdings einige Schwachpunkte:

- Es werden keine statistischen Angaben zur Nutzung der verschiedenen ELSTER-Authentisierungsstufen (ELSTER-Basis, ELSTER-Spezial, ELSTER-Plus) und eventueller Missbrauchsfälle gemacht. Für eine begründete Bewertung des ELSTER-Verfahrens wäre aber eine derartige Datenbasis erforderlich.

- Die generellen Sicherheitseigenschaften, Risiken oder Schwachstellen des ELSTER-Verfahrens werden nicht analysiert. Stattdessen wird lediglich die derzeitige technisch-organisatorische Implementierung betrachtet und in diesem Zusammenhang auch auf ein Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und auf ein BSI-Zertifikat verwiesen. Beide Zertifikate genügen aber nicht, um die allgemeinen Sicherheitseigenschaften ausreichend zu belegen. Hierfür wäre zum Beispiel eine Zertifizierung nach Common Criteria geeignet.

- Ein Vergleich des „anderen sicheren Verfahrens“ mit den Sicherheitseigenschaften und Anforderungen der QES findet nicht statt. Somit fehlt im Bericht die für eine Evaluierung des „anderen sicheren Verfahrens“ erforderliche zentrale Abwägung zwischen der QES und ELSTER, und zwar gemessen an den Eigenschaften der QES.

Trotzdem haben Bundestag und Bundesrat das Steuervereinfachungsgesetz 2011 beschlossen, in dem das „andere sichere Verfahren“ unbefristet zugelassen wird. Das Bundesministerium der Finanzen will darüber hinaus sogar prüfen, inwieweit im Steuerrecht tatsächlich die Schriftform erforderlich ist und diese – wo möglich – abschaffen. Damit würde dann auch die formale Erforderlichkeit der QES gänzlich wegfallen.

Generell werden auf dem Weg zu mehr E-Government insbesondere Schriftformerfordernisse in Verwaltungsverfahren als Hindernis angesehen, da bei Übertragung in die elektronische Form zunächst gem. § 3a Verwaltungsverfahrensgesetz immer der Einsatz der QES vorgesehen werden müsste. Es gibt viele Stimmen, die die Anforderungen der QES in Verwaltungsverfahren im Regelfall als zu hoch ansehen und daraus folgend den Abbau von Schriftformerfordernissen fordern. Statt jedoch den Abbau von Schriftformerfordernissen auf gesetzlicher Ebene konsequent in Angriff zu nehmen, wird zunehmend als Ersatz für die QES der Einsatz der elektronischen Identitätsfunktion des neuen Personalausweises oder alternativer Verfahren wie De-Mail zur Authentisierung in elektronischen Verwaltungsverfahren vorgeschlagen. Die QES gerät mehr und mehr ins Abseits.

Vernachlässigt wird in diesen Diskussionen allerdings immer der Sicherheitsverlust, der mit dem Verzicht auf die QES einhergehen würde. Die vorgeschlagenen Alternativen können allein weder die Authentizität noch die Integrität von elektronisch übermittelten Dokumenten gewährleisten.

Das ELSTER-Verfahren wird unbefristet in den Finanzbehörden weitergeführt. Die qualifizierte elektronische Signatur zur Sicherung der Integrität und Authentizität von elektronisch übermittelten Steuererklärungen wird dagegen weiterhin nicht angeboten. Der Trend, in E-Government-Verfahren von vornherein auf die QES zu verzichten, verstärkt sich.

4 Arbeit und Soziales

4.1 Jobcenter unter neuer Aufsicht

Nachdem das Bundesverfassungsgericht in seinem Urteil vom 20. Dezember 2007 die gemeinsame Aufgabenwahrnehmung von Bundes- und Kommunalbehörden auf dem Gebiet der Grundsicherung für Arbeitsuchende (Arbeitsgemeinschaften – ARGEn) für nicht mit dem Grundgesetz vereinbar erklärt hatte, musste bis zum 31. Dezember 2010 eine Neuorganisation erfolgen.

Die vom Bundesverfassungsgericht geübte Kritik an der Mischverwaltung erstreckte sich auch auf die unklaren Regelungen zur Zuständigkeit bei der Datenschutzkontrolle. Für den Bürger muss klar erkennbar sein, welche Stelle für welche Aufgaben letztlich verantwortlich ist.

Mit der gesetzlichen Neuregelung ist seit dem 1. Januar 2011 dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die datenschutzrechtliche Kontrolle der „gemeinsamen Einrichtungen“, der sogenannten Jobcenter, übertragen worden. Bis zu diesem Zeitpunkt unterlagen die ARGEn als Stellen der Länder der Kontrolle der Landesdatenschutzbeauftragten. Lediglich soweit die Bundesagentur für Arbeit zentrale EDV-Programme bundesweit zum Einsatz brachte oder generelle Verfahren betroffen waren, lag die Zuständigkeit beim Bundesdatenschutzbeauftragten. Für die sogenannten Optionskommunen, die Leistungen des Zweiten Buches Sozialgesetzbuch (SGB II) ohne Beteiligung der Agentur für Arbeit erbringen, bleibt die Zuständigkeit der jeweiligen Landesbeauftragten für den Datenschutz auch weiterhin bestehen.

In Brandenburg haben sich folgende Landkreise für die Option entschieden: Oberhavel, Oder-Spree, Ostprignitz-Ruppin, Spree-Neiße und Uckermark. Sie unterliegen damit der datenschutzrechtlichen Aufsicht der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg.

Inzwischen haben sich zwei weitere brandenburgische Kommunen für die eigenständige Aufgabenwahrnehmung entschieden. Ab dem 1. Januar 2012 werden die Landkreise Havelland und Potsdam-Mittelmark nun gleichfalls die Arbeitsuchenden nach dem SGB II selbstständig betreuen.

Mit der Neuorganisation der Grundsicherung für Arbeitsuchende wurden klare Regelungen zur datenschutzrechtlichen Zuständigkeit getroffen. Im Land Brandenburg gibt es zum Stichtag 1. Januar 2012 sieben Optionskommunen, die der datenschutzrechtlichen Aufsicht der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht unterliegen.

4.2 Unsichere Versendung von Versorgungsamtsakten

Jeder Sozialleistungsträger ist gem. § 35 Erstes Buch Sozialgesetzbuch verpflichtet, dafür zu sorgen, dass unbefugte Dritte keine Kenntnis von Sozialdaten erhalten. Entsprechend ist auch der Postversand von den Behörden zu organisieren. Dieser Verpflichtung kam das Landesamt für Soziales und Versorgung des Landes Brandenburg nicht nach.

Ein Bürger hatte Leistungen nach dem Opferentschädigungsgesetz beim Landesamt beantragt. Zur Feststellung der Schädigungsfolgen und der notwendigen Kausalitätsbewertung zwischen dem schädigenden Ereignis und der eingetretenen Gesundheitsstörung wurde vom Versorgungsamt ein Arzt in einer Klinik für Forensische Psychiatrie mit der Erstellung eines medizinischen Gutachtens beauftragt.

Zur sach- und qualitätsgerechten Durchführung der Begutachtung sollte dem beauftragten Arzt die aus zwei Bänden bestehende Versorgungsakte vorab zugesandt werden. Durch einen Behördenfehler wurde das Paket nicht an den Gutachter, sondern an den Antragsteller adressiert und mit einfacher Post an diesen versandt. Da der Adressat nicht zu Hause war, wurde es ersatzweise in der Nachbarschaft abgegeben. Somit bestand für Unbefugte die Möglichkeit, den Inhalt des Paketes zur Kenntnis zu nehmen.

Aufgrund dieser Vorkommnisse wurde der Postversand im Landesamt neu organisiert. Sofern eine persönliche Übergabe der Versorgungsamtsakten nicht möglich ist, erfolgt künftig die Zustellung per „Einschreiben mit Rückschein“. Die persönliche Übergabe gegen Unterschrift hat dabei grundsätzlich Vorrang vor dem Postversand. Zudem wurden die Mitarbeiter nochmals auf die Einhaltung sozialdatenschutzrechtlicher Regelungen hingewiesen. Die fehlerhafte Adressierung wurde gerügt.

Angesichts der sofortigen Änderung der bisherigen Verfahrensweise und der damit verbundenen Beseitigung von Mängeln durch das Landesamt sah die

Landesdatenschutzbeauftragte von einer Beanstandung ab. Die Neuorganisation des Postversandes führte zu einer wesentlichen Verbesserung des Datenschutzniveaus.

Die Versendung sensitiver Gesundheitsdaten ist so zu organisieren, dass eine unbefugte Kenntnisnahme durch Dritte verhindert wird. Das Sozialgeheimnis ist zu wahren.

4.3 Übermittlung von Kontodaten Dritter an Leistungsempfänger

Im Berichtszeitraum kam es bei einem Jobcenter im Zusammenhang mit der Verwendung der Leistungssoftware A2LL[21] erneut zu Unstimmigkeiten bei der Bescheiderstellung. Ein Bürger wandte sich an uns, da das an ihn gerichtete Schreiben Kontodaten einer ihm fremden Person enthielt.

Mit seinem Leistungsbescheid vom August 2010 erhielt der Petent nicht nur die Information, dass und in welcher Höhe ihm Sozialleistungen nach dem Zweiten Buch Sozialgesetzbuch gewährt werden. Zugleich enthielt der Bescheid Namen und Kontoverbindungsdaten eines Dritten. Was war geschehen?

Wie uns das zuständige Jobcenter auf Nachfrage mitteilte, hatte der Petent im Mai 2007 die Übernahme der Kosten für eine mehrtägige Klassenfahrt seiner Tochter beantragt. Dem Antrag wurde damals stattgegeben und das Jobcenter überwies die Teilnahmegebühren für die Klassenfahrt auf das Konto des Veranstalters. Hierzu musste dessen Bankverbindung in die vom Jobcenter verwendete Leistungssoftware A2LL eingegeben werden. Das Jobcenter ging davon aus, dass die Bankverbindung zwar im System gespeichert wurde, jedoch nach Überweisung der Teilnahmegebühr nicht mehr in späteren Bescheiden erscheinen würde. Dass die Daten des Zahlungsempfängers im August 2010 dennoch wieder in den Bescheid aufgenommen wurden, konnte das Jobcenter nur mit einer Fehlfunktion im Zuge der Installation einer neuen Programmversion von A2LL erklären. Obwohl das Problem nun bekannt war, enthielt ein weiterer Bescheid vom September 2010 wiederum die Kontoverbindungsdaten des Dritten.

Wir forderten das Jobcenter auf, Maßnahmen zu ergreifen, um künftig derartige Datenübermittlungen auszuschließen. Die Geschäftsleitung des Jobcenters wies daraufhin zunächst die Mitarbeiter an, bei Drittzahlungsempfängern den Zahlungszeitraum entsprechend dem jeweiligen Zahlungsgrund zeitlich

[21] vgl. Tätigkeitsbericht 2008/2009, A 7.1.8

zu beschränken. Für die Bewilligung von Klassenfahrten bedeutet dies, dass der Zahlungszeitraum auf einen Monat begrenzt wird. Insofern dürften nach Erledigung und Bewilligung des Vorganges die Kontoverbindungsdaten der Drittzahlungsempfänger nicht mehr in den Bescheiden der Leistungsempfänger ausgewiesen werden.

Grundsätzlich ist die Bundesagentur für Arbeit und nicht das einzelne Jobcenter für die ordnungsgemäße Funktionsweise des Softwareprogramms A2LL verantwortlich. Einen Verstoß des Jobcenters vor Ort gegen datenschutzrechtliche Vorschriften haben wir somit nicht feststellen können.

Das Datenverarbeitungsprogramm A2LL bewältigt die durch das Gesetz gestellten Anforderungen nicht vollständig. Dies wirkt sich auch auf die Einhaltung datenschutzrechtlicher Normen aus. Die Bundesagentur für Arbeit hat bei der Entwicklung einer neuen Leistungssoftware in jedem Fall die sozialdatenschutzrechtlichen Regelungen zu beachten und umzusetzen.

4.4 Abschied von ELENA

Seit dem 1. Januar 2010 waren die Arbeitgeber verpflichtet, monatlich die Entgeltdaten ihrer Beschäftigten an eine Zentrale Speicherstelle bei der Rentenversicherung Bund zu melden. Wie bereits in unserem letzten Tätigkeitsbericht[22] ausgeführt, bestanden erhebliche datenschutzrechtliche Bedenken gegen die Schaffung dieser bundesweiten Datenbank. Wegen der nicht ausreichenden Verbreitung der qualifizierten elektronischen Signatur ist das Verfahren nun gestoppt worden.

Das ELENA-Verfahren (Elektronischer Entgeltnachweis) sah vor, dass die Bürger eine elektronische Signaturkarte erhalten, um Leistungen bei Behörden, wie z. B. Arbeitslosengeld, Elterngeld oder Wohngeld zu beantragen. Mit dieser Signatur sollten die Behördenmitarbeiter auf die in der Datenbank hinterlegten Informationen zugreifen können. Die Nutzung der qualifizierten elektronischen Signatur war eine zwingende datenschutzrechtliche Verfahrensvoraussetzung. Da diese Signatur auch in absehbarer Zeit nicht bundesweit verbreitet sein wird, wurde das ELENA-Verfahren eingestellt. Das Aufhebungsgesetz[23] bestimmt u. a. die unverzügliche Löschung der über 700 Millionen gespeicherten Datensätze und hebt die Verpflichtung der Arbeitgeber zur Datenübermittlung auf.

---

22 vgl. Tätigkeitsbericht 2008/2009, A 7.5

23 Gesetz zur Änderung des Beherbergungsstatistikgesetzes und des Handelsstatistikgesetzes sowie zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises vom 23. November 2011 (BGBl. I S. 2298)

Bereits vor Inkrafttreten dieses Gesetzes kündigte die Bundesregierung ein Nachfolgeverfahren für ELENA an. Dieses soll einfacher und unbürokratischer gestaltet werden. Abstriche an datenschutzrechtlichen Verfahrensregelungen darf es jedoch nicht geben. In einem Eckpunktepapier wies der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf die datenschutzrechtlichen Anforderungen an das Nachfolgeverfahren hin. Insbesondere sind die Grundsätze der Datensparsamkeit und die strikte Zweckbindung einzuhalten. In jedem Fall müssen die Rechte der Betroffenen, beispielsweise auf Auskunft, beachtet und entsprechend in das Verfahren implementiert werden. Die Betroffenen sollten soweit wie möglich, die Kontrolle über ihre Daten behalten. Eine Kernforderung bleibt, dass die zur Sicherung der personenbezogenen Daten zu treffenden technischen und organisatorischen Maßnahmen der hohen Schutzbedürftigkeit dieser Daten entsprechen. Das bedeutet, dass sich die eindeutige Identifizierung aller Verfahrensbeteiligten, die Verschlüsselung und Protokollierung am Stand der Technik orientieren müssen.

Die in der Vergangenheit geäußerten Bedenken der Datenschutzbeauftragten, dass mit dem ELENA-Verfahren eine anlassunabhängige, zentrale Datenerhebung und -speicherung personenbezogener Informationen durch den Staat erfolgt, die gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen könnte, bleiben bestehen. Die datenschutzrechtlichen Kritikpunkte müssen bei der Entwicklung des Nachfolgeverfahrens berücksichtigt werden.

Eine anlassunabhängige, zentrale Sammlung aller Entgeltdaten verstößt gegen datenschutzrechtliche Grundsätze. Sollte ELENA ein neues Verfahren nachfolgen, so muss dieses das Recht auf informationelle Selbstbestimmung wahren.

4.5 Diskriminierung Arbeitsuchender im Internet

In dem sozialen Netzwerk StudiVZ.net existierte eine Diskussionsgruppe mit dem Namen „Ich fürchte keine Hölle: Ich bin ARGE-Mitarbeiter!“. Deren Mitglieder tauschten sich über – nach ihrer Ansicht offenbar lustige, seltene bzw. ausgefallene – Vornamen der Kinder von Sozialleistungsempfängern aus.

In einigen Fällen wurden vollständige Namen der Leistungsempfänger genannt. Durch zusätzliche Informationen sowie die Namen der im Netzwerk registrierten ARGE-Mitarbeiter waren einige der betroffenen Kinder und deren Familien als Bezieher von Leistungen zur Grundsicherung für Arbeitsuchende identifizierbar.

Ein Verstoß gegen das Sozialgeheimnis war damit gegeben. Die Übermittlung von Daten an unzuständige Dritte – hier sogar außerhalb der mit der Bearbeitung des jeweiligen Leistungsfalls betrauten ARGE – über das Internet erfolgte ohne Rechtsgrundlage.

Wie die weitere Sachverhaltsaufklärung ergab, war die Netzwerkgruppe bei StudiVZ.net bereits gelöscht. Die Bundesagentur für Arbeit teilte in ihrer Stellungnahme an den Bundesbeauftragten für den Datenschutz mit, dass der Vorfall überprüft wurde. In den Fällen, in denen die Verletzung der Verschwiegenheitspflicht festgestellt und die entsprechenden Mitarbeiter ermittelt werden konnten, wurden disziplinarische bzw. arbeitsrechtliche Konsequenzen gezogen. Zudem wurden die Themen „Verschwiegenheitspflichten“ und „Einhaltung des Sozialdatenschutzes“ mit den Mitarbeitern erneut erörtert.

Eine Beteiligung von Mitarbeitern von brandenburgischen ARGEn an diesem Forum wurde unserer Behörde nicht bekannt. Dennoch wiesen wir in Gesprächen mit den ARGEn auf diese gravierende Verletzung des Sozialdatenschutzes hin und forderten die Geschäftsführungen zur datenschutzrechtlichen Sensibilisierung ihrer Mitarbeiter auf.

Die Tatsache, dass ein Bürger auf Sozialleistungen angewiesen ist, unterfällt dem Schutzbereich des Sozialgeheimnisses. Jeder Bedienstete eines Sozialleistungsträgers ist verpflichtet, das Sozialgeheimnis zu wahren. Diese Verpflichtung gilt auch für den internen Geschäftsgang beim Leistungsträger und besteht über die Beendigung des Beschäftigungsverhältnisses hinaus.

5 Auskunfteien

5.1 Gesetzliche Neuregelungen

Das Bundesdatenschutzgesetz (BDSG) wurde bereits im vorigen Berichtszeitraum novelliert. Einige Änderungen traten jedoch erst im Jahre 2010 in Kraft. Dies betrifft unter anderem die Rechte von Verbrauchern gegenüber Auskunfteien. Ziel der Novelle auf diesem Gebiet war es, die Betroffenen davor zu bewahren, durch die automatisierte Datenverarbeitung der Auskunfteien in ungerechtfertigter Weise, beispielsweise bei der Bewilligung von Krediten, benachteiligt zu werden. Neu eingeführt wurden zu diesem Zweck die Befugnisse zur Datenübermittlung an Auskunfteien (§ 28a BDSG) sowie die Bestimmungen, mit denen das Scoring-Verfahren transparenter werden soll (§ 28b BDSG). Das Auskunftsrecht des Betroffenen gegenüber den Auskunfteien (§ 34 BDSG) wurde im Rahmen der Gesetzesnovelle erweitert.

5.1.1 Datenübermittlung an Auskunfteien

§ 28a Bundesdatenschutzgesetz (BDSG) regelt, unter welchen Voraussetzungen personenbezogene Daten an Auskunfteien übermittelt werden dürfen.

Nach § 28a Abs. 1 BDSG ist die Übermittlung an Auskunfteien nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist und die Daten eindeutig Rückschlüsse auf die Zahlungsunfähigkeit oder -unwilligkeit der betroffenen Person zulassen. Forderungen, die durch ein Urteil, Insolvenzverfahren oder Ähnliches förmlich festgestellt wurden oder solche, die der Betroffene ausdrücklich anerkennt, können unter diesen Voraussetzungen übermittelt werden. Andere Forderungen dürfen lediglich dann einer Auskunftei gemeldet werden, wenn sie unbestritten und mindestens zweimal erfolglos angemahnt worden sind. Zwischen der ersten Mahnung und der Übermittlung an die Auskunftei müssen mindestens vier Wochen liegen. Zusätzlich muss die betroffene Person rechtzeitig von der bevorstehenden Übermittlung unterrichtet werden.

Unter dem Vorbehalt einer Interessenabwägung dürfen Kreditinstitute nach § 28a Abs. 2 BDSG lediglich Rahmendaten zu einem konkreten Vertragsverhältnis an Auskunfteien übermitteln. Der Betroffene ist hierüber vor Abschluss des Vertrags zu unterrichten, um ihm eine andere Entscheidung zu ermöglichen. Anders als vor der Novellierung des Gesetzes dürfen Informationen über bloße Anfragen nach einem Kredit auf keinen Fall mehr übermittelt werden.

Neu ist auch die Regelung des § 28a Abs. 3 BDSG, nach der Unternehmen, die Daten an Auskunfteien übermitteln, nachträgliche Änderungen mitzuteilen haben. Die Auskunfteien haben die Löschung der ursprünglichen Daten zu bestätigen.

5.1.2 Scoring

Als Scoring bezeichnet man ein Verfahren, mit dem aufgrund tatsächlicher Erkenntnisse eine Prognose für ein zukünftiges Verhalten erstellt wird. Der ermittelte Wahrscheinlichkeitswert (Score-Wert) soll einen Anhaltspunkt für die Verlässlichkeit des Betroffenen, z. B. als Kreditnehmer liefern. § 28b Bundesdatenschutzgesetz (BDSG) regelt, welche personenbezogenen Daten in dessen Berechnung einfließen dürfen. Dabei können zwar auch Daten einbezogen werden, die unabhängig von dem Scoring-Verfahren für eigene Geschäftszwecke bzw. die Übermittlung an Auskunfteien genutzt werden dürften (§§ 28 und 29 BDSG). Die Informationen müssen aber eine mathematisch-statistisch erwiesene Relevanz für das mit dem Scoring prognostizierte Vertragsverhalten – etwa die Rückzahlung eines Kredits – haben.

Durch den Bezug auf ein wissenschaftlich anerkanntes Verfahren soll eine willkürliche Vorgehensweise verhindert werden. Ein Score-Wert darf darüber hinaus nicht ausschließlich auf der Grundlage von Anschriftendaten ermittelt werden, d. h. es müssen neben den Anschriftendaten auch weitere, wesentliche Parameter in die Berechnung einfließen. Im Falle der Nutzung von Anschriftendaten sind die Betroffenen vorher darüber zu unterrichten. Dies ist jeweils zu dokumentieren. Verantwortliche Stellen dürfen Daten, die sie ausschließlich für die Identitätsprüfung erhalten haben (etwa frühere Anschriften der Betroffenen), nicht ohne Einwilligung für das Scoring nutzen, da dies eine Zweckänderung darstellt.

Soweit Kreditinstitute im Hinblick auf ihre Kunden selbst ein Scoring-Verfahren durchführen, haben sie die Vorschriften des § 10 Abs. 1 Kreditwesengesetz zu beachten. Danach dürfen Angaben zur Staatsangehörigkeit sowie zu den in § 3 Abs. 9 BDSG genannten, besonders schutzbedürftigen personenbezogenen Daten (z. B. über die ethnische Herkunft, Gesundheit etc.) nicht genutzt werden. Zulässig ist hingegen die Nutzung zutreffender, spezieller Daten zum Zahlungsverhalten sowie zu den Einkommens-, Vermögens- und Beschäftigungsverhältnissen.

5.1.3 Auskunftsrechte für die Betroffenen

Durch die Änderung des Bundesdatenschutzgesetzes (BDSG) wurde das Auskunftsrecht der Bürger nach § 34 des Gesetzes erweitert. Seit dem 1. April 2010 kann jeder in Erfahrung bringen, welche Informationen einer Auskunftei zur eigenen Person vorliegen und welche Stellen Auskünfte eingeholt haben. So ist es jedem möglich zu bewerten, ob diese Daten richtig sind und die Übermittlung zulässig war. Insbesondere das Scoring-Verfahren soll für die Betroffenen dadurch transparenter gestaltet werden.

Der Auskunftsanspruch umfasst sämtliche zur Person gespeicherten Daten, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Auskünfte müssen unter anderem über die Herkunft und Empfänger der Daten erteilt werden. Diese Auskunft kann nur verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt. Außerdem ist über den Zweck der Speicherung zu informieren.

Auskunfteien sind darüber hinaus jetzt verpflichtet, die gespeicherten Score-Werte mitzuteilen. Der Informationsanspruch auf die Score-Werte umfasst im Wesentlichen:

- den aktuellen Score-Wert,

- die innerhalb der letzten 12 Monate übermittelten Score-Werte,
- den Namen und die letztbekannte Anschrift der Empfänger der Score-Werte,
- die zur Berechnung der Score-Werte genutzten Datenarten sowie
- das Zustandekommen und die Bedeutung der Score-Werte.

Die Auskunft ist einzelfallbezogen, in nachvollziehbarer und allgemein verständlicher Form zu erteilen. Das Auskunftsrecht zu Score-Werten gilt auch dann, wenn eine Auskunftei die zur Berechnung der Score-Werte erforderlichen Daten zwar noch nicht personenbezogen speichert, den Personenbezug aber bei der Berechnung herstellt. Falls die Auskunftei vom Betroffenen den Nachweis seiner Identität durch Personalausweiskopie verlangt, ist dieser berechtigt, nicht erforderliche Daten auf der Kopie zu schwärzen.[24]

Die Auskunft ist einmal im Jahr kostenlos. Für jede weitere Auskunft innerhalb eines Jahres kann ein kostendeckendes Entgelt für den Aufwand verlangt werden. Die unterlassene, nicht richtige, unvollständige oder nicht rechtzeitig erteilte Auskunft ist nach § 43 Abs. 1 Nr. 8a bis 8c BDSG ein Bußgeldtatbestand.

5.2 Bonitätsauskünfte über Mietinteressenten

Um dem Risiko eventueller Zahlungsausfälle vorzubeugen, holen Vermieter bei Auskunfteien häufig Bonitätsauskünfte über Mietinteressenten ein. In einigen Fällen müssen Bewerber sogar eine sogenannte Selbstauskunft vorzeigen.

Vermieter dürfen erst dann Bonitätsinformationen über Mietinteressenten bei Auskunfteien einholen, wenn der konkrete Abschluss eines Mietvertrages nur noch von dem positiven Ergebnis einer Bonitätsprüfung abhängt. Sie müssen ein berechtigtes Interesse an den Bonitätsauskünften glaubhaft darlegen. Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit die Miete und die Nebenkosten nicht begleichen, ist ein berechtigtes Interesse an den Auskünften durchaus anzuerkennen.

Dem stehen die schutzwürdigen Belange der Mietinteressenten gegenüber. In die nach § 29 Bundesdatenschutzgesetz (BDSG) erforderliche Interessenabwägung sind insbesondere die existenzielle Bedeutung von Wohnraum, die Vorgaben der gesetzlichen Regelung im Bereich des Mietrechts (wie Kündi-

[24] vgl. A 14.2

gungsmöglichkeiten, Mietkautionen oder Vermieterpfandrecht) und der mögliche Eintritt von Sozialbehörden in die Zahlungspflicht zu berücksichtigen. Auskunfteien dürfen somit nur einen eingeschränkten Datenkatalog an Vermieter übermitteln. Dabei handelt es sich um folgende Datenkategorien:

- Informationen aus öffentlichen Schuldner- oder Insolvenzverzeichnissen,

- sonstige Daten über negatives Zahlungsverhalten, bei denen die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und eine Bagatellgrenze von insgesamt 1.500 Euro überschritten wird.

Die Beschränkung der Auskunft auf das zurückliegende Jahr bedeutet für den Betroffenen eine „zweite Chance“. Wer alle ausstehenden Forderungen beglichen und sich ein Jahr lang als solvent erwiesen hat, soll nicht durch erledigte Sachverhalte aus der Vergangenheit unvertretbar bei der Suche nach Wohnraum behindert werden. Die festgelegte Bagatellgrenze soll verhindern, dass offene Kleinstbeträge den Abschluss eines Mietvertrages unverhältnismäßig erschweren.

Unzulässig ist die Übermittlung von Wahrscheinlichkeitswerten (sog. Score-Werten), sofern diese auf anderen Informationen als den oben beschriebenen Datenkategorien basieren. Außerdem ist es unzulässig, die Vorlage einer Selbstauskunft zu verlangen, die Mietinteressenten bei den Auskunfteien selbst einholen können. Solche Selbstauskünfte können wesentlich mehr Angaben über die finanziellen Verhältnisse der Betroffenen enthalten, als sie etwa den Vermietern als Vertragspartei der Auskunftei mitgeteilt würden. Auch darf von den Mietinteressierten keine Einwilligung in die Einholung einer Bonitätsauskunft verlangt werden, da diese Einwilligung aufgrund der Zwangslage der Betroffenen regelmäßig nicht freiwillig erteilt werden kann und damit unwirksam ist.

Wohnungswirtschaft bzw. Auskunfteien sind nach wie vor aufgefordert, Bonitätsinformationen über Mietinteressenten nur in einem Umfang zu erheben bzw. zu übermitteln, der die schutzwürdigen Belange der Betroffenen angemessen berücksichtigt.

5.3 Datenverarbeitung durch eine Wirtschaftsauskunftei

Der Inhaber dreier Firmen erhält seit Jahren von einer Auskunftei Fragebögen zu seiner unternehmerischen Tätigkeit. Neben der genauen Anschrift und den Tätigkeitsmerkmalen werden Daten über Aktiva und Passiva, Bilanzen sowie zur Bankverbindung abgefragt. Der Unternehmer

erkundigte sich bei uns, ob dies zulässig ist, und welche seiner Daten durch die Auskunftei an Dritte weitergegeben werden dürfen.

Personenbezogene Daten dürfen nach § 29 Bundesdatenschutzgesetz (BDSG) durch Auskunfteien erhoben und an Dritte weitergegeben werden, soweit der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Außerdem darf der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. In jedem Fall sind die Persönlichkeitsrechte des Betroffenen mit den Interessen des Anfragenden abzuwägen.

Regelmäßig sind schutzwürdige Belange des Betroffenen nicht beeinträchtigt, wenn durch die Auskunfteien nur richtige, objektive und aussagekräftige Informationen über die Bonität und sonstige wirtschaftliche Verhältnisse weitergegeben werden. Auskunfteien dürfen ohne Einwilligung der Betroffenen personenbezogene Daten erheben, speichern und an Dritte weitergeben, wenn die Daten aus allgemein zugänglichen Quellen wie Telefon- und Adressbüchern sowie Branchenverzeichnissen oder öffentlichen Registern wie dem Handelsregister oder dem Schuldnerverzeichnis stammen. Auch bei Hinweisen auf nicht vertragsgemäßes Zahlungsverhalten im Waren- und Dienstleistungsverkehr überwiegt das berechtigte Interesse der Anfragenden an der Kenntnis der Daten.

Schutzwürdige Interessen des Betroffenen stehen der Verwendung der Daten entgegen, wenn die Angaben nicht der Beurteilung seiner Kreditwürdigkeit und Zahlungsfähigkeit dienen. Aussagen wie beispielsweise „playboyhaftes Verhalten“ oder „schlechter Gesundheitszustand“ verletzen daher das Persönlichkeitsrecht des Betroffenen. Aus demselben Grund dürfen Vermögensangaben über Ehe- und Lebenspartner sowie Verwandte nicht übermittelt werden.

Eine Auskunft dürfen nur solche anfragenden Stellen bekommen, die vor einem konkreten Vertragsabschluss stehen und die Informationen benötigen, um das finanzielle Risiko besser abschätzen zu können.

Auskunfteien fordern Unternehmen und Privatpersonen teilweise auf, Auskunft über ihre Wirtschafts- und Vermögensverhältnisse zu erteilen. Dies soll dazu dienen, von vornherein eine Speicherung unrichtiger Daten zu vermeiden. Die Erteilung einer solchen Auskunft ist stets freiwillig. Das trifft auch auf die Beantwortung der im vorliegenden Fall übersandten Fragebögen zu. Darauf haben wir den Petenten hingewiesen. Wenn ihnen konkrete Informationen fehlen, verarbeiten einige Auskunfteien auch statistische Daten (Schätzdaten) zu Unternehmen und gewerblich tätigen Einzelpersonen. Diese Daten müssen entsprechend gekennzeichnet werden. Wir haben dem Petenten empfohlen, eine Selbstauskunft bei der betreffenden Auskunftei

einzuholen, um die Richtigkeit seiner Daten sowie die Zulässigkeit ihrer Speicherung zu überprüfen.

Die Weitergabe personenbezogener Daten durch Auskunfteien muss in jedem Einzelfall auf ihre Geeignetheit und Erforderlichkeit geprüft werden. Das Interesse des Anfragenden ist zudem mit den Persönlichkeitsrechten des Betroffenen abzuwägen. Auskünfte, die eine Auskunftei beim Betroffenen per Fragebögen einholt, sind stets freiwillig.

6 Bauen

6.1 Daten von Immobilieneigentümern im Internet

Im Rahmen eines Planfeststellungsverfahrens zum Ausbau einer Bundesstraße veröffentlichte die Behörde das Grunderwerbsverzeichnis zwecks Anhörung der Betroffenen im Internet. Sie versäumte es jedoch, die darin enthaltenen personenbezogenen Daten der Grundstückseigentümer zu anonymisieren.

Ein betroffener Grundstückseigentümer informierte uns über die Angelegenheit. Wir stellten fest, dass die Planfeststellungsbehörde das Verzeichnis im Rahmen der Anhörung tatsächlich einschließlich der Daten zu den Eigentumsverhältnissen der Betroffenen ins Internet gestellt hatte. Teilweise fanden sich darin nicht nur die vollständige Anschrift, sondern im Falle einer Eigentümerin sogar deren Geburtsname und -datum.

Veröffentlichungen personenbezogener Daten durch öffentliche Stellen unterliegen dem Vorbehalt einer gesetzlichen Regelung, die eine eindeutige Erlaubnis hierfür enthalten muss. Im vorliegenden Fall ist eine solche Regelung jedoch nicht zu erkennen. Zwar muss der ausgelegte Plan im Rahmen des Planfeststellungsverfahrens Erläuterungen enthalten, die das Vorhaben, seinen Anlass und die davon betroffenen Grundstücke und Anlagen genau bezeichnen. Auch gehört eine separate Auflistung der Grundeigentümer zu den Planunterlagen. Diese dient aber lediglich der Verwaltung zur Ermittlung der nicht ortsansässigen Eigentümer. Sie gehört nicht zu den auszulegenden Unterlagen und darf keinesfalls im Internet veröffentlicht werden.

Die geschilderte Rechtslage geht auch aus dem Erlass des Ministeriums für Infrastruktur und Raumordnung zu den Richtlinien nach dem Bundesfernstraßengesetz vom 4. Januar 2008 hervor. Mit diesem Erlass wird die Anwendung der Planfeststellungsrichtlinien 2007 des Bundesministeriums für Verkehr für die Auftragsverwaltung durch die brandenburgischen Behörden

vorgeschrieben. Neben den Verfahren zur Planfeststellung von Bundesfernstraßen gelten sie in weiten Teilen auch für die Planung von Landesstraßen. Für die im Zuständigkeitsbereich der Landkreise, kreisfreien Städte und Gemeinden des Landes Brandenburg liegenden Straßen wird ihre Anwendung empfohlen.

Die Planfeststellungsbehörde darf die Daten der vom Vorhaben betroffenen Grundstückseigentümer nicht im Internet veröffentlichen. Im konkreten Fall wurde die abweichende Praxis der Behörde umgehend unterbunden.

6.2 Fotografien von Grundstückszufahrten durch das Tiefbauamt

Eine Stadtverwaltung erkundigte sich nach der datenschutzrechtlichen Zulässigkeit von Fotografien der Grundstückszufahrten einer Straße. Sie beabsichtigte, mithilfe der Bilder den Zustand der Zufahrten sowie ihre Entscheidung, diese auszubauen, zu dokumentieren.

Städte und Gemeinden sind auf der Grundlage des Brandenburgischen Straßengesetzes verpflichtet, die Straßen den Verkehrsbedürfnissen entsprechend zu unterhalten und auszubauen. Anlieger dieser Straßen haben dafür Sorge zu tragen, dass der Ausbauzustand der Zufahrten zu ihren Grundstücken den sich daraus ergebenden Anforderungen entspricht. Bei der Entscheidung über die Notwendigkeit des Ausbaus einer Zufahrt ist neben deren aktuellem Zustand beispielsweise zu berücksichtigen, ob sich Fahrzeuge auf dem Grundstück befinden bzw. ob der Grünstreifen befahren wird. Die Stadtverwaltung entscheidet regelmäßig im Rahmen einer Ortsbesichtigung, ob ein Ausbau der Zufahrt gegebenenfalls auch entgegen dem Willen des Grundstückeigentümers erforderlich ist. Kommt die Verwaltungsbehörde zur Überzeugung, dass die Zufahrt ausgebaut werden muss, so hat der Grundstückseigentümer die hierfür entstehenden Kosten zu tragen.

Die Fotografie einer Grundstückszufahrt weist einen Bezug bzw. eine Beziehbarkeit zur Person des Grundstückeigentümers oder Nutzers auf und fällt daher unter den Begriff des personenbezogenen Datums. Die Erhebung personenbezogener Daten ist u. a. nur zulässig, wenn dies zur Erfüllung der gesetzlichen Aufgabe durch die zuständige Stelle erforderlich ist. Davon ist insbesondere im Interesse einer für den Betroffenen nachvollziehbaren Aktenführung im Rahmen des Verwaltungsverfahrens in der Regel auszugehen. Dennoch muss die Erhebung nach datenschutzrechtlichen Grundsätzen erfolgen:

Die Erforderlichkeit ist im Hinblick auf alternative, weniger eingriffsintensive Maßnahmen zur Erhebung von Informationen zu prüfen. Die Stadtverwaltung

teilte uns in diesem Zusammenhang mit, Fotografien nur dann verwenden zu wollen, wenn die Grundstückseigentümer im Anhörungsverfahren keine Stellungnahme abgegeben oder sich gegen den Ausbau ihrer Zufahrt ausgesprochen haben, die Behörde den Ausbau jedoch für notwendig hält. Im Sinne der Datensparsamkeit dürfen die Bilder nur solche personenbezogenen Informationen beinhalten, die für die Aufgabenerledigung erforderlich sind. Die Dokumentation der Kfz-Kennzeichen von Fahrzeugen, die auf den Grundstücken geparkt sind, gehört nicht dazu. Sie dürfen von vornherein nicht fotografiert werden. Soweit dies aber bereits erfolgt ist, sind die vorhandenen Daten zu löschen (z. B. durch Schwärzen). Die betroffenen Grundstückseigentümer sind über die Absicht der Behörde, ihre Zufahrten im Rahmen eines Ortstermins zu fotografieren, rechtzeitig in Kenntnis zu setzen. Ihnen ist Gelegenheit zu geben, bei der Erhebung anwesend zu sein.

Das Fotografieren einer Grundstückszufahrt stellt eine Erhebung personenbezogener Daten dar. Diese kann zur Erfüllung der Aufgaben auf dem Gebiet des Straßenausbaus erforderlich sein. Zu beachten ist, dass auf den Bildern keine Kfz-Kennzeichen abgebildet und die Grundstückseigentümer über die Aufnahmen rechtzeitig informiert werden.

6.3 Projektfortschritte im Virtuellen Bauamt

Das Virtuelle Bauamt ist eine Internetplattform des Landes, die die elektronische Vorbereitung und Einreichung von Bauanträgen ermöglicht. Das Projekt hat in den letzten zwei Jahren datenschutzrechtliche Fortschritte gemacht.

In unserem letzten Tätigkeitsbericht[25] zeigten wir diverse, im Projekt unzureichend geklärte Fragen auf. Diese sind inzwischen einvernehmlich mit den zuständigen Verantwortlichen abgestimmt worden. Hierzu gehören folgende Aspekte:

- Die Verantwortlichkeiten der beteiligten Stellen nach dem Brandenburgischen Datenschutzgesetz und dem Telemediengesetz wurden bezüglich der einzelnen Komponenten des Virtuellen Bauamtes und der korrespondierenden Phasen der Bauantragsabwicklung eindeutig festgelegt.

- Die Datenerhebung in der Komponente „Vorbereitungsraum“ kann nur auf freiwilliger Basis erfolgen. Dies wird jetzt in einer Erklärung zur Datenverarbeitung für die Nutzer transparent gemacht.

[25] vgl. Tätigkeitsbericht 2008/2009, A 2.7.3

- Es wurde eine Einwilligungserklärung nach § 13 Telemediengesetz erstellt. Sie informiert ausführlich über die Art, den Umfang und die Zwecke der Erhebung und Verwendung personenbezogener Daten und nennt die Daten verarbeitenden Stellen.

- Nicht datenschutzgerechte Module wurden aus der Plattform entfernt.

Im Rahmen der landesweiten Einführung stehen nun vor der datenschutzrechtlichen Freigabe die Erstellung und Umsetzung von IT-Sicherheitskonzepten an, um durch technische und organisatorische Maßnahmen die Gefahren für die informationelle Selbstbestimmung der Nutzenden zu minimieren.

Durch unsere intensive Begleitung des Projektes Virtuelles Bauamt konnten die notwendigen datenschutzrechtlichen Verbesserungen erreicht werden. In der nächsten Zeit wird es darauf ankommen, auch die erforderlichen technischen und organisatorischen Maßnahmen in allen Daten verarbeitenden Stellen vollständig zu ermitteln und umzusetzen.

7 Beschäftigtendatenschutz

7.1 Einsicht in Personalakten bei Lohnsteueraußenprüfung

Ein eingetragener Verein fragte an, ob das Finanzamt berechtigt ist, im Rahmen einer Lohnsteueraußenprüfung ganz oder nur teilweise in Personalakten Einsicht zu nehmen.

Die Lohnsteueraußenprüfung dient der Ermittlung der steuerlichen Verhältnisse des Steuerpflichtigen, kann sich jedoch auch auf die Verhältnisse anderer Personen beziehen, wenn der Steuerpflichtige – wie in diesem Fall – verpflichtet war, für Rechnung dieser Personen Steuern zu entrichten.

Die Außenprüfung umfasst nach § 199 Abs. 1 Abgabenordnung (AO) die tatsächlichen und rechtlichen Verhältnisse, die für die Steuerpflicht und für die Bemessung der Steuer maßgebend sind (Besteuerungsgrundlagen). Insoweit hat auch der Steuerpflichtige bei der Feststellung der Sachverhalte mitzuwirken, die für die Besteuerung erheblich sein können. Nach § 42f Abs. 2 Satz 2 AO haben zudem die Arbeitnehmer des Steuerpflichtigen/Arbeitgebers dem mit der Außenprüfung Beauftragten Auskunft über Art und Höhe ihrer Einnahmen zu geben und auf Verlangen die ggf. in ihrem Besitz befindlichen Lohnsteuerkarten sowie Belege über bereits entrichtete Lohnsteuer vorzulegen.

Nach § 42f Abs. 3 der Lohnsteuerrichtlinie (LStR) hat sich die Lohnsteueraußenprüfung hauptsächlich darauf zu erstrecken, ob sämtliche Arbeitnehmer (auch die nicht ständig beschäftigten) erfasst wurden, alle zum Arbeitslohn gehörigen Einnahmen, gleichgültig, in welcher Form sie gewährt wurden, dem Steuerabzug unterworfen wurden und ob bei der Berechnung der Lohnsteuer von der richtigen Lohnhöhe ausgegangen wurde. Gemäß § 200 Abs. 1 Satz 2 AO sind insbesondere Auskünfte zu erteilen, Aufzeichnungen, Bücher, Geschäftspapiere und andere Urkunden zur Einsicht und Prüfung vorzulegen. Bei der Lohnsteueraußenprüfung und damit der Überwachung der ordnungsgemäßen Einbehaltung und Abführung der Steuern vom Lohn (Lohnsteuer, Kirchensteuer und Solidaritätszuschlag) geht es z. B. um die korrekte Abrechnung der Bruttolöhne, die Lohnkonten der Arbeitnehmer, Nettolohnzahlungen, Sachbezüge (geldwerte Vorteile), Fahrkostenersatz für Fahrten zwischen Wohnung und Arbeitsstätte, Pauschalierung der Lohnsteuer, Aushilfslöhne (geringfügig und kurzfristig Beschäftigte), steuerfreie Zuschläge für Sonntags-, Feiertags- und Nachtarbeit, Geschenke und Bewirtungen, besondere Zuwendungen (Geburtsbeihilfen, Leistungen zur Gesundheitsförderung), Kinderbetreuungskosten, die Abgrenzung zwischen Mitarbeitern und Freiberuflern und die Arbeitsverträge mit nahen Angehörigen. Vorzulegen sind insoweit Lohn- und Geschäftsbücher sowie Anstellungsverträge und Verträge, die die Gewährung geldwerter Vorteile beinhalten könnten (Miet-, Kauf- oder Darlehensverträge).

In Personalakten können sowohl steuerlich relevante als auch steuerlich nicht relevante Daten enthalten sein. So können Anstellungs- oder Dienstverträge, Darlehensverträge, Miet- oder Kaufverträge oder sonstige Nebenabreden, die die Gewährung von geldwerten Vorteilen zum Inhalt haben, z. B. Aufschluss über Sonderzahlungen, wie Gratifikationen, Beihilfen und Abfindungen geben. Gegen die Vorlagepflicht einzelner Unterlagen aus der Personalakte, wie z. B. den Dienstvertrag, bestehen insoweit keine Bedenken. Weitere Dokumente dürfen nur dann eingesehen werden, wenn der Prüfer in anderen Unterlagen Sachverhalte festgestellt hat, die zur Überprüfung der ordnungsgemäßen Lohnversteuerung berechtigen (z. B. bei der Durchsicht der Konten finden sich konkrete Anhaltspunkte dafür, dass ein Arbeitnehmer besondere Zuwendungen erhalten hat). In den Personalakten ebenfalls enthalten sind in der Regel jedoch auch Lebensläufe, Zeugnisse, Beurteilungen und Angaben zu Krankheiten oder Schwerbehinderungen. Diese höchstpersönlichen Daten haben keine lohnsteuerliche Relevanz und sind daher nicht vorzulegen. Vielmehr müsste im konkreten Einzelfall eine Interessenabwägung zwischen dem Schutz der Privatsphäre und der lückenlosen Ermittlung des Steueranspruchs vorgenommen werden. Zu beachten ist dabei der Grundsatz des geringstmöglichen Eingriffs in die Privatsphäre. Gegebenenfalls hat der Arbeitgeber für die Trennung der Daten zu sorgen.

Das Finanzamt darf nur in die Teile der Personalakte Einsicht nehmen, die zur Überprüfung der ordnungsgemäßen Lohnversteuerung erforderlich sind.

7.2 Krankmeldung ohne Krankenschein aber mit Angabe der Erkrankung?

Ein Dienststellenleiter hatte seine Personalstelle angewiesen, bei Krankmeldungen ohne Krankenschein Bedienstete nach dem Grund der Erkrankung zu befragen. Der Personalrat zweifelte an der Rechtmäßigkeit dieser Datenerhebung.

Die Frage nach den Gründen einer Arbeitsunfähigkeit ist aus datenschutzrechtlicher Sicht unzulässig. Personenbezogene Daten dürfen in Dienst- und Arbeitsverhältnissen nur nach § 29 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) bzw. den Vorschriften des Landesbeamtengesetzes verarbeitet werden. Weder § 29 Abs. 1 BbgDSG noch § 61 Abs. 1 Landesbeamtengesetz (LBG) oder § 5 Abs. 1 Entgeltfortzahlungsgesetz (EntgFG) legitimierten diese Anweisung.

Der Arbeitgeber/Dienstherr kann bei begründetem Missbrauchsverdacht die Vorlage eines Krankenscheins früher als nach drei Kalendertagen oder sofort verlangen. Der Gesetzgeber hat das ausdrücklich in § 61 Abs. 1 LBG und § 5 Abs. 1 EntgFG geregelt.

Ein Arbeitgeber oder Dienstherr hat in keinem Fall das Recht, einen arbeitsunfähigen Mitarbeiter nach dem Grund seiner Erkrankung zu fragen.

7.3 Datenübermittlungen im Bewerbungsverfahren

Ein Arbeitgeberzusammenschluss (GmbH) bat um datenschutzrechtliche Hinweise zur Übermittlung von Bewerbungen durch ein Mitgliedsunternehmen an die GmbH.

Der Arbeitgeberzusammenschluss, der aus einer Vielzahl regionaler Unternehmen besteht, hat u. a. zum Ziel, Arbeitskräfte gezielt in diesen Unternehmen einzusetzen. Die GmbH bietet nicht nur selbst Arbeits- und Ausbildungsplätze an, sondern möchte auch das Bewerberpotenzial der Mitgliedsunternehmen berücksichtigen.

Personenbezogene Daten dürfen gem. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur dann übermittelt werden, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewil-

ligt hat. Eine Erlaubnisnorm zur Weitergabe der Bewerberdaten ist in diesem Fall nicht ersichtlich.

Wer sich bei einem Mitgliedsunternehmen bewirbt, geht davon aus, dass nur dieses Unternehmen seine Bewerbung zur Kenntnis nimmt. Der Arbeitgeber erhebt die personenbezogenen Daten des Bewerbers nur für einen bestimmten Zweck und darf sie nicht an andere Unternehmen weiterreichen. Dies gilt auch für einen Unternehmenszusammenschluss.

Ein Bewerber, dessen Unterlagen weitergegeben werden sollen, muss in die Übermittlung unter Beachtung des § 4a BDSG einwilligen. Diesem gesetzlichen Erfordernis kann auf zwei Wegen Rechnung getragen werden:

- Das Unternehmen weist bereits bei seiner Stellenausschreibung darauf hin, dass die Betroffenen schriftlich einwilligen können, wenn sie im Falle einer Nichtberücksichtigung die Weitergabe ihrer Bewerbung an den Arbeitgeberzusammenschluss wünschen.

- Das Unternehmen informiert den Bewerber im Ablehnungsschreiben über die Möglichkeit der Übermittlung der Bewerbung an den Arbeitgeberzusammenschluss. Erst bei Vorlage der schriftlichen Einwilligung darf die Bewerbung weitergegeben werden.

Ausgeschlossen ist, dass die Mitgliedsunternehmen den Arbeitgeberzusammenschluss damit beauftragen, die Einwilligung einzuholen. Hierfür werden bereits personenbezogene Daten des Bewerbers zur Kontaktaufnahme benötigt.

Unternehmen dürfen Bewerbungen nicht an andere Arbeitgeber übermitteln, es sei denn, die Bewerber haben ausdrücklich eingewilligt.

7.4 Videoüberwachung von Mitarbeitern einer Produktionsfirma

In einer Produktionsfirma wurden die Mitarbeiter ununterbrochen videoüberwacht und das sowohl in der Produktionshalle als auch im Außenbereich.

Bei der Kontrolle vor Ort, die aufgrund eines anonymen Hinweises eingeleitet wurde, haben wir in der nicht öffentlich zugänglichen und nicht allzu großen Fertigungshalle acht Kameras festgestellt. Der zu den Betriebszeiten öffentlich zugängliche, aber eingefriedete Außenbereich wurde auch an mehreren Stellen überwacht.

Die Geschäftsleitung begründete den Zweck der Videoüberwachung mit einem Materialdiebstahl, der zum Zeitpunkt der Einrichtung der Überwachung bereits ein Jahr zurücklag, und zwar sowohl im Innen- als auch im Außenbereich. Die Alarmanlage habe sich seinerzeit nicht als ausreichender Schutz erwiesen. Die Videokameras sollten weiteren Diebstählen vorbeugen.

7.4.1 Offene Videoüberwachung in der Fertigungshalle

Wir haben gefordert, die Kameras in der Produktionshalle abzubauen. Der Einsatz der Videokameras war unzulässig, weil er gegen § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) verstieß. Nach dieser Vorschrift dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. § 32 Abs. 1 Satz 1 Alt. 2 BDSG erfasst insbesondere Maßnahmen zur Kontrolle des Verhaltens und der Leistung von Arbeitnehmern.

Nach dem allgemeinen datenschutzrechtlichen Grundsatz der Verhältnismäßigkeit ist jede Daten verarbeitende Stelle aber nur soweit zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten berechtigt, wie diese geeignet, erforderlich und angemessen ist.

Die Videoüberwachung ist zwar geeignet, um Mitarbeiter von Diebstählen abzuhalten oder begangene Diebstähle aufzudecken. Hinsichtlich der Erforderlichkeit bestehen bereits Zweifel, weil weniger eingriffsintensive Mittel als eine permanente Überwachung zur Verfügung stehen, um den gewünschten Zweck zu erreichen.

Die andauernde Videoüberwachung der Mitarbeiter in der Produktion war jedenfalls keine angemessene Maßnahme. Es hätte seitens der Verantwortlichen einer Rechtsgüterabwägung bedurft. Das Interesse des Arbeitgebers an der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten wird grundrechtlich von seinem Eigentumsrecht und dem Recht am eingerichteten und ausgeübten Gewerbebetrieb erfasst. Dem steht aber insbesondere das allgemeine Persönlichkeitsrecht der Beschäftigten entgegen. Keines der genannten Grundrechte geht dem anderen vor. Für die Angemessenheit einer grundrechtsbeschränkenden Maßnahme ist daher die Intensität des Eingriffs entscheidend.

Von den 21 Mitarbeitern des Unternehmens wurden mehr als 10 der ständigen Videoüberwachung ausgesetzt. Keiner dieser Mitarbeiter hatte hierfür einen Anlass gegeben. Nur ein Diebstahl im Vorfeld des Einsatzes der Kame-

ras wurde durch einen Mitarbeiter begangen, dem daraufhin fristlos gekündigt wurde. Mit den Videokameras innerhalb der Fertigungshalle erzeugte die Unternehmensleitung einen permanenten Überwachungsdruck bei den Beschäftigten, der insbesondere durch die anonyme Eingabe bestätigt wurde. Hinzu kommt, dass die Dauer der Überwachungsmaßnahme einen umso schwereren Grundrechtseingriff darstellt, je länger sie anhält (in diesem Fall ca. zwei Jahre dauerhaft). Dabei kam es nicht darauf an, wann und wie lange die Betriebsleitung die übertragenen Videoaufzeichnungen am Auswertungs-PC zur Kenntnis nehmen konnte.

7.4.2 Offene Videoüberwachung im Außenbereich

Bezüglich der Kameras im Außenbereich haben wir verlangt, sie so zu konfigurieren, dass eine Videoüberwachung nicht zu den Betriebs- oder Geschäftszeiten stattfindet. Während dieser Zeiten war der Einsatz der Videokameras unzulässig und hat gegen § 6b Abs. 3 i. V. m. Abs. 1 Nr. 3 BDSG verstoßen.

Auch in diesem Fall hätten, wie oben beschrieben, die widerstreitenden Interessen des Unternehmers mit denen der Beschäftigten abgewogen werden müssen. Gerade die Mitarbeiter, die im Außenbereich ihrer Arbeit nachgingen, waren durch Videokameras, die die unmittelbare Umgebung der Gebäudekomplexe beobachteten, der ständigen Überwachung ausgesetzt.

Während der Geschäfts- und Betriebszeiten kann durchaus auf andere Weise kontrolliert werden, ob Unberechtigte Material oder fertige Produkte entwenden. Sobald jedoch das Betriebsgelände verschlossen wird, ist der Einsatz der Kameras zur Überwachung des Außenbereichs unproblematisch.

Nur unter den engen Voraussetzungen des § 32 BDSG ist eine offene Videoüberwachung von Mitarbeitern in nicht öffentlich zugänglichen Räumen zulässig. Das Unternehmen ist unseren Forderungen sofort nachgekommen und hat die Kameras im Innenbereich abgebaut. Die Außenkameras wurden so konfiguriert, dass eine Überwachung nur außerhalb der Geschäftszeiten stattfindet.

7.5 PersOn und PTravel – Personaldatenschutz bei gemeinsamen Verfahren

Mit der letzten Novellierung des Brandenburgischen Datenschutzgesetzes (BbgDSG)[26] im Mai 2010 wurden auch Regelungen zum Datenschutz bei so genannten gemeinsamen Verfahren eingeführt. Inzwischen liegen erste Erfahrungen aus zwei landesweiten Projekten vor.

Gemeinsame Verfahren zeichnen sich gem. § 9 Abs. 1 BbgDSG dadurch aus, dass mehrere Daten verarbeitende Stellen personenbezogene Daten in oder aus einem gemeinsamen Datenbestand automatisiert verarbeiten. Die Einrichtung solcher Verfahren ist zulässig, soweit sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen sind. Unsere Behörde ist vorab zu unterrichten.

In § 9 Abs. 1a BbgDSG wird gefordert, dass vor der Einrichtung eines gemeinsamen Verfahrens eine Stelle bestimmt wird, der die Planung, Einrichtung und Durchführung des Verfahrens obliegt. Weiter sind die beteiligten Stellen, ihre Aufgaben und ihr Verantwortungsbereich im Rahmen der Datenverarbeitung sowie die zu treffenden technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und IT-Sicherheit schriftlich festzulegen. § 9 Abs. 1b BbgDSG erlaubt Betroffenen, ihre Rechte u. a. auf Auskunft, Berichtigung und Löschung ihrer Daten gegenüber jeder der an dem gemeinsamen Verfahren beteiligten Stellen geltend zu machen.

Im Berichtszeitraum begleiteten wir zwei Projekte, bei denen in gemeinsamen Verfahren personenbezogene Daten der Beschäftigten der Landesverwaltung automatisiert verarbeitet werden:

- Das Projekt PersOn dient der Unterstützung des Tarifvertrages über Maßnahmen zur Begleitung des Umbaus in der Landesverwaltung (TV Umbau). Danach haben Beschäftigte, deren Arbeitsplatz z. B. aufgrund von strukturellen Umgestaltungen in der Landesverwaltung ganz oder teilweise wegfällt, einen Anspruch auf Vermittlung eines anderen Arbeitsplatzes und ggf. Maßnahmen der Qualifizierung, Einkommenssicherung oder Mobilitätsprämien. Weiterhin ermöglicht das DV-Verfahren solchen Beschäftigten, die einen neuen Arbeitsplatz in der Landesverwaltung suchen (den sogenannten Rotationswilligen), die gezielte Recherche nach freien Beschäftigungspositionen.

[26] Gesetz zum Schutz personenbezogener Daten im Land Brandenburg vom 15. Mai 2008 (GVBl. I/08, S. 114), zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Mai 2010 (GVBl. I/10, Nr. 21)

- Im Projekt PTravel wird die in der Koalitionsvereinbarung der aktuellen Landesregierung als Ziel formulierte Zentralisierung der Reisekostenbearbeitung bei der Zentralen Bezügestelle des Landes Brandenburg (ZBB) umgesetzt. Das zugehörige DV-Verfahren bildet dabei den kompletten Prozess der Beantragung, Genehmigung und Abrechnung von Dienstreisen ab. Als Besonderheit ist hier zu beachten, dass die Beauftragung der ZBB mit der Reisekostenabrechnung datenschutzrechtlich eine Funktionsübertragung darstellt, die gem. § 63 Abs. 3 Landesbeamtengesetz einer Rechtsverordnung bedarf.

Die Verantwortlichen beider Projekte haben unsere Behörde frühzeitig in die Arbeit eingebunden. Auf diese Weise war es uns möglich, den Prozess der Umsetzung der gesetzlichen Anforderungen von Anfang an zu begleiten. In beiden Projekten wurden durch die für die Planung, Einrichtung und Durchführung des Verfahrens zuständige zentrale Stelle (für PersOn das Zentrale Personalmanagement im Ministerium des Innern, für PTravel die Zentrale Bezügestelle im Geschäftsbereich des Ministeriums für Finanzen) u. a. IT-Sicherheitskonzepte für die zentralen Verfahrenskomponenten sowie Musterkonzepte für die dezentralen Verfahrenskomponenten in den beteiligten Stellen erarbeitet. Diese Vorgehensweise hatten wir bereits vor der Einführung der gesetzlichen Regelungen zu gemeinsamen Verfahren im Projekt Neues Finanzmanagement angeregt und dort erfolgreich begleitet.[27]

Schwierigkeiten bei der Einführung des Verfahrens PersOn gab es in Bezug auf die Mitbestimmung durch die Personalräte. Diese ist gem. § 65 Nr. 1 Personalvertretungsgesetz des Landes Brandenburg u. a. für die Einführung und Anwendung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten außerhalb von Besoldungs-, Vergütungs- u. ä. Leistungen erforderlich. Die Zuständigkeit jedes Personalrats erstreckt sich jedoch nur auf den eigenen Bereich, für Hauptpersonalräte auf den Geschäftsbereich des jeweiligen Ressorts. Da im Land Brandenburg kein Gesamtpersonalrat für die gesamte Landesverwaltung existiert (wie in anderen Bundesländern), gibt es auch keinen Personalrat, der für alle anderen bei der Einführung der zentralen, gemeinsam genutzten Verfahrenskomponenten von PersOn mitbestimmen könnte.

In Abstimmung mit den Beteiligten haben wir hierzu eine pragmatische Übergangslösung vorgeschlagen: Jeder örtliche bzw. Hauptpersonalrat kann beim Zentralen Personalmanagement im Ministerium des Innern die erforderlichen Unterlagen einsehen und so alle Informationen erhalten, die für seine Entscheidung über eine Mitbestimmung notwendig sind. Alternativ wäre es denkbar, einen (Haupt-)Personalrat mit dem Mandat auszustatten, die Mitbe-

[27] vgl. Tätigkeitsbericht 2008/2009, A 10.1.1

stimmung für die zentralen Verfahrenskomponenten für alle anderen Personalräte durchzuführen.

Die ersten Erfahrungen mit den neuen Regelungen des Brandenburgischen Datenschutzgesetzes zu gemeinsamen Verfahren sind positiv. Durch die frühzeitige Einbeziehung unserer Behörde konnten die gesetzlichen Anforderungen umgesetzt werden. Noch offen bleibt, wie bei der Verarbeitung von Personaldaten in gemeinsamen Verfahren die Mitbestimmungsrechte der Personalräte umfassend berücksichtigt werden. Der Gesetzgeber ist gefordert, das Personalvertretungsgesetz des Landes in diesem Punkt anzupassen.

7.6 Zugriffe von Vertretern auf E-Mails

Immer wieder tritt im dienstlichen Alltag das Problem auf, wann und unter welchen Bedingungen der Arbeitgeber bzw. Dienstherr oder eine vertretungsberechtigte Person auf die E-Mails eines Mitarbeiters zugreifen darf, wenn dieser krankheitsbedingt oder aus anderen Gründen ausfällt.

Bei der Organisation von Vertretungsrechten für den E-Mail-Verkehr ist zu beachten, dass die Persönlichkeitsrechte der Mitarbeiter betroffen sein können und die Inhalts- und Adressdaten unter Umständen dem Post- und Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz unterliegen. Hinzu kommt, dass möglicherweise Mitarbeiter im Rahmen von Vertretungszugriffen Kenntnis von personenbezogenen Daten erlangen, die für ihre Aufgabenerfüllung nicht erforderlich sind.

Basis für die Regelung von Vertretungszugriffen sind organisatorische Festlegungen (z. B. Dienstanweisungen), die klar definieren, wie mit E-Mails als Kommunikationsmittel im Dienstgeschäft umzugehen ist. Die erste Grundvoraussetzung ist die Klarstellung, ob auch eine private Nutzung des dienstlichen E-Mail-Programms gestattet ist, da die private E-Mail-Korrespondenz der Mitarbeiter dem Post- und Fernmeldegeheimnis unterliegt. Auch wenn die private Nutzung untersagt ist, ist es möglich, dass der Betroffene – ohne selbst tätig zu werden – private Nachrichten unter seiner dienstlichen E-Mail-Adresse erhält. Diese Tatsache wird bei der Vergabe von Vertreterrechten häufig außer Acht gelassen und unterstellt, dass bei einer rein dienstlichen Nutzung des E-Mail-Programms alle Nachrichten – einschließlich der eingehenden – dienstlichen Charakter haben.

Der Vertretungszugriff ist organisatorisch so zu regeln, dass bei Abwesenheit des Empfängers ein fachlich zuständiger Mitarbeiter Einsicht nehmen kann. Ist hierbei erkennbar, dass sich auch private E-Mails im Postfach des Abwesenden befinden, dürfen diese nicht geöffnet werden.

Verschiedene Stellen machten uns darauf aufmerksam, dass häufig zwar Regelungen für Vertretungszugriffe in der Verwaltung bestehen, diese aber dann nicht zum Tragen kommen, wenn alle Mitarbeiter eines Fachbereichs oder diejenigen, die für den Vertretungszugriff vorgesehen sind, ausfallen. Dies kann insbesondere bei kleinen Amts- oder Kommunalverwaltungen der Fall sein. In einem solchen Fall können seitens der Dienststellenleitung bis zur Rückkehr des betroffenen Mitarbeiters oder seines Vertreters neue Zugriffsrechte erteilt werden. Diese Änderungen sind zu dokumentieren. Der betroffene Mitarbeiter ist nach seiner Rückkehr darüber zu informieren, dass auf seine Daten zugegriffen wurde. Häufig wird im Nachhinein vergessen, die Vertretungsrechte auf den ursprünglichen Zustand zurückzusetzen. Dies ist jedoch zwingend erforderlich. Gegebenenfalls kann im Nachgang auch eine Neuregelung der Vertretungsrechte seitens der Leitung erfolgen.

Besondere Beachtung muss die Behandlung der E-Mail-Postfächer der Interessenvertretungen (wie Personalrat, Gleichstellungsbeauftragte, Schwerbehindertenbeauftragte) sowie der behördlichen Datenschutzbeauftragen finden. Diese können personenbezogene Daten enthalten, die unter Umständen das Dienstverhältnis, den Gesundheitszustand oder sonstige sensitive Informationen über Mitarbeiter betreffen. Zugriffsrechte im Vertretungsfall dürfen hier nur an Mitglieder des jeweiligen Gremiums vergeben werden. Auch ein Zugriff der Leitung ist hier nicht erlaubt.

Grundlage für den Zugriff auf E-Mails von Mitarbeitern im Rahmen einer Vertretung sind klar nachvollziehbare Regelungen seitens der Dienststelle. Die Einsichtnahme in private E-Mails ist grundsätzlich nicht erlaubt. Änderungen der Vertretungszugriffe sind zu dokumentieren und den Betroffenen zur Kenntnis zu geben.

8 Finanzen

8.1 Vorlage von Kontoauszügen bei Kreditanträgen

Einige Kreditinstitute lassen sich im Rahmen der Prüfung von Kreditanträgen Kontoauszüge der letzten sechs Wochen vorlegen.

Dies ist insofern bedenklich, als neben den kreditrelevanten Daten auf den Kontoauszügen auch sensitive Daten enthalten sein können, wie z. B. Überweisungen an Ärzte, Psychotherapeuten oder politische Parteien. Bei einem Gemeinschaftskonto können die Kontoauszüge zudem personenbezogene Daten von einer Person enthalten, die eventuell keinen Kreditantrag gestellt hat.

Weder die genannten sensitiven Daten noch die Angaben zu den anderen Kontoinhabern sind erforderlich, um den Kreditantrag zu prüfen. Die Betroffenen haben ein Recht, diese Daten zu schwärzen. Sie müssen von den Kreditinstituten auf dieses Recht hingewiesen werden.

Zur Prüfung eines Kreditantrages dürfen personenbezogene Daten nur im erforderlichen Umfang erhoben werden.

8.2 Datenschutzrechtliche Grundlagen für Inkassodienste

Häufig beauftragen Unternehmen Inkassobüros mit der Einziehung ausstehender Forderungen. Personenbezogene Daten der Schuldner werden dabei zwangsläufig weitergegeben. Die Regelungen, die dabei zu beachten sind, hängen wesentlich von der Gestaltung des Inkassovertrags ab.

Soweit Gläubiger ihre Forderungen per Vertrag an ein Inkassounternehmen abtreten, macht Letzteres diese Forderungen im eigenen Namen geltend. Datenschutzrechtlich handelt es sich um eine Funktionsübertragung. Diese liegt vor, wenn das Inkassounternehmen die Aufgabe weitgehend selbstständig und ohne Weisung ausführt. Es handelt insbesondere dann eigenverantwortlich, wenn es die Maßnahmen zur Einziehung von Forderungen frei wählen kann und Entscheidungen hierzu trifft. Die Datenverarbeitung durch das Inkassounternehmen richtet sich im Falle einer solchen Funktionsübertragung nach den Vorschriften des § 28 Abs. 1 Bundesdatenschutzgesetz (BDSG); sie erfolgt für eigene Geschäftszwecke. Das Inkassounternehmen darf die ihm vom Gläubiger übermittelten Daten grundsätzlich nur für den Zweck verarbeiten und nutzen, zu dessen Erfüllung sie übermittelt wurden.

An Stelle einer selbstständigen Aufgabenwahrnehmung durch den Dienstleister kann der Inkassovertrag aber auch eine an die Weisungen des Gläubigers gebundene Hilfstätigkeit vorsehen. Das ist beispielsweise der Fall, wenn das Inkassounternehmen lediglich den Zahlungseingang überwacht, Mahnungen erstellt oder die aktuelle Adresse bzw. Bonität des Schuldners feststellt. In solchen Ausnahmefällen handelt es sich um eine Auftragsdatenverarbeitung nach § 11 BDSG. Dabei ist der Gläubiger als Auftraggeber für die Tätigkeit des Inkassounternehmens datenschutzrechtlich verantwortlich. Die konkreten Befugnisse zur Datenverarbeitung müssen per Vertrag schriftlich festgelegt werden.

Treten Gläubiger ihre Forderungen an Inkassounternehmen ab, verarbeiten diese die Daten der Schuldner nach den Vorschriften für eigene Geschäftszwecke gemäß § 28 BDSG. Werden die Inkassobüros ausnahmsweise nur hilfsweise tätig, handelt es sich um eine Datenverarbeitung im Auftrag gemäß § 11 BDSG.

8.3 Neues Finanzmanagement in der Landesverwaltung

8.3.1 Fortschritte bei der Umsetzung des IT-Sicherheitskonzeptes

In unserem letzten Tätigkeitsbericht[28] hatten wir darauf hingewiesen, dass die Umsetzung des IT-Sicherheitskonzeptes für das Verfahren zum Haushalts-, Kassen- und Rechnungswesen nur langsam vorankommt. Inzwischen sind Fortschritte zu verzeichnen.

Als problematisch sahen wir unter anderem an, dass notwendige Sicherheitsmaßnahmen beim externen Dienstleister nicht oder nur unzureichend umgesetzt waren. Im Berichtszeitraum haben wir daraufhin die Realisierung von IT-Sicherheitsmaßnahmen bei den IT-Systemen des externen Dienstleisters in einem längeren Prozess zusammen mit den Verantwortlichen abgestimmt. Die IT-Sicherheit hat sich in diesem Bereich positiv entwickelt.

Darüber hinaus plant das Ministerium der Finanzen, eine Auditierung der IT-Sicherheit für das Verfahren durchzuführen, also eine Überprüfung durch unabhängige IT-Sicherheitsexperten. Wir haben dem Ministerium bei der Planung und Umsetzung des Projektes unsere Beratung und Unterstützung zugesagt.

Bei der Umsetzung von IT-Sicherheit und Datenschutz im Verfahren zum Haushalts-, Kassen- und Rechnungswesen konnten inzwischen deutliche Verbesserungen erzielt werden. Eine Überprüfung der Sicherheit durch externe Experten ist in Aussicht gestellt.

8.3.2 SAP-Separation der Landesbetriebe

Damit die doppisch buchenden Landesbetriebe den Betrieb ihrer DV-Verfahren im Neuen Finanzmanagement (NFM) technisch selbstständig und flexibler durchführen können, wurde im Berichtszeitraum ihre Herauslösung aus dem zentralen SAP-System der Landesverwaltung und die Installation jeweils eigener SAP-Systeme vorgenommen.

[28] vgl. Tätigkeitsbericht 2008/2009, A 10.1.2

Das Ministerium der Finanzen (MdF) hatte zuvor eine Richtlinie erlassen, in der die zentralen Regelungen für die Organisation und Steuerung eines verteilten Betriebs des Neuen Finanzmanagements festgelegt wurden. Die Landesbetriebe sind demnach verpflichtet, den technischen SAP-Betrieb inklusive Applikationsbetreuung beim jetzigen externen Dienstleister und die SNC-Verschlüsselung im Rahmen der zentralen Betriebsverträge durch individuelle Betriebsverträge für ihren NFM-Betrieb zu sichern. Diese Regelung dient auch dazu, ein einheitliches Datenschutz- und IT-Sicherheitsniveau in der Landesverwaltung zu gewährleisten.

Auf unsere Nachfrage hin haben uns die Verantwortlichen kompetent und ausführlich über den Separationsprozess informiert. Die Migration der Daten erfolgte durch Kopieren des gesamten Ursprungsmandanten und anschließendes Löschen der nicht benötigten Daten. Beim Dienstleister wird die Trennung der SAP-Systeme über die Einrichtung gesonderter Hardware bzw. eigener sogenannter LPARs, einer speziellen Virtualisierungstechnik in Großrechnersystemen, realisiert. Die Landesbetriebe mussten weiterhin eigene Prozesse definieren, um Änderungs- und Unterstützungsdienste des SAP-Kompetenzzentrums im MdF in Anspruch zu nehmen. Alle Schritte der Migration und Separation wurden von den Projektverantwortlichen im Finanzministerium begleitet und kontrolliert; dabei wurden auch die datenschutzrechtlichen Notwendigkeiten vermittelt. Das Projekt konnte 2011 planmäßig und erfolgreich abgeschlossen werden.

Die Einführung des verteilten NFM-Betriebes in der Landesverwaltung wurde plangemäß durchgeführt. Die Verantwortlichen haben datenschutzrechtliche Erfordernisse rechtzeitig berücksichtigt und an die künftig eigenständig agierenden Landesbetriebe weitergegeben.

8.4 IT-Sicherheit im Technischen Finanzamt

Unsere Behörde hat im Technischen Finanzamt Cottbus (TFA) eine datenschutzrechtliche Kontrolle der Informationstechnik durchgeführt. Das TFA fungiert als IT-Rechenzentrum aller brandenburgischen Finanzämter und verarbeitet u. a. sensitive Steuerdaten in großen Mengen. Die Realisierung der IT-Sicherheit im TFA hat daher einen besonders hohen Stellenwert.

Schwerpunkte unserer Kontrolle waren technische und organisatorische Aspekte der Gewährleistung von Datenschutz und IT-Sicherheit im TFA, insbesondere der Status des IT-Sicherheitsmanagements sowie der Stand des IT-Sicherheitskonzepts für ausgewählte Bereiche (Passwortregelungen, Umgang mit Notebooks, Virenschutz, Notfallplan, Sicherheit der Rechenzentrumsinfrastruktur). Die Ergebnisse lassen sich wie folgt zusammenfassen:

Im TFA gibt es ein IT-Sicherheitsmanagementteam, das neben Administratoren, dem Sicherheits- und dem Datenschutzbeauftragten auch Personen aus der Leitungsebene umfasst. Wesentliche Schwerpunkte der Tätigkeit des Sicherheitsmanagementteams sind die Aufstellung und Umsetzung eines Arbeitsplans zur Gewährleistung von Datenschutz und IT-Sicherheit im IT-Verbund sowie die Beratung und Realisierung von Konzepten und Lösungen zu ausgewählten technischen und organisatorischen Sicherheitsfragen. Zu begrüßen ist, dass Aspekte der IT-Sicherheit bei Projekten zur Entwicklung und Einführung von DV-Verfahren im TFA bereits frühzeitig als fester Bestandteil der Projekttätigkeit integriert werden. Weiterhin hat das Team die IT-Sicherheitsrichtlinie und eine Reihe von instruktiven Sicherheitsmerkblättern für Benutzer erstellt, die übergeordnete Sicherheitsziele und -strategien sowie praktisch anwendbare Methoden zur IT-Sicherheit festlegen. In der IT-Sicherheitsrichtlinie fehlte jedoch der Hinweis auf die Verantwortungsübernahme der Führungsebene für die Informationssicherheit, die nach dem BSI-Standard 100-1 zu den Pflichten des leitenden Managements gehört. Das TFA hat zugesagt, diese Festlegung in seiner IT-Sicherheitsrichtlinie zu ergänzen.

Die IT-Sicherheit bei den Passwortregelungen für Systempasswörter und bei dem Umgang mit Notebooks war gut, bei der IT-Rechenzentrumsinfrastruktur sehr gut. Bezüglich der Passwörter haben wir empfohlen, Komplexitätsregelungen einzuführen und die Passworthistorie zu erweitern. Das TFA hat unsere Empfehlungen aufgenommen und entsprechende Festlegungen getroffen. Für die mobilen Endgeräte haben wir angeregt, ein Quarantänenetz einzurichten, um auf den Notebooks vor Zugang zum internen LAN Sicherheitsupdates zu laden und zu installieren. Das TFA beschäftigt sich auch hier aktiv mit der Umsetzung dieser komplexen Aufgabe.

Für die IT-Infrastruktur des TFA wurde mit der Erstellung eines Sicherheitskonzeptes nach den BSI-Standards 100-2 und 100-3 bereits im Jahr 2006 begonnen. Es besteht allerdings Überarbeitungsbedarf. Auch sind noch nicht alle relevanten Bausteine des BSI-Grundschutzkataloges erfasst worden. Darüber hinaus ist der Umsetzungsstatus bei vielen der modellierten Sicherheitsmaßnahmen noch nicht dokumentiert. Das TFA erklärte die Schwierigkeiten bei der Aktualisierung des Sicherheitskonzeptes mit der hohen Arbeitsbelastung der Administratoren aufgrund vordringlicher Projekte. Wir regten deshalb an, zu prüfen, in welchem Umfang eine externe Firma mit der Erstellung ausgewählter Teile des Sicherheitskonzepts und insbesondere mit der Grundschutzerhebung (Interview-Phase) beauftragt werden kann. Für die Umsetzung und Pflege der Maßnahmen sollte geprüft werden, wie die dafür notwendigen Prozesse dauerhaft in die Arbeitsabläufe im TFA integriert werden können. Das IT-Sicherheitsmanagement wird für eine externe Vergabe geeignete Bausteine ermitteln und die erforderlichen Schritte einleiten.

Bezüglich der dauerhaften Integration der Pflege des Sicherheitskonzeptes in die Geschäftsprozesse konnte das TFA allerdings noch keine befriedigende Antwort geben. Es bleiben daher unsererseits Zweifel, wie die gewaltige Aufgabe der Ersterstellung und Umsetzung eines ganzheitlichen Sicherheitskonzeptes durch das TFA bewältigt werden kann. Wir werden den Fortgang des Sicherheitsprozesses weiter kritisch begleiten.

Das Technische Finanzamt verfügt über ein kompetentes IT-Sicherheitsmanagement. Die faktische IT-Sicherheit befindet sich auf einem hohen Niveau. Die Erstellung eines umfassenden Sicherheitskonzeptes als Dokumentations- und Planungsinstrument des IT-Sicherheitsprozesses steht noch aus.

9 Gesundheit

9.1 Öffentlicher Gesundheitsdienst

9.1.1 Sozialpsychiatrischer Dienst und Betreuung aus einer Hand?

Nachdem die Betreuungsbehörde und der sozialpsychiatrische Dienst im Gesundheitsamt eines Landkreises als eine Organisationseinheit zusammengefasst wurden, führten wir vor Ort eine Kontrolle durch. Uns interessierte insbesondere, ob die Anforderungen an den Datenschutz trotz der personellen und organisatorischen Zusammenführung gewährleistet waren.

Bereits im Vorfeld der Zusammenführung beider Fachbereiche hatten wir uns dem Landkreis gegenüber kritisch zu dem Vorhaben geäußert und auf die datenschutzrechtlichen Anforderungen aufmerksam gemacht. Insbesondere empfahlen wir eine Trennung der Funktionen der jeweiligen Mitarbeiter.

Dies setzte die Behörde zwar grundsätzlich um, indem sie dem jeweiligen Fachgebiet einzelne Beschäftigte zuordnete und auch deren Vertreter lediglich aus demselben Fachgebiet bestellte. In Ausnahmefällen bat der sozialpsychiatrische Dienst aber Kollegen der Betreuungsbehörde, ihn zu einem als kritisch eingeschätzten Außentermin zu begleiten. Dieses Vorgehen kann zwar ausnahmsweise zulässig sein, doch sind dabei spezielle Anforderungen an die Trennung von Person und Funktion zu beachten: Der sozialpsychiatrische Dienst unterliegt den Datenschutzbestimmungen des § 55 Abs. 4 Brandenburgisches Psychisch-Kranken-Gesetz (BbgPsychKG). Alle bei diesem Dienst beschäftigten oder von ihm beauftragten Personen dürfen danach fremde Geheimnisse und personenbezogene Daten, die ihnen im Rahmen

ihrer Tätigkeit anvertraut oder sonst bekannt geworden sind, nicht unbefugt offenbaren. Lässt sich der sozialpsychiatrische Dienst bei einem Außentermin durch einen Mitarbeiter der Betreuungsbehörde begleiten, findet eine solche unbefugte Offenbarung aber statt. Deshalb ist es erforderlich, die Kollegen förmlich zu beauftragen und auf ihre spezielle Schweigepflicht hinzuweisen. Sie dürfen nicht als Mitarbeiter der Betreuungsbehörde auftreten und die ihnen bekannt werdenden Informationen nicht in dieser Funktion verwenden.

Es kam vor, dass der sozialpsychiatrische Dienst während des Außentermins einen Betreuungsbedarf feststellte und sogleich dem Betroffenen anbot, alle Angaben zu notieren, um beim Amtsgericht die Einrichtung einer Betreuung anzuregen. Der Betroffene wurde auch über das in einem solchen Fall durchzuführende Verfahren informiert. Dieses Vorgehen genügt den datenschutzrechtlichen Anforderungen nach unserer Auffassung nicht. Nach § 56 Abs. 3 Nr. 1 BbgPsychKG darf der sozialpsychiatrische Dienst personenbezogene Daten nur mit Einwilligung des Betroffenen übermitteln. Das Erheben von Daten für die Anregung einer Betreuung setzt nach § 55 Abs. 1 BbgPsychKG ebenfalls die Einwilligungserklärung des Betroffenen voraus. Das Erfordernis eines ausdrücklichen Einverständnisses des Betroffenen wird durch das bloße Angebot, die Angaben zu notieren, nicht erfüllt.

Sowohl der sozialpsychiatrische Dienst als auch die Betreuungsbehörde verfügen über eigene Dienstzimmer mit verschließbaren Schränken. Sie bewahren darin ihre jeweiligen Akten auf. Auch die elektronische Aktenführung mit Hilfe einer jeweils eigenen Software spiegelt die Trennung beider Fachgebiete wider. Allerdings besteht für die Mitarbeiter die Möglichkeit, auf die Akten und Dateien aller Kollegen ihres jeweiligen Fachgebiets zuzugreifen. Dies hielten wir für zu weit gehend. Der Zugriff auf die Akten der Kollegen innerhalb des eigenen Sachgebiets ist ausschließlich in Vertretungsfällen erforderlich. Wir haben deshalb empfohlen, die Zugriffsrechte restriktiv zu vergeben und die Zugriffe zu protokollieren.

Bei der Zusammenlegung des sozialpsychiatrischen Dienstes mit der Betreuungsbehörde können zwar organisatorische und personelle Synergieeffekte genutzt werden. Es ist aber darauf zu achten, beide Aufgaben weiterhin ausreichend eigenständig zu erfüllen und so die datenschutzrechtlich gebotene Trennung der Funktionen zu wahren.

9.1.2 Fragebogen für die amtsärztliche Untersuchung

Eine öffentliche Stelle ließ künftige Mitarbeiter vor der Einstellung amtsärztlich untersuchen. In einem Fragebogen zur Vorbereitung dieser Untersuchung sollten die Bewerber regelmäßig umfangreiche Angaben zu ihrem Gesundheitszustand und zur gesundheitlichen Vorgeschichte ma-

chen sowie sich mit einer weit reichenden Übermittlung dieser Daten einverstanden erklären. Wir wurden gebeten, dieses Formular zu beurteilen.

Wir wiesen zunächst darauf hin, dass die regelmäßige gesundheitliche Begutachtung durch das Gesundheitsamt ohnehin nur für Beamte zulässig ist. Nach § 18 i. V. m. § 43 Landesbeamtengesetz ist die gesundheitliche Eignung für die Berufung in ein Beamtenverhältnis aufgrund eines ärztlichen Gutachtens festzustellen. Beschäftigte (Angestellte) müssen nach § 3 Abs. 4 des Tarifvertrags für den öffentlichen Dienst hingegen nur bei begründeter Veranlassung eine ärztliche Bescheinigung als Nachweis für die Leistungsfähigkeit beibringen. Die regelmäßige Verwendung des auf den gesundheitlichen Gesamtzustand abzielenden Fragebogens kam somit ausschließlich für die Feststellung der Dienstfähigkeit von Beamten in Frage. Das Gesundheitsamt sagte zu, diese Einschränkung künftig zu beachten.

Der Fragebogen sah unter anderem die pauschale Entbindung der behandelnden Ärzte und des Amtsarztes von der Schweigepflicht vor. Für einen Betroffenen, der mehrere behandelnde Ärzte angibt, wäre nicht erkennbar gewesen, von welchem der Amtsarzt welche Befunde anfordern würde. Darüber hinaus ergibt sich die Notwendigkeit, solche Befunde einzuholen, ohnehin erst nach der Untersuchung des Betroffenen. Dieser kann erst dann entscheiden, in welche konkreten Datenerhebungen er einwilligt, ob er selbst Unterlagen beibringen oder die Mitwirkung verweigern möchte. Der Fragebogen sah zudem vor, dass der Betroffene in eine Übermittlung des vollständigen Gutachtens an den Dienstherrn einwilligt. Dies ist für dessen Entscheidung über die Verbeamtung allerdings nicht erforderlich. Es genügt, ihm das Ergebnis mitzuteilen. Mit der Streichung der zu pauschalen Erklärung war das Gesundheitsamt sofort einverstanden.

Die vorgesehenen Fragen zum Gesundheitszustand reichten weit in die Vergangenheit. Angaben zu körperlichen Erkrankungen, Unfällen, Operationen usw. sollten sich jedoch auf die letzten fünf (allenfalls zehn) Jahre beschränken. Für bestimmte Berufsgruppen, wie Erzieher, kann es allerdings erforderlich sein, dass auch Kinderkrankheiten erfragt werden. Da das Formular eine Vielzahl von Fällen abdecken soll, war es erforderlich, den Betroffenen ein ausdrückliches Recht einzuräumen, den Fragebogen unvollständig oder gar nicht auszufüllen. Datenerhebungen können dann im Bedarfsfall immer noch im persönlichen Gespräch zwischen Amtsarzt und Bewerber erhoben werden. Das Gesundheitsamt erklärte sich bereit, einen entsprechenden Hinweis bis zur Erarbeitung eines neuen Formulars in das Anschreiben an den Bewerber aufzunehmen.

Ein Fragebogen zur amtsärztlichen Untersuchung muss für den Betroffenen die Entscheidung ermöglichen, bestimmte Auskünfte über seinen Gesundheitszustand erst im Gespräch mit dem Amtsarzt zu geben. Pauschale und weitgehende Einwilligungserklärungen zur Datenübermittlung zwischen behandelnden Ärzten, Amtsarzt und dem potenziellen Dienstherrn sind unzulässig.

9.1.3 Eigenmächtiges Ergänzen des Fragebogens zur Einschulungsuntersuchung

Pünktlich zu den Einschulungsuntersuchungen erhielten wir wieder eine Beschwerde über die dabei verwendeten Formulare. Es zeigte sich, dass der betroffene Landkreis den durch eine Verordnung landeseinheitlich vorgegebenen Fragebogen verändert und erweitert hatte: Den Hinweis auf die Freiwilligkeit hatte der Landkreis gestrichen, jedoch wurden zusätzlich Angaben zur Krankenkasse des Kindes und zum behandelnden Kinderarzt erhoben.

Der Landkreis erklärte dazu, der Hinweis auf die Freiwilligkeit sei versehentlich entfallen. Die Angabe zur Krankenkasse des Kindes sei im Hinblick auf Impfungen und entsprechende Meldungen an das zuständige Landesamt wichtig. Der behandelnde Kinderarzt werde erfragt, damit bei notwendigem Behandlungs- und Beobachtungsbedarf eine Überweisung an diesen erfolgen kann.

Wir wiesen den Landkreis darauf hin, dass er die Vorgaben der Verordnung nicht eigenmächtig ändern darf. Unserer Auffassung nach waren die Ergänzungen im Rahmen der Einschulungsuntersuchung auch nicht erforderlich.

§ 6 Abs. 2 Brandenburgisches Gesundheitsdienstgesetz (BbgGDG) erlegt es zwar den Gesundheitsämtern auf, bei der Schuleingangsuntersuchung den Impfstatus der Kinder zu überprüfen und nach Zustimmung der Sorgeberechtigten zu ergänzen, jedoch sind die Betroffenen nicht verpflichtet, ein Impfdokument vorzulegen. Die Schulfähigkeit hängt nicht am Impfstatus. Es besteht keine Impfpflicht und dementsprechend müssen selbst gänzlich ungeimpfte Kinder ihrer Schulpflicht nachkommen.

Nehmen die Sorgeberechtigten das Angebot des Gesundheitsamtes an, den Impfstatus zu verbessern, so ist die Impfung mit den erforderlichen Daten gesondert zu dokumentieren. Dies ist auch im Hinblick auf die Abrechnung mit der zuständigen Krankenkasse erforderlich. Krankenkassen dürfen im Falle eines konkreten Überprüfungsbedarfs nur in diese Dokumentation, nicht aber in die Einschulungsunterlagen Einsicht erhalten.

Auch die Anschrift des behandelnden Arztes müssen Sorgeberechtigte dem Kinder- und Jugendgesundheitsdienst nicht offenbaren. Im Regelfall genügt es, den Betroffenen ein Dokument mit Hinweisen auf festgestellte gesundheitliche Probleme des Kindes mitzugeben. Die Familien können dann einen Arzt ihrer Wahl aufsuchen und entscheiden, ob durch diesen eine Rückmeldung an das Gesundheitsamt erfolgen soll.

Landkreise dürfen den vom Land vorgegebenen Umfang der Datenerhebung im Rahmen der Einschulungsuntersuchungen nicht eigenmächtig erweitern.

9.1.4 Herausgabe betriebsärztlicher Unterlagen an den neuen Betriebsarzt

Ein Landkreis hatte ein Unternehmen mit der Wahrnehmung betriebsärztlicher Aufgaben nach dem Arbeitssicherheitsgesetz beauftragt. Nachdem der hierfür eingesetzte Arzt sein Arbeitsverhältnis mit diesem Unternehmen beendet hatte, kündigte der Landkreis den Vertrag und forderte die Herausgabe der betriebsärztlichen Unterlagen. Das Unternehmen verweigerte diese, obwohl sein ehemaliger Mitarbeiter vom Landkreis inzwischen als Betriebsarzt eingestellt worden war.

Für Betriebsärzte gilt die ärztliche Schweigepflicht des § 203 Strafgesetzbuch (StGB) – auch im Verhältnis zum Arbeitgeber bzw. Dienstherrn. Ein Beschäftigter hat jedoch – anders als beim normalen Arzt-Patienten-Verhältnis – keine freie Arztwahl. Für bestimmte Untersuchungen ist ausschließlich der Betriebsarzt zuständig. Bei einer Weitergabe von Akten an dessen Nachfolger steht die Funktion „Betriebsarzt“ und nicht das besondere Vertrauensverhältnis zwischen Arzt und Patient im Vordergrund. § 203 StGB steht deshalb einer Aktenübergabe an den nachfolgenden Betriebsarzt regelmäßig nicht entgegen; datenschutzrechtlich ist die Übergabe grundsätzlich für die weitere Aufgabenerfüllung erforderlich. Sind der bisherige Betriebsarzt und der neue Betriebsarzt identisch, weil der Arzt lediglich seinen Arbeitgeber gewechselt hat, so ist ein Bruch der ärztlichen Schweigepflicht ohnehin nicht denkbar.

Beim Wechsel eines Betriebsarztes steht der Übergabe der patientenbezogenen Unterlagen an den Nachfolger die ärztliche Schweigepflicht regelmäßig nicht entgegen.

9.2 Krankenhäuser

9.2.1 Zulässigkeit eines externen Schreibdienstes für ein Krankenhaus

Ein Klinikum wollte einen externen Dienstleister mit dem Schreiben von ärztlichen Diktaten beauftragen. Patienten sollten dazu unter der Überschrift „Einverständniserklärung in Datenverarbeitung und Datenübermittlung“ folgenden Text abzeichnen: „Hiermit wird zu meiner Kenntnis darauf hingewiesen, dass die medizinischen Diktate auch von einem externen Dienstleister im Auftrag des Klinikums geschrieben werden.“ Das Krankenhaus bat uns zu seinem Vorhaben um Stellungnahme.

Patientendaten unterliegen der ärztlichen Schweigepflicht (§ 203 Abs. 1 Nr. 1, Abs. 3 Strafgesetzbuch – StGB). Werden solche Daten im Auftrag verarbeitet, so sind technische und organisatorische Maßnahmen zu treffen, die eine Wahrung der Geheimnisse sicherstellen (§ 11 Abs. 2 Satz 3 Brandenburgisches Datenschutzgesetz). Dies ist jedoch nicht möglich, da die Kenntnis der Daten Voraussetzung für die Arbeit des externen Schreibdienstes ist. Hinzu kommt, dass der externe Schreibdienst anders als ein internes Sekretariat nicht der ärztlichen Schweigepflicht unterliegt. Zu demselben Ergebnis kommt man bei Anwendung des Bundesdatenschutzgesetzes für private Kliniken.

Den uns vorgelegten Dokumenten war zu entnehmen, dass sich die Klinik für eine Durchbrechung der ärztlichen Schweigepflicht auf eine Einwilligungserklärung der Betroffenen stützen wollte. Die konkrete Formulierung ließ dies jedoch nicht erkennen. Sie zeigte vielmehr, dass es Betroffenen nicht freigestellt sein sollte, sich für oder gegen den Einsatz des externen Schreibdienstes zu entscheiden. Weder wurde der Patient über seine Rechte aufgeklärt, noch blieb ihm die Entscheidung über das Einbeziehen des privaten Schreibdienstes überlassen.

Mit der Freiwilligkeit einer Einwilligungserklärung lässt es sich auch nicht vereinbaren, die Behandlung eines Patienten wegen seiner Weigerung, eine Einwilligungserklärung in die externe Datenverarbeitung zu erteilen, abzulehnen. Es müsste daher jederzeit gewährleistet sein, die Schreibarbeiten durch Klinikmitarbeiter erledigen zu lassen. Eine Einwilligungslösung erschien uns daher nicht praktikabel.

Der vorgesehene Vertrag mit dem Dienstleister sah darüber hinaus vor, dass Patientendaten von diesem nur fünf Jahre nach Vertragsende geheim gehalten werden. § 203 Abs. 3 letzter Satz und Abs. 4 StGB legt demgegenüber fest, dass die Schweigepflicht auch über den Tod des Patienten oder des

Schweigepflichtigen hinaus grundsätzlich unbegrenzt gelten soll. Vertraglich kann diese gesetzliche Vorgabe nicht geändert werden.

Unsere dringende Empfehlung lautete, von der geplanten Datenverarbeitung im Auftrag Abstand zu nehmen.

Die Beauftragung eines externen Schreibdienstes mit der Verarbeitung von Patientendaten stellt einen Verstoß gegen die ärztliche Schweigepflicht dar und ist unzulässig.

9.2.2 Patientenarmbänder mit RFID-Chip für Demenzkranke

Ein Klinikum für Psychiatrie und Neurologie beabsichtigte, einen Neubau speziell für Demenzkranke zu errichten, ohne dabei zu unterscheiden, ob sich diese mit oder ohne Unterbringungsbeschluss im Krankenhaus aufhalten. Die Patienten sollten Armbänder mit einem RFID-Chip erhalten, der eine Zuordnung zum konkreten Träger ermöglicht. Eine Ortung im Gebäude oder auf dem Klinikgelände war nicht vorgesehen. Geplant war jedoch die Alarmierung des Pflegepersonals, wenn ein Patient die Einrichtung ohne Begleitung verlässt. Wir wurden zu dem Vorhaben um eine datenschutzrechtliche Beurteilung gebeten.

Unserer Bewertung lagen folgende Fallkonstellationen zugrunde: die öffentlich-rechtliche Unterbringung nach dem Brandenburgischen Psychisch-Kranken-Gesetz (BbgPsychKG), die zivilrechtliche Unterbringung nach § 1906 Bürgerliches Gesetzbuch und der freiwillige Aufenthalt in der Einrichtung.

- Bei der geschlossenen Unterbringung gehört das sichere Unter-Verschluss-Halten der Betroffenen zur Aufgabe der beliehenen Krankenhäuser. Nach § 55 Abs. 1 Nr. 1 BbgPsychKG dürfen diese personenbezogene Daten erheben, speichern und nutzen, soweit es zur Erfüllung ihrer Aufgaben nach dem Brandenburgischen Psychisch-Kranken-Gesetz erforderlich ist. Bevor ein zwangsweise untergebrachter Patient z. B. im Wege der Beurlaubung den geschlossenen Bereich verlassen darf, stehen bereits jetzt vielfältige Datenverarbeitungen an, bei denen die persönlichen Verhältnisse, der Gesundheitszustand und der Behandlungsplan zu betrachten sind. Ein Mehr an Datenverarbeitungen erfolgt durch die Nutzung des Armbands nicht. Diese ist für die geschlossene Unterbringung daher zulässig.

  Müssen sich Patienten im offenen oder gelockerten Vollzug vor Verlassen der Klinik abmelden, findet bei dem vorgeschlagenen RFID-Einsatz ebenfalls keine zusätzliche Datenverarbeitung statt. Die Armband-

Lösung kann auch in diesem Fall als erforderlich nach § 55 Abs. 1 Nr. 1 BbgPsychKG angesehen werden. Um im Fall einer offenen Unterbringung ein Kommen und Gehen des Betroffenen auch ohne Kenntnis der Einrichtung zu ermöglichen, müsste sowohl die Nutzung des Armbandes als auch die zusätzliche Datenverarbeitung durch eine Einwilligung des Betroffenen oder seines Betreuers nach § 55 Abs. 1 Nr. 3 BbgPsychKG legitimiert werden. Freiwillig wäre eine solche Erklärung nur dann, wenn eine alternative Verfahrensweise ohne die zusätzliche Datenverarbeitung angeboten würde.

- Die zwangsweise zivilrechtliche Unterbringung muss zum Wohle des Betreuten erfolgen. Der Betreuer schließt dazu einen Unterbringungsvertrag mit der Einrichtung. Eine Unterbringung mit freiheitsentziehendem Charakter bedarf außerdem der Genehmigung des Betreuungsgerichts.

  Datenerhebungen und -verwendungen, die zur Durchführung des Behandlungs- bzw. Unterbringungsvertrages nach § 28 Abs. 1 Nr. 1 Brandenburgisches Krankenhausentwicklungsgesetz bzw. § 28 Abs. 1 Bundesdatenschutzgesetz erforderlich sind, sind zulässig. Die Datenverarbeitung darf nicht umfassender ausfallen als bei der herkömmlichen geschlossenen Unterbringung. Außerdem muss der Zweck des sicheren Unter-Verschluss-Haltens hinreichend gewahrt sein.

  Bei einer offenen zivilrechtlichen Unterbringung ist für Funkortungschips in einem Armband die Zustimmung durch den Betroffenen bzw. seinen Betreuer zu fordern. Auch die damit verbundene Datenverarbeitung ist wiederum einwilligungsbedürftig. Freiwillig ist eine solche Erklärung nur dann, wenn eine Alternative ohne die zusätzliche Datenverarbeitung angeboten wird.

- Für diejenigen, die sich freiwillig in der Einrichtung befinden, bringt die geplante Ausgestaltung mehr Einschränkungen ihrer Bewegungsfreiheit, aber auch ihres Grundrechtes auf Datenschutz mit sich. Es ist eine Einwilligung in die Nutzung des Armbandes und die damit verbundene Datenverarbeitung zu fordern. Freiwillig ist eine solche Erklärung nur dann, wenn eine Alternative ohne die zusätzliche Datenverarbeitung angeboten wird.

Außer in den Fällen der zwangsweisen geschlossenen Unterbringung ist regelmäßig eine Einwilligung des Betroffenen oder seines Betreuers in die Verwendung eines Armbands mit Ortungsfunktion erforderlich. Die Freiwilligkeit dieser Erklärung setzt voraus, dass dem Patienten eine Alternative angeboten wird.

9.2.3 Krankenhausinformationssysteme – Orientierung für Kliniken und Hersteller

Krankenhäuser setzen spezielle Software ein, um die Daten ihrer Patienten zu verwalten. Im Rahmen solcher Krankenhausinformationssysteme haben teilweise zahlreiche Beschäftigte einen nahezu unbeschränkten Zugriff auf sensitive Gesundheitsdaten.

Krankenhausinformationssysteme sind unverzichtbare Hilfsmittel bei der ärztlichen Behandlung in Krankenhäusern. Die gespeicherten Patientendaten sind jederzeit schnell abrufbar und bilden eine wesentliche Grundlage für eine effektive Behandlung. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Bei Kontrollbesuchen in zurückliegenden Jahren mussten wir u. a. feststellen, dass der Zugriff von Krankenhausbeschäftigten auf sensitive Patientendaten nicht restriktiv genug gestaltet wurde, dass die Administratoren zu viele Rechte besaßen und dass die Passwortgestaltung nicht datenschutzgerecht erfolgte.

Für die Gewährleistung der Vertraulichkeit bei der Verarbeitung von Patientendaten sind die Krankenhäuser zunächst selbst verantwortlich. Sie dürfen den Zugriff auf solche sensitiven Daten nur erlauben, wenn die rechtlichen Befugnisse vorliegen. Das bedeutet unter anderem, dass nur solche Beschäftigten auf die Daten zugreifen dürfen, für deren Arbeit dies erforderlich ist. Außerdem ist zu gewährleisten, dass die Patienten nachvollziehen können, wer zu welchem Zeitpunkt auf ihre Daten zugegriffen hat. Eine revisionssichere Protokollierung muss sicherstellen, dass jederzeit – auch nachträglich – überprüft werden kann, ob die Zugriffe zulässig waren.

Eine Expertengruppe von Datenschutzbeauftragten des Bundes und der Länder sowie der Evangelischen Kirche in Deutschland und der Katholischen Kirche hat unter Beteiligung von Software-Herstellern und Kliniken eine Orientierungshilfe Krankenhausinformationssysteme[29] herausgegeben. Diese konkretisiert die Anforderungen des Datenschutzes und der ärztlichen Schweigepflicht an den Einsatz von Informationssystemen in den Krankenhäusern und beschreibt technische und organisatorische Maßnahmen zu deren Umsetzung.

Die vorliegende Orientierungshilfe wird unserer Behörde im Rahmen künftiger Kontroll- und Beratungstätigkeiten als Grundlage dienen. Dabei berücksichtigen wir jedoch, dass die im Einsatz befindlichen Krankenhausinformationssysteme die erforderlichen technischen und organisatorischen Maßnahmen

[29] siehe http://www.lda.brandenburg.de

derzeit noch nicht in vollem Umfang umsetzen und akzeptieren eine angemessene Übergangszeit.

Die Orientierungshilfe richtet sich sowohl an die Hersteller von Krankenhausinformationssystemen als auch an die Betreiber und fordert sie auf, entsprechende Produkte datenschutzgerecht zu gestalten bzw. einzusetzen.

9.3 Arztpraxen

9.3.1 Durchbrechung der ärztlichen Schweigepflicht bei Fälschung von Rezepten durch Patienten

Ein Patient manipulierte eine Medikamentenverordnung. Die Apotheken schöpften Verdacht und lehnten nach Rücksprache mit dem verordnenden Arzt die Medikamentenausgabe ab. Daraufhin wechselte der Betrüger die Taktik und brachte gefälschte Telefaxe in Umlauf, in denen der verordnende Arzt scheinbar darum bat, ein bestimmtes Medikament auszuhändigen und zusagte, das Rezept nachzureichen. Der Arzt wollte sich vor einer Strafanzeige gegen den Patienten bei uns vergewissern, ob er sich damit selbst wegen eines unbefugten Bruchs der ärztlichen Schweigepflicht nach § 203 Strafgesetzbuch (StGB) strafbar machen könnte.

Der Arzt erfuhr von den Betrugsversuchen nicht durch den Patienten, sondern durch die Apotheken, die sich bei ihm rückversichern wollten. Somit wurde ihm ein Geheimnis des Patienten wegen des Arzt-Patienten-Verhältnisses von dritter Seite bekannt. Die Information fällt daher auch unter die ärztliche Schweigepflicht.

Selbst wenn der Mediziner von seinem Patienten selbst über die Manipulation von Rezepten erfährt, dürfte eine Güterabwägung zum Ergebnis kommen, dass das Interesse des Arztes an einer Durchbrechung der ärztlichen Schweigepflicht überwiegt. Das Verhalten des Patienten richtet sich nicht nur gegen die Interessen des Arztes und der Versichertengemeinschaft, sondern auch gegen das Vertrauensverhältnis zwischen dem Arzt und dem Patienten. Hinzu kommt, dass eine gesundheitliche Gefährdung des Patienten oder ggf. auch anderer Personen durch die Verwendung des nicht verordneten Medikaments angenommen werden muss. Dass ein – im Vergleich zu einer Strafanzeige weniger eingriffsintensives – Gespräch des Arztes mit seinem Patienten diesen von weiteren Manipulationsversuchen abhalten könnte, ist angesichts der hartnäckigen und wiederholten Betrugsversuche in der Vergangenheit nicht zu erwarten.

Fälscht ein Patient Aufzeichnungen des Arztes und setzt er diese wiederholt für einen Rezeptbetrug ein, so kann der Arzt zu einem Bruch seiner Schweigepflicht durch Stellen einer Strafanzeige berechtigt sein.

9.3.2 Krankenakten im Flur einer Arztpraxis

Ein Patient beschwerte sich darüber, dass im Flur einer Hausarztpraxis Patientenakten für die Ärzte in Prospektständern bereitgelegt wurden.

Das unbeaufsichtigte Aufbewahren von Patientenakten im Flur ist sowohl im Hinblick auf die ärztliche Schweigepflicht als auch den Datenschutz unzulässig. Bereits aufgrund unserer schriftlichen Intervention unterbanden die Ärzte die Vorgehensweise und baten, ihre Betriebsblindheit zu entschuldigen. Bei einem Besuch der Räumlichkeiten durch uns legte das Praxisteam großen Wert darauf zu zeigen, dass Patientenakten und -daten gesichert verarbeitet würden. Allerdings mussten wir feststellen, dass die Sicherung der Räumlichkeiten insgesamt Mängel aufwies. Auch fehlte ein Gerät für die datenschutzgerechte Vernichtung von Unterlagen.

Nach der Übernahme der Aufsicht über nicht-öffentliche Stellen Mitte 2010 zeigten bereits die ersten Kontakte mit Arztpraxen, dass dort zugunsten praktischer Lösungen die Beachtung der ärztlichen Schweigepflicht manchmal in den Hintergrund rückt. Eine Bereitschaft, hier Korrekturen vorzunehmen, war jedoch festzustellen.

Für generelle Fragen des Datenschutzes wie die Sicherung der Räumlichkeiten oder datenschutzgerechtes Löschen von Patientendaten scheint eine Sensibilisierung in vielen Arztpraxen erst noch erforderlich.

9.3.3 3, 2, 1, meins – ein Archiv für Röntgenbilder bei eBay

Das komplette Archivsystem für Röntgenbilder einer brandenburgischen Arztpraxis gelangte als Angebot auf die Internetplattform des Auktionshauses eBay. Wer wollte, konnte die Hängemappen einschließlich Namen und Geburtsdaten der durchleuchteten Patienten ersteigern.

Aufmerksam wurden wir auf das Angebot durch den Hinweis eines eBay-Nutzers. Es war offensichtlich, dass der Verkauf des Archivsystems zu einer unbefugten Offenbarung von Patientendaten geführt hätte. Das Auktionshaus entfernte das Angebot umgehend, nachdem wir auf die Vertraulichkeit der Angaben aufmerksam gemacht hatten. Auf unsere Nachfrage teilte der Inhaber der Praxis, aus der das Archivsystem stammte, mit, er sei von einer ordnungsgemäßen Entsorgung ausgegangen. Das Angebot habe ein Mitar-

beiter ohne Wissen des Inhabers eingestellt. Der Mitarbeiter sei deswegen abgemahnt und die Hängemappen seien entsorgt worden.

Auf eine erneute Nachfrage teilte die Arztpraxis mit, dass die Mappen mit den Patientendaten durch den praxiseigenen Aktenvernichter mit der Sicherheitsstufe 2 der DIN 32757 zum Vernichten von Informationsträgern entsorgt worden seien. Dies stellt jedoch keine datenschutzgerechte Löschung von Patientendaten dar. Angesichts des besonderen Schutzbedarfs für personenbezogene Daten dieser Art ist eine höhere Sicherheitsstufe erforderlich. Wir haben deshalb empfohlen, patientenbezogene Unterlagen künftig nur noch nach der Sicherheitsstufe 4 der genannten Norm zu vernichten.

Auch ohne die eigentlichen Röntgenbilder enthalten entsprechend beschriftete Hängemappen schutzbedürftige Patientendaten und sind unter Einhaltung der Sicherheitsvorschriften für die Vernichtung von Informationsträgern zu entsorgen.

9.3.4 Anbindung von Praxis-EDV-Systemen an medizinische Netze

Seit Januar 2011 müssen die an der vertragsärztlichen Versorgung teilnehmenden Ärzte die Abrechnungsdaten leitungsgebunden an ihre Kassenärztliche Vereinigung übersenden. Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen bieten hierfür eine Netzinfrastruktur an, die eine sichere Übertragung von medizinischen Daten ermöglicht.

Die Anbindung von Praxis-EDV-Systemen an medizinische Netze erfordert die Realisierung von technischen und organisatorischen Maßnahmen, die geeignet sind, die der ärztlichen Schweigepflicht gem. § 203 Strafgesetzbuch unterliegenden Daten wirksam vor Missbrauch zu schützen.

In einer Entschließung[30] forderten die Datenschutzbeauftragten des Bundes und der Länder deshalb u. a.:

- Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

- Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

[30] siehe Anlage 1.3.4: Entschließung „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ vom 16./17. März 2011

- Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

- Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

- Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

- Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

- Grundstandards - wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Werden für die verwendeten Verschlüsselungs- und Authentisierungskomponenten Softwarelösungen eingesetzt, so dürfen aus Sicherheitsgründen die genutzten Rechner nicht mit dem internen Netz der Praxis verbunden sein.

Bei der Verarbeitung von medizinischen Daten sind hohe Anforderungen hinsichtlich der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit zu stellen. Es sind technische und organisatorische Maßnahmen zu ergreifen, die einen Missbrauch von medizinischen Daten zuverlässig verhindern.

9.4 Krankenkassen

9.4.1 Arztnavigator – Ärztebewertung im Internet

Das von der Bertelsmann Stiftung betriebene Internetportal „Weiße Liste“ hat zum Ziel, die Suche nach einem Krankenhaus, Arzt oder Pflegeheim zu erleichtern. Es bietet Versicherten neuerdings auch die Möglichkeit, Ärzte zu bewerten. Um u. a. Manipulationen und unzulässige Mehrfachbeurteilungen zu vermeiden, setzt die Bewertung eine Registrierung der Versicherten voraus. Für diese sind die an dem Bewertungsportal beteiligten Krankenkassen verantwortlich. Geprüft haben wir die dafür erforderliche Datenverarbeitung durch die AOK Berlin-Brandenburg (jetzt AOK Nordost).

Die AOK ist für die Registrierung und Erstauthentisierung der Nutzer verantwortlich. Um eine Bewertung abzugeben, müssen diese sich zunächst anhand ihrer Krankenversicherungsnummer anmelden und sich einen Benutzernamen und ein Kennwort geben. Während der AOK-Bundesverband

davon ausgeht, dass es sich bei der Krankenversicherungsnummer nicht um ein personenbezogenes Sozialdatum handelt, vertreten wir hierzu eine andere Auffassung. Ihre Verwendung zu Zwecken der Registrierung bedarf demnach einer Rechtsgrundlage. Die von der AOK angeführte Bestimmung des § 305 Abs. 3 Fünftes Buch Sozialgesetzbuch ist aus unserer Sicht keine ausreichende Rechtsgrundlage. Sie betrifft ausschließlich allgemeine Information über zugelassene Leistungserbringer und berechtigt nicht zu der hier stattfindenden Datenverarbeitung. Damit kommt nur eine Einwilligungslösung in Betracht.

Das Bewertungsportal wird von den beteiligten Krankenkassen über eigene Webseiten zugänglich gemacht. Die AOK bietet es unter der Bezeichnung „AOK Arztnavigator“[31] an. Ihre Seite erweckt den Eindruck, man befinde sich auf einem Angebot der AOK. Erst ein unscheinbarer Verweis auf die „Weiße Liste“ sowie die Angaben im Impressum erklären, dass es sich um ein Angebot der Bertelsmann Stiftung handelt. Für die Nutzer muss aber eindeutig erkennbar sein, welche Stelle die Verantwortung für die aufgerufene Seite trägt. Dies gilt umso mehr, wenn das Angebot personenbezogene Daten verarbeitet. Eine Einwilligung der Versicherten in die Datenverarbeitung ist nur wirksam, wenn die Betroffenen hinreichend über diese informiert werden. Dies ist angesichts der fehlenden Transparenz des Bewertungsportals fraglich.

Verlässliche Portale für Arztbewertungen können für die Patienten von großer Hilfe sein, wenn auch dem Sozialdatenschutz Rechnung getragen wird. Eine Rechtsgrundlage ist hierfür ebenso unentbehrlich wie die Klarheit darüber, wer das Portal betreibt.

9.4.2 Krankenversichertenkarte nur noch mit Lichtbild

Im Rahmen der Einführung der elektronischen Gesundheitskarte fühlten sich einige Versicherte schlecht darüber informiert, ob sie verpflichtet sind, das von den Krankenkassen angeforderte Lichtbild vorzulegen. Ein Versicherter erhielt von seiner Kasse einen durchscheinenden Briefumschlag zwecks Rücksendung des Lichtbilds.

Nach § 291 Abs. 2 Fünftes Buch Sozialgesetzbuch ist die Krankenversichertenkarte mit einem Lichtbild zu versehen. Erst die Vorlage der in dieser Form vorgeschriebenen Krankenversicherungskarte berechtigt künftig zu einer ärztlichen oder zahnärztlichen Behandlung auf Kosten der Kasse. Ausnahmen gelten nur für Versicherte bis einschließlich 14 Jahren sowie für Perso-

[31] siehe http://www.aok-arztnavi.de

nen, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist, z. B. Pflegebedürftige.

Anlässlich unserer Nachfrage zur Verwendung durchscheinender Briefumschläge führte die betroffene Krankenkasse eine umfassende Prüfung durch. Sie stellte fest, dass die von ihr verwendeten Kuverts den Schutz der Sozialdaten im Falle eines gezielten Versuchs, diese zur Kenntnis zu nehmen, nicht ausreichend gewährleisten. Die Kasse sagte zu, blickdichte Umschläge zum Zweck der Rücksendung der Lichtbilder zu verschicken.

Krankenversichertenkarten berechtigen künftig in der Regel nur noch mit einem Lichtbild zur ärztlichen oder zahnärztlichen Behandlung.

9.5 Prüfung der Zentralen Stelle Mammographie

Mammographie-Screening ist ein Programm zur Früherkennung von Brustkrebs. Es gliedert sich in regionale Versorgungsprogramme. Durch einen Kooperationsvertrag zwischen den jeweiligen Arbeitsgemeinschaften Mammographie-Screening Berlin und Brandenburg wurden die Mitarbeiter in die Arbeit der jeweils anderen Zentralen Stelle eingebunden. Die Tätigkeit dieser Bürogemeinschaft haben wir kontrolliert.

Nachdem wir auf schriftlichem Wege bereits etliche datenschutzrechtliche Verbesserungen an einer internen Dienstanweisung und verschiedenen Verträgen mit Dienstleistern (z. B. zur Entsorgung von Datenträgern, zum Druck und Versand der Einladungsschreiben) erreichen konnten, bestand das Ziel der Überprüfung vor Ort vor allem darin, festzustellen, inwieweit die erforderliche Trennung zwischen den Zentralen Stellen beider Länder erfolgt.

Die Callcenter der Zentralen Stellen Berlins und Brandenburgs sind zwar in getrennten Räumen untergebracht, jedoch miteinander vernetzt. Die brandenburgischen Mitarbeiter bearbeiten die Einladungen für die Brandenburgerinnen; die für das Land Berlin zuständigen Mitarbeiter die Einladungen für die Hauptstädterinnen. Es gibt jedoch nur eine gemeinsame Hotline für die beiden Zentralen Stellen; Telefonate werden daher von allen angenommen. Dabei erfolgen die Bearbeitung des Terminkalenders der betroffenen Screening-Einheit oder notwendige Änderungen der Stammdaten der Frau sowie weitere Eintragungen, die aufgrund des Telefonats vorzunehmen sind, durch denjenigen, der den Anruf entgegennahm.

Generell für beide Stellen tätig sind die Geschäftsführerin, das Sekretariat und die behördliche Datenschutzbeauftragte. Bei allen diesen Personen ist eine Kenntnisnahme personenbezogener Daten nicht völlig auszuschließen,

ob durch die Wahrnehmung von Kontroll- oder Aufsichtsbefugnissen oder das Öffnen und Verteilen der Post.

Nach außen wurde bei gemeinsamer Hotline und gleicher Anschrift fast nur noch die Bezeichnung „Zentrale Stelle“ oder „Zentrale Stelle Mammographie“ verwendet. Die Zusammenarbeit der beiden Zentralen Stellen war für die betroffenen Frauen somit zum Zeitpunkt unseres Kontrollbesuches kaum ersichtlich.

Die Vermischung der Aufgaben zweier öffentlicher Stellen ist so nicht zulässig. Die beiden Zentralen Stellen müssen datenschutzgerecht so getrennt werden, dass von Angehörigen der Berliner Stelle keine Daten der brandenburgischen Stelle zur Kenntnis genommen werden können und umgekehrt. Alternativ könnte die Zusammenarbeit durch einen Staatsvertrag geregelt werden. Diesbezüglich haben wir uns auch an das Aufsicht führende Gesundheitsministerium gewandt.

Ein IT-Sicherheitskonzept nach den Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik liegt in der Zentralen Stelle bis heute nicht vor, obwohl wir dies von Anfang an gefordert hatten. Zur Erhöhung der Datensicherheit und zur Wahrung des Datenschutzes sind inzwischen zwar erste wesentliche Anforderungen erfüllt worden, doch müssen weitere folgen, um einen gesetzeskonformen Zustand zu erreichen.

Die Bürogemeinschaft der Zentralen Stellen Berlins und Brandenburgs wirft nach wie vor datenschutzrechtliche Probleme auf. Weder existiert eine rechtliche Grundlage für die Zusammenarbeit, noch liegt ein IT-Sicherheitskonzept vor.

10 Informationstechnik in der Landesverwaltung

10.1 IT-Strategie der Landesverwaltung – Wohin soll die Reise gehen?

Die dauerhafte Gewährleistung von IT-Sicherheit und Datenschutz kann nur im Rahmen eines kontinuierlichen, zielgerichteten und systematischen Vorgehens gelingen. Dies verlangt auch, die Grundsätze des Einsatzes der Informationstechnik mittel- und langfristig zu planen. Dabei sind – z. B. im Rahmen einer IT-Strategie – für einen Zeitraum von mehreren Jahren wesentliche Ziele und Inhalte des IT-Einsatzes sowie Wege zur Erreichung der Ziele zu formulieren.

Gemäß der IT-Standardisierungsrichtlinie des Landes Brandenburg[32] legt die IT-Strategie verbindlich den Rahmen für den weiteren Ausbau der Informationstechnik in der Landesverwaltung fest. Alle Behörden, Einrichtungen und Betriebe der Landesverwaltung planen und realisieren den IT-Einsatz in ihren jeweiligen Bereichen nach Maßgabe der in der IT-Strategie festgelegten Ziele, Leitlinien und Migrationswege. Die IT-Strategie selbst ist als Anlage 1 Bestandteil der Standardisierungsrichtlinie. Sie wird flankiert von den IT-Standards als Anlage 2, durch welche ressortübergreifend grundlegende Techniken (wie Protokolle, Schnittstellen, Datenformate und Methoden) sowie konkrete Anwendungsprogramme im Sinne der Vereinheitlichung und Gewährleistung der Kompatibilität der IT im Land festgelegt werden. Sowohl IT-Strategie als auch IT-Standards enthalten auch Regelungen zu Fragen der IT-Sicherheit und des Datenschutzes.

Während die IT-Standards nach ihrer Veröffentlichung 2004 in den Jahren 2008 und 2010 aktualisiert wurden, fehlt eine solche Fortschreibung für die IT-Strategie des Landes bislang. Auch wenn mit Ablauf des fünfjährigen Geltungszeitraums für die Ziele und Migrationswege in der IT-Strategie die dortigen Aussagen nicht ungültig werden, halten wir eine Auswertung und eine Weiterentwicklung der konzeptionellen Vorstellungen zum künftigen IT-Einsatz in der Landesverwaltung für erforderlich. Dies ist insbesondere vor dem Hintergrund der bereits begonnenen Zentralisierung und Konsolidierung der Informationstechnik, der zunehmenden Fülle und Komplexität der zu lösenden Aufgaben bei gleichzeitig sinkenden Beschäftigtenzahlen sowie dem Zwang zu erhöhter Wirtschaftlichkeit von besonderer Bedeutung. Zu beachten sind dabei auch Rahmenbedingungen auf nationaler Ebene durch die Festlegungen im IT-Planungsrat.

Auswirkungen einer fehlenden Fortschreibung der IT-Strategie des Landes könnten z. B. sein:

- der Verzicht auf notwendige Entscheidungen und das Zurückfallen hinter den Stand der Technik oder hinter den Stand anderer Bundesländer,

- das Treffen unwirtschaftlicher Ad-hoc-Entscheidungen ohne den Blick für übergreifende Ziele, die Beliebigkeit der Entwicklung und das Hinterherlaufen hinter kurzfristigen technischen Trends,

- das doppelte Entwickeln oder Beschaffen von Lösungen, da Beteiligte in unterschiedlichen Projekten von den Arbeiten anderer und der Verortung in der IT-Gesamtstrategie des Landes unzureichende Kenntnis haben,

[32] Richtlinie über die Anwendung der IT-Strategie und von IT-Standards in der Landesverwaltung Brandenburg vom 15. Juni 2004, zuletzt geändert durch Bekanntmachung am 9. November 2010

- die mangelnde Nachvollziehbarkeit und Akzeptanz für Entscheidungen zum IT-Einsatz sowie eine abnehmende Motivation der Beschäftigten im IT-Bereich.

Mittel- und langfristig könnte dies auch zu einer Verringerung des Niveaus an IT-Sicherheit und Datenschutz in der Landesverwaltung führen.

Zuständig für die Weiterentwicklung der IT-Strategie des Landes ist gemäß der E-Government- und IT-Organisationsrichtlinie[33] die E-Government- und IT-Leitstelle im Ministerium des Innern. Eine entsprechende Vorlage wäre durch den Ausschuss der IT-Beauftragten der Ressorts (RIO-Ausschuss) zu beschließen. Bereits Ende 2008 haben wir in diesem Ausschuss die Weiterentwicklung der IT-Strategie des Landes angeregt. Zwar war das Thema Mitte 2010 dort mehrfach auf der Tagesordnung, allerdings nur um eine Ideensammlung anzuregen und organisatorische Fragen abzustimmen. Inhaltliche Ergebnisse sind uns bis heute nicht bekannt.

Es ist dringend erforderlich, dass die Landesregierung ihre IT-Strategie von 2004 fortschreibt. Hierbei sind einerseits das Erreichte kritisch abzurechnen und noch offene Punkte zu identifizieren. Andererseits sind die Ziele des IT-Einsatzes in der Landesverwaltung unter Berücksichtigung des nationalen Kontextes festzulegen sowie die Wege dorthin zu bestimmen.

10.2 IT-Sicherheitsmanagement in der Landesverwaltung

Nach seiner Konstituierung im Jahr 2008 hat sich das IT-Sicherheitsmanagementteam der Landesverwaltung als Gremium auf Arbeitsebene mittlerweile fest etabliert. Es besteht aus den IT-Sicherheitsbeauftragten der Ressorts und trifft sich regelmäßig zur Diskussion, Abstimmung und Festlegung von ressortübergreifenden Sicherheitsstandards für den IT-Einsatz in der Landesverwaltung.

Als wesentliche Arbeitsschwerpunkte des IT-Sicherheitsmanagementteams der Landesverwaltung in den zurückliegenden beiden Jahren sind zu nennen:

- Erörterung von Fragen der IT-Sicherheit in ressortübergreifenden oder landesweiten DV-Verfahren wie NFM[34] (Neues Finanzmanagement), Pe-

[33] Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg vom 22. September 2009

[34] vgl. Tätigkeitsbericht 2008/2009, A 10.1

rIS[35] (Personalinformationssystem) und EL.DOK[36] (Elektronisches Dokumentenmanagement- und Vorgangsbearbeitungssystem),

- Diskussion und Beschlussfassung über landesweit einheitliche Kategorien zur Festlegung des Schutzbedarfs für DV-Verfahren in Anlehnung an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik,

- Beschlussfassung über den Aufbau eines zentralen Sicherheitsinformationssystems (SIS) für die Landesverwaltung beim Brandenburgischen IT-Dienstleister, Zusammenführung und Konsolidierung von IT-Sicherheitskonzepten im SIS unter Beachtung von Zuständigkeiten der Ressorts bzw. des Dienstleisters, Einführung eines einheitlichen zentralen Werkzeugs für das IT-Sicherheitsmanagement,

- Diskussion von IT-Sicherheitsvorfällen[37] in der Landesverwaltung, Ableitung allgemeingültiger Schlussfolgerungen, Erarbeitung von Richtlinien und Meldewegen zum Umgang mit Computer-Notfällen,

- Erörterung der Eigenschaften mobiler Endgeräte (insbesondere iPhone, Blackberry oder Windows Mobile Smartphones) zur Gewährleistung von IT-Sicherheit und Datenschutz bei ihrem Einsatz und Bewertung entsprechender Lösungen.

In der Zukunft wird sich das IT-Sicherheitsmanagementteam einerseits auf die Erstellung von landesweit einheitlichen, technischen Systemrichtlinien z. B. zum Schutz vor Viren und anderer Schadsoftware oder zur Absicherung von Netzübergängen aus dem Landesverwaltungsnetz in das Internet, zu externen, privatwirtschaftlichen Dienstleistern oder zu Netzen anderer öffentlicher Stellen konzentrieren. Andererseits sollen die Vorarbeiten zu Richtlinien, Handlungsempfehlungen, Vorgaben, Mustern usw. für die Informationssicherheitsrevision und für Sicherheitsaudits weitergeführt werden. Durch ihre Anwendung wird eine Überprüfung der Angemessenheit und Wirksamkeit von IT-Sicherheitsmaßnahmen sowie des erreichten Niveaus an IT-Sicherheit und Datenschutz in der Landesverwaltung und dessen dauerhafte Aufrechterhaltung ermöglicht.

---

35 vgl. Tätigkeitsbericht 2008/2009, A 4.6.3

36 vgl. Tätigkeitsbericht 2008/2009, A 4.5.5

37 vgl. A 10.5

Die Arbeit des IT-Sicherheitsmanagementteams ist auch künftig kontinuierlich fortzusetzen. Trotz der erreichten Ergebnisse sehen wir Raum für Verbesserungen. Insbesondere die Intensivierung der Diskussionen, das verstärkte Einbringen von Anforderungen und Lösungsvorschlägen durch die IT-Sicherheitsbeauftragten der Ressorts sowie die Beschleunigung der Entscheidungsfindung und -umsetzung sind nach unserer Ansicht geboten.

10.3 Landesverwaltungsnetz 4.0

Im Jahr 2011 wurde das Landesverwaltungsnetz in der Version 4.0 in Betrieb genommen. Damit steht im Land Brandenburg flächendeckend ein modernes Verwaltungsnetz zur Verfügung.

Das Landesverwaltungsnetz Brandenburg (LVN BB) wird gemeinsam vom Technischen Finanzamt, dem Zentraldienst der Polizei und dem Brandenburgischen IT-Dienstleister betrieben. Im Oktober 2009 informierte uns das Ministerium des Innern über die beabsichtigte Ausschreibung von Infrastrukturleistungen für das neue Landesverwaltungsnetz 4.0 und gab uns frühzeitig die Möglichkeit, unsere Forderungen aus Sicht des Datenschutzes in die Ausschreibungsunterlagen einfließen zu lassen. Der Zuschlag wurde im April 2011 erteilt.

Das neue Landesverwaltungsnetz bietet zahlreiche technische Innovationen. So steht beispielsweise eine höhere Übertragungsbandbreite zur Verfügung, das neue Internetprotokoll IPv6 wird unterstützt und die Verfügbarkeit des Netzes wurde weiter erhöht.

Im Landesverwaltungsnetz werden personenbezogene Daten übertragen. Es sind daher technische und organisatorische Maßnahmen zu realisieren, die einen Missbrauch der übertragenen Daten ausschließen. Zur Gewährleistung der Vertraulichkeit ist insbesondere eine Verschlüsselung der übertragenen Daten unabdingbar. Für personenbezogene Daten mit normalem Schutzbedarf reicht eine Leitungsverschlüsselung, bei hohem oder sehr hohem Schutzbedarf halten wir eine Ende-zu-Ende-Verschlüsselung für erforderlich. Erstere ist im LVN 4.0 als Grundschutz gewährleistet, für Letztere ist die jeweilige Daten verarbeitende Stelle bzw. der Verantwortliche des DV-Verfahrens selbst zuständig.

Ein modernes Landesverwaltungsnetz setzt die Realisierung von technischen und organisatorischen Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit voraus. Durch die frühzeitige Einbeziehung unserer Behörde konnten wir erreichen, dass grundlegende Forderungen wie beispielsweise die Leitungsverschlüsselung der im LVN BB übertragenen Daten umgesetzt wurden.

10.4 Erstellung von Protokolldateien

Ein Landesbetrieb fragte an, unter welchen Voraussetzungen Protokolldateien ein- und ausgehender E-Mails gespeichert werden dürfen.

Enthalten Protokolle personenbezogene Daten, unterliegt ihre Nutzung gem. § 13 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) einer engen Zweckbindung. Ausdrücklich untersagt ist gem. § 29 Abs. 4 BbgDSG die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle. Eine vollständige Aufzeichnung aller benutzerspezifischen Aktivitäten durch die Systembetreuung, insbesondere die Speicherung der Inhalte elektronischer Post ist grundsätzlich nicht erforderlich und daher auch nicht zulässig. Beim Verdacht auf eine missbräuchliche Nutzung des E-Mail-Dienstes kann es ausnahmsweise notwendig werden, den Umfang der Protokollierung vorübergehend zu erweitern. Die Entscheidung hierüber sollte sich an der Häufigkeit und Bedeutung der aufzuklärenden Umstände orientieren und unter Beteiligung der Personalvertretung getroffen werden.

Inwieweit eine Protokollierung datenschutzrechtlichen Anforderungen entspricht, bemisst sich weiterhin nach der Dauer der Aufbewahrung der Protokolldaten und den bestehenden Zugriffs- und Auswertungsmöglichkeiten. Die Aufbewahrungsdauer von Protokolldaten ein- und ausgehender E-Mails sollte daher den Zeitraum von 30 Tagen grundsätzlich nicht überschreiten. Soweit Protokolle zum Zweck gezielter Kontrollen angefertigt werden, ist eine kürzere Aufbewahrungsdauer vorzusehen; in der Regel reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

Weiterhin sollten bei der Protokollierung von E-Mails folgende technische und organisatorische Maßnahmen berücksichtigt werden:

- Der Umfang der Protokolldaten sollte nach dem Grundsatz der Erforderlichkeit festgelegt, im Verfahrensverzeichnis dokumentiert und den Nutzerinnen und Nutzern bekannt gegeben werden (z. B. Datum, Uhrzeit, Empfänger- und Absenderadresse, Anzahl der übertragenen Bytes und Fehlercode der Übertragung).

- Die Verwendung der Protokolldaten muss an genau definierte Zwecke gebunden werden, so zum Beispiel an die Aufrechterhaltung der Systemsicherheit, die Analyse und Korrektur technischer Fehler im Netz, die Optimierung der Rechnerleistungen im Netzwerk, die Ermittlung der Kosten verbrauchter Ressourcen zwecks interner Leistungsverrechnung sowie an die Kontrolle der Einhaltung dienst- oder arbeitsrechtlicher Vorgaben.

- Die Verwendungszwecke und Aufbewahrungsfristen von Protokolldaten sind aus Gründen der Transparenz im Verfahrensverzeichnis zu dokumentieren, sie müssen den Mitarbeiterinnen und Mitarbeitern vor Nutzung des E-Mail-Dienstes bekannt gegeben werden.

- Der Zugriff auf die Protokolldaten muss auf das technische Personal begrenzt bleiben, das für den Netzwerkbetrieb und die Bereitstellung der jeweiligen Dienste zuständig ist. Diese Personen sind verpflichtet, sich an die beschriebene Zweckbindung zu halten und außerhalb der beschriebenen Zwecke keine Detailinformationen aus den Protokollen weiterzugeben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in den Orientierungshilfen „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ sowie „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ intensiv mit der Problematik der Protokollierung beschäftigt.[38]

Bei jeder Protokollierung in DV-Systemen sind die Grundsätze der Datensparsamkeit, der Zweckbindung und der Transparenz einzuhalten. Durch technische und organisatorische Maßnahmen ist der Zugriff auf Protokolldaten auf das erforderliche Maß zu begrenzen.

10.5 Conficker – Lückenhafter Virenschutz in der Landesverwaltung

Durch Pressemeldungen erfuhren wir, dass der Computerwurm Conficker Rechner des Ministeriums der Finanzen (MdF) befallen hatte. Unsere Nachfragen beim MdF und beim Brandenburgischen IT-Dienstleister (ZIT-BB) enthüllten eklatante Mängel im Sicherheitsmanagement.

Der Sicherheitsvorfall wurde im Rahmen von Wartungsarbeiten des IT-Dienstleisters an zentralen IT-Systemen des MdF festgestellt. Ein Virenscan der verdächtigen Systeme ergab, dass sie mit dem Computerwurm Conficker

[38] siehe http://www.lda.brandenburg.de

infiziert waren. Der ZIT-BB hat daraufhin sämtliche Arbeitsplatz-PCs, Notebooks und Server des MdF auf Schadsoftware gescannt, die Virenschutzprogramme aktualisiert und den Patchstand der Betriebssysteme überprüft. Im Ergebnis waren zwei Arbeitsplatz-PCs, zwei Notebooks und drei Server, davon ein Windows Domain Controller, mit Conficker infiziert.

Trotz unserer konkreten Nachfragen waren die Stellungnahmen des MdF und des ZIT-BB über den Vorfall vage und bruchstückhaft. Das genaue Vorgehen bei der Untersuchung und Säuberung der Systeme blieb völlig im Dunkeln. Angaben zur Variante des Wurms Conficker und zur Untersuchung der Integrität der Systeme und der Wurmaktivitäten fehlten genauso wie Aussagen zur Prüfung der Beeinträchtigung von personenbezogenen Daten durch den Wurm. Trotz der mangelhaften Analyse kamen die Berichte des IT-Sicherheitsbeauftragten des MdF und des IT-Dienstleisters zu dem Schluss, dass „zu keinem Zeitpunkt ein Risiko bezüglich Vertraulichkeit und Integrität der Daten“ bestanden hätte bzw. dass „davon auszugehen sei, dass sich der durch den Wurm verursachte Schaden auf den Ausfall der Systeme beschränkt hat und personenbezogene Daten weder ausgespäht noch verändert wurden“. Diese Aussagen sind für uns nicht nachvollziehbar.

Als mögliche Ursachen für den Vorfall wurden die offenbar vernachlässigte Aktualisierung von Antivirensoftware und Betriebssystemen auf Notebooks im Zusammenhang mit der Überleitung der IT-Technik an den ZIT-BB, eine zu seltene Anbindung der Notebooks an das lokale Netz zwecks Durchführung von Updates sowie ein nicht mehr genutzter Server ohne erforderliche Windows Updates und Antivirensoftware benannt. Auf den Umstand, dass bereits seit über zwei Jahren wirksame Aktualisierungen für das Microsoft-Betriebssystem und Virenschutzprodukte gegen Conficker zur Verfügung stehen und dementsprechend die betroffenen Systeme mindestens zwei Jahre lang nicht aktualisiert worden sein mussten, wurde nicht eingegangen.

Folgende Mängel in der IT-Sicherheitsorganisation wurden festgestellt:

- Das IT-Sicherheitskonzept des MdF befindet sich erst in einem Entwurfsstadium. Ein Virenschutzkonzept scheint im MdF nicht zu existieren.

- Es fehlen Regelungen, die die erforderlichen Aktualisierungen des Betriebssystems und der Virenscanner, insbesondere auch von mobilen Endgeräten, sicherstellen.

- Dem IT-Dienstleister fehlt bereits seit Jahren ein vollständiger Überblick über die von ihm betreuten Systeme inklusive Standorten, Patchlevel und installierten Anwendungen.

- Ein zentrales Virenschutzkonzept des IT-Dienstleisters wurde noch nicht umgesetzt. Vielmehr hat für das Ressort übergreifende Virenschutzmanagement erst 2011 eine Ausschreibung stattgefunden.

- Das MdF als Daten verarbeitende Stelle steht in der Verantwortung, sich als Auftraggeber des ZIT-BB von den vor Ort getroffenen technischen und organisatorischen Maßnahmen für den Datenschutz und die IT-Sicherheit zu überzeugen, sieht sich aber nicht in der Lage, entsprechende Kontrollaktivitäten durchzuführen.

Als Gegenmaßnahmen für die Zukunft plant das MdF die Einführung eines Informationssicherheits-Managementsystems, von Notfallmanagement-Prozessen und von Regelungen für häusliche und mobile Arbeitsplätze. Der ZIT-BB beabsichtigt den Aufbau einer Datenbank mit allen von ihm betreuten Systemen (Configuration Management Database), die Einführung eines zentralen Virenschutzmanagements (s. o.) und die Bestellung eines Security Incident Response Team. Weiterhin sollen Sicherheitspatches und Virenschutzprodukte konsequent installiert und auf aktuellem Stand gehalten werden.

Zu den wenigsten der geplanten Maßnahmen wurden uns Verantwortliche oder Termine für die Realisierung und Kontrolle genannt. Außerdem sind einige der genannten Maßnahmen allgemeinerer Art, die teilweise bereits seit Jahren als Ziele benannt, aber bis heute nicht umgesetzt sind. Konkrete Sofortmaßnahmen zur kurzfristigen Abmilderung des Infektionsrisikos wurden nicht aufgeführt.

Insgesamt zeigen sowohl der Sicherheitsvorfall als solcher als auch seine Behandlung durch das MdF und den ZIT-BB die Mängel im IT-Sicherheitsmanagement auf. Eine klare Planung zur schnellen Beseitigung der Mängel ist dagegen nicht erkennbar. Der Bericht vermittelt stattdessen den Eindruck, dass im Grunde ja nichts passiert sei und der Vorfall keine Auswirkungen auf die Informationssicherheit gehabt habe.

Es ist erforderlich, dass das MdF einen konkreten Maßnahmenplan zur Senkung des Risikos für einen Befall mit Schadsoftware erstellt. Dieser Maßnahmenplan muss die unmittelbaren Konsequenzen aus dem Vorfall enthalten und sowohl Umsetzungstermine als auch verantwortliche Personen für die Realisierung und die Kontrolle der Maßnahmen festlegen, um eine zügige Implementierung der Maßnahmen sicherzustellen.

11 Jugend und Familie

11.1 Bildaufnahmen in der Kita

Immer wieder erreichen uns Anfragen zur Verwendung von Bildern oder Videoaufnahmen der Kita-Kinder für verschiedene Zwecke, insbesondere zur Dokumentation der Entwicklung, für Einblicke in das Alltagsgeschehen, zur Veröffentlichung in der örtlichen Presse oder auf der Kita-eigenen Homepage.

Um die Entwicklung eines Kindes zu dokumentieren, ist es in aller Regel ausreichend, wenn die Erzieher entsprechende Wahrnehmungen in Beobachtungsbögen festhalten und qualifizierte Entwicklungsberichte fertigen. Eine Dokumentation mittels Fotos ist nur in Einzelfällen in Bezug auf ein bestimmtes Kind zulässig. Die schriftliche Einwilligung der Eltern ist in jedem Einzelfall einzuholen. Auch wenn diese Einwilligung vorliegt, sind die datenschutzrechtlichen Grundsätze der Erforderlichkeit und der Zweckbindung zu beachten. Die Daten sind zu löschen, sobald der Zweck ihrer Erhebung entfallen ist.

Die Veröffentlichung von Fotos oder Videoaufnahmen richtet sich nach den Bestimmungen des Kunsturhebergesetzes (KunstUrhG). Das Recht am eigenen Bild ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts: Jeder entscheidet grundsätzlich selbst darüber, ob überhaupt und in welchem Zusammenhang Bilder von ihm verbreitet oder öffentlich zur Schau gestellt werden. Die Darstellung ist regelmäßig nicht mit den Ausnahmetatbeständen des § 23 KunstUrhG vereinbar. Bilder dürfen nur mit Einwilligung aller darauf Abgebildeten veröffentlicht werden.

Die Einwilligungserklärung muss bewusst abgegeben werden und eindeutig sein. Jeder Einwilligende ist über die wesentlichen Eckpunkte der geplanten Nutzung der Fotos zu informieren. Neben Angaben dazu, gegenüber wem die Erklärung abgegeben wird, müssen Hinweise darauf enthalten sein, dass die Einwilligung jederzeit widerrufen werden kann. Es ist ratsam, für die konkreten Anlässe bzw. Situationen jeweils gesonderte Einwilligungen der Eltern einzuholen. Bei Veranstaltungen könnte z. B. schon bei der Anmeldung ein Hinweis auf die geplante Veröffentlichung von Bildern mit der Bitte um Einwilligung erfolgen. Pauschale Einwilligungen, z. B. im Aufnahmeantrag, genügen den dargestellten Anforderungen nicht.

Die an uns gerichteten Anfragen bezogen sich vor allem auf folgende Situationen:

- Fotos oder Videoaufnahmen, mit denen Eltern Einblicke in das Alltagsgeschehen der Kita gegeben werden sollen (z. B. bestimmte Projekte, besondere Unternehmungen, regelmäßige Feste), dürfen nur in der Kita selbst und nicht im Außenbereich (z. B. Schaukasten) gezeigt werden.

- Bei der Weitergabe von Fotos an die jeweiligen Eltern der Kinder bzw. der Anfertigung von Abzügen ist darauf zu achten, dass Einwilligungen hinsichtlich aller auf den Fotos abgebildeten Personen vorliegen.

- Die Eltern sollten auch über einen Termin mit einem Fotografen in der Kita in geeigneter Weise rechtzeitig informiert werden. Der Fotograf darf die gefertigten Bilder nicht ohne Einwilligung der Eltern ausstellen.

- Bei der beabsichtigten Veröffentlichung von Fotos in Printmedien muss sich die Einwilligung der Eltern, ausdrücklich auf diese beziehen. In der Einwilligungserklärung sollte zudem darauf hingewiesen werden, dass Zeitungen und andere Druckmedien ggf. im Internet eingesehen und von dort herunter geladen werden können.

- Hinsichtlich der Publikation von Fotos auf der Kita-eigenen Homepage muss sich die Einwilligung der Eltern ausdrücklich auf die Internetveröffentlichung beziehen. Einmal im Internet veröffentlichte Bilder lassen sich kaum mehr daraus entfernen.

Um dem Grundsatz der Datensparsamkeit Rechnung zu tragen, sollte auf die Nennung der Namen von Abgebildeten verzichtet werden. Nicht personenbezogene Alternativen (z. B. Spieler, Teilnehmer, Kind der Sternchengruppe, Dreijähriger) sind zu bevorzugen.

Voraussetzung für die Veröffentlichung der Aufnahmen von Kindern ist die Einwilligung der Eltern. Diese sollte den Anlass für die Aufnahmen sowie die beabsichtigte Art ihrer Nutzung möglichst konkret benennen.

11.2 Neue Datenerhebung wegen neuer Software?

Ein freier Träger machte uns darauf aufmerksam, dass das zuständige Jugendamt von Kindertagesstätten in freier Trägerschaft personenbezogene Daten der betreuten Kinder angefordert hat, um die Daten mit weniger Aufwand in eine neue Datenbank eingeben zu können.

Aus den Tabellen sollten die Vor- und Nachnamen der Kinder, die Geburtsdaten, die Wohnanschriften, der Betreuungsumfang, etwaige Befristungen und bei abweichenden Familiennamen auch die Namen der Eltern hervorgehen. Das Jugendamt berief sich darauf, dass diese Daten ohnehin im Rahmen der

Anspruchsprüfung des Brandenburgischen Kindertagesstättengesetzes von den Eltern verarbeitet werden dürfen.

Die betreffenden Daten waren durch das Jugendamt unmittelbar bei den Eltern bereits im Rahmen der Antragsprüfung auf einen Betreuungsplatz erhoben worden. Eine nochmalige Erhebung dieser Daten war nicht erforderlich und damit unzulässig. Die freien Träger haben zwar im Rahmen der Finanzierung an das Jugendamt die Anzahl der Kitaplätze differenziert nach Altersgruppen zu melden, darüber hinausgehende personenbezogene Daten sind von ihnen jedoch nicht an das Jugendamt zu übermitteln. Somit lag weder eine Erhebungsbefugnis seitens des Jugendamtes noch eine Übermittlungsbefugnis seitens der freien Träger vor. Daher haben wir das Jugendamt aufgefordert, die Datenerhebung einzustellen und die bereits erhobenen Daten zu löschen. Das Jugendamt ist dieser Forderung gefolgt.

Die doppelte Erhebung bereits vorliegender personenbezogener Daten – z. B. bei der Einführung einer neuen Software – ist unzulässig.

11.3 Vertraulichkeit von Informantendaten in der Jugendhilfe

Auch nach unserer Veröffentlichung im letzten Tätigkeitsbericht[39] erreichten uns unterschiedliche Anfragen zum Umgang mit den Informantendaten. In einem Fall erkundigte sich ein Jugendamtsmitarbeiter, ob der Name eines Informanten den betroffenen Eltern bekannt gegeben werden durfte. In einem anderen Fall ging es um die Frage, ob der Name eines Hinweisgebers zu einer Kindeswohlgefährdung an die Polizei oder die Staatsanwaltschaft herauszugeben war.

Namen von Informanten unterliegen, wenn sie von einem Jugendamt im Hinblick auf dessen Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden, dem Sozialgeheimnis. Dies gilt unabhängig davon, ob Vertraulichkeit ausdrücklich gefordert oder zugesichert worden ist. Gemäß § 67d Zehntes Buch Sozialgesetzbuch (SGB X) ist eine Übermittlung dieser Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im Sozialgesetzbuch vorliegt.

Während eines laufenden Verfahrens haben die betroffenen Eltern bei Vorliegen eines berechtigten Interesses gemäß § 25 Abs. 1 SGB X ein Recht auf Akteneinsicht. Aus § 83 Abs. 1 SGB X ergibt sich – unabhängig von einem Verwaltungsverfahren – zudem ein Recht auf Auskunft über die eigenen

39 vgl. Tätigkeitsbericht 2008/2009, A 1.3

Sozialdaten, was grundsätzlich auch Informationen zu deren Herkunft, also z. B. den Namen des Informanten, umfasst. Allerdings ist das Jugendamt nach § 25 Abs. 3 SGB X nicht zur Gestattung der Akteneinsicht befugt, soweit die Vorgänge wegen eines berechtigten Interesses des Informanten geheim gehalten werden müssen. Gemäß § 83 Abs. 4 SGB X hat eine Auskunftserteilung zu unterbleiben, soweit diese die ordnungsgemäße Erfüllung der in der Zuständigkeit des Jugendamtes liegenden Aufgaben gefährden würde oder die Daten wegen der überwiegenden berechtigten Interessen des Informanten geheim gehalten werden müssen.

Das Bundesverwaltungsgericht hat in einem solchen Fall entschieden, dass das Geheimhaltungsinteresse des Informanten das Informationsinteresse der betroffenen Eltern immer dann überwiegt, wenn keine Anhaltspunkte dafür vorliegen, dass der Informant wider besseres Wissen und in der Absicht einer Rufschädigung gehandelt oder leichtfertig falsche Informationen gegeben hat.[40]

Eine Befugnis zur Übermittlung seines Namens an die betroffenen Eltern kommt somit nur noch mit entsprechender Einwilligung des Informanten gemäß § 67b SGB X in Betracht. Eine solche Einwilligung hat jedoch schriftlich zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Auch eine Übermittlung von Sozialdaten an Polizei und Staatsanwaltschaft ist nach § 68 Abs. 1 SGB X nur zulässig, soweit kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen des Informanten beeinträchtigt werden.

Anders zu entscheiden ist bei Vorliegen einer richterlichen Anordnung. Hier ist die Übermittlung des Namens des Informanten gemäß § 73 Abs. 3 SGB X zulässig, und zwar auch dann, wenn eine Übermittlung nach § 68 Abs. 1 SGB X an Polizei und Staatsanwaltschaft gerade nicht erfolgen darf. Rechtlich umstritten ist, ob Informantendaten als Angaben i. S. d. § 65 Achtes Buch Sozialgesetzbuch angesehen werden können, die zum Zweck persönlicher und erzieherischer Hilfe anvertraut werden. In diesem Fall wäre eine Übermittlung auch bei Vorliegen einer richterlichen Anordnung unzulässig.

[40] vgl. Urteil des Bundesverwaltungsgerichts vom 4. September 2003, 5 C 48/02

Ohne Informationen aus dem sozialen Umfeld könnte das Jugendamt seinem Schutzauftrag bei Kindeswohlgefährdungen nicht nachkommen. Daher hat es in den Fällen, in denen keine Anhaltspunkte dafür vorliegen, dass ein Informant wider besseres Wissen und in der Absicht einer Rufschädigung handelte oder leichtfertig falsche Informationen gab, grundsätzlich keine Befugnis, dessen Namen herauszugeben.

12 Justiz

Pressemitteilungen der Gerichte zu Strafverfahren

Zu Beginn des Jahres 2010 sichteten wir die Pressemitteilungen der Strafgerichte im Land und mussten dabei feststellen, dass bei den Informationen zu künftigen oder vergangenen Gerichtsterminen in etlichen Fällen so viele Angaben über Straftäter erfolgten, dass deren Identifikation möglich war.

Die Sachverhaltsdarstellungen zu den Straftaten enthielten teilweise Angaben, aus denen Rückschlüsse auf einen konkreten Beschuldigten gezogen werden konnten. Statt „der Angeklagte“ zu schreiben, wurden in den Texten vielfach Initialen verwendet oder gar der ganze Vorname genannt. Dazu kamen teilweise noch Angaben zum Alter oder dem Wohnort. Je mehr solche Informationen zum Angeklagten erfolgen, desto eher lässt sich ein Bezug zu einer konkreten Person herstellen.

Auch Angaben zum Beruf oder zur ausgeübten Tätigkeit können Rückschlüsse ermöglichen. In Zeiten des Internet sind diese selbst durch Ortsferne viel einfacher geworden – unabhängig davon, ob es bei dem Straftäter nun um einen Rechtsanwalt oder Arzt in einem abgelegenen Dorf oder einen ehemaligen Geschäftsführer einer konkreten Firma geht.

Die Gerichte sind unseren Empfehlungen nachgekommen.

Pressemitteilungen der Gerichte sollten Sachverhalte möglichst anonymisiert darstellen. Es sollte deshalb auf die Nennung von Namen, Initialen, kleineren Wohnorten sowie ggf. auch auf Berufs- oder Tätigkeitsbezeichnungen verzichtet werden.

13 Kommunales

13.1 Keine gemeinsame Nutzung von Kundendaten durch städtische Unternehmen

Stadtverwaltungen erkundigen sich immer wieder, ob kommunale Unternehmen zum Zweck der Abrechnung und der Vollstreckung ihrer Forderungen auf einen gemeinsamen Bestand von Kundendaten zugreifen dürfen.

In den von uns bearbeiteten Fällen ging es um Aufgaben der Grundversorgung, die unter anderem von Stadtwerken, Wohnungsbaugesellschaften oder Wasser- und Abwasserzweckverbänden wahrgenommen wurden. Diese Unternehmen verfügten beispielsweise über Adressen, Bankverbindungen oder über Ergebnisse von Bonitätsprüfungen ihrer Kunden. Die Verwaltungen beabsichtigten, einen solchen Datenbestand zusammenzuführen und sowohl für die Abrechnung von Leistungen als auch für die Vollstreckung von Forderungen unterschiedlicher städtischer Unternehmen zu verwenden.

Unternehmen, denen Aufgaben der Grundversorgung obliegen, sind aus datenschutzrechtlicher Sicht als eigenständige Daten verarbeitende Stellen anzusehen. Diese funktionale Trennung gilt unabhängig von der Rechtsform, in der sie organisiert sind. Somit sind sowohl privatrechtliche Gesellschaften als auch kommunale Eigenbetriebe oder öffentlich-rechtliche Zweckverbände jeweils separate Daten verarbeitende Stellen. Für Dienstleister, die mit der Abrechnung beauftragt sind, gilt dasselbe wie für deren Auftraggeber: Der Dienstleister darf Daten grundsätzlich nur für solche Zwecke verwenden, für die sie auch erhoben wurden. Außerdem darf er ausschließlich auf solche personenbezogenen Daten zugreifen, die aus dem Geschäftsbereich seines Auftraggebers stammen. Weder der Dienstleister noch der Auftraggeber dürfen auf Kundendaten aus dem Geschäftsbereich anderer Unternehmen zugreifen.

Städtische Unternehmen, die zivilrechtliche Forderungen erheben, können ein Inkassounternehmen beauftragen.[41] Für die Vollstreckung der Forderungen benötigen aber auch Inkassobüros ein zivilgerichtliches Urteil und sind auf den Einsatz eines hoheitlichen Vollstreckungsbeamten (z. B. Gerichtsvollzieher) angewiesen. Im Falle der Beauftragung des Inkassobüros durch mehrere städtische Unternehmen gilt ebenso wie bei der Abrechnung, dass der Dienstleister nur auf die Daten aus dem Geschäftsbereich des jeweiligen Auftraggebers zugreifen darf. Öffentlich-rechtliche Forderungen basieren hingegen auf Verwaltungsakten (z. B. Gebührenbescheiden) und sind ohne-

[41] vgl. A 8.2

hin von den öffentlichen Stellen selbst zu vollstrecken. Die Beauftragung eines Inkassounternehmens für solche hoheitlichen Aufgaben beispielsweise durch einen Zweckverband ist daher datenschutzrechtlich nicht zulässig.

Weder für Zwecke der Abrechnung von Leistungen noch der Vollstreckung von Forderungen dürfen städtische Unternehmen auf die Kundendaten anderer Unternehmen zugreifen. Dies gilt auch, wenn sie einen externen Dienstleister beauftragen.

13.2 Niederschriften öffentlicher Gemeindevertretersitzungen

Dürfen Niederschriften des öffentlichen Teils der Gemeindevertretersitzungen personenbezogene Daten enthalten? Ist es erlaubt, die Niederschriften z. B. im Amtsblatt, in Ratsinformationssystemen oder gar im Internet zu veröffentlichen? Erhalten Bürger Einsicht? Das sind immer wiederkehrende Fragen, die uns erreichen.

Die Kommunalverfassung des Landes Brandenburg regelt in § 42, dass über jede Sitzung der Gemeindevertretung eine Niederschrift zu fertigen ist, deren Mindestinhalt vom Gesetzgeber festgelegt wurde. Neben Zeit und Ort der Sitzung, den Namen der Teilnehmer, der Tagesordnung, den Ergebnissen der Wahlen und Abstimmungen muss sie auch den Wortlaut der Anträge und Beschlüsse enthalten.

Sind Namensnennungen, Adressen oder Grundstücksbezeichnungen beispielsweise für Anträge oder Beschlüsse nicht erforderlich, dürfen sie nicht festgehalten werden. Das gilt sowohl für die Formulierung der genannten Mindestinhalte selbst als auch für die Niederschriften. Werden in der Niederschrift über den Mindestinhalt hinausgehende Informationen – insbesondere personenbezogene Daten von Betroffenen – festgehalten, darf dies ebenfalls nur unter Beachtung der Erforderlichkeit und Datensparsamkeit erfolgen.

Begehrt ein Bürger Akteneinsicht in eine datenschutzgerecht gefertigte Niederschrift des öffentlichen Teils der Sitzung, so kann diese nach § 5 Abs. 2 Nr. 1 Akteneinsichts- und Informationszugangsgesetz gewährt werden. Auch steht dann einer Veröffentlichung gemäß § 4 Brandenburgisches Datenschutzgesetz im Amtsblatt, in Ratsinformationssystemen oder im Internet nichts entgegen. Beide Rechtsgrundlagen verweisen insoweit auf das Öffentlichkeits- und Transparenzgebot der Kommunalverfassung des Landes Brandenburg.

Niederschriften dürfen nur dann personenbezogene Daten enthalten, wenn sie für die Niederschrift selbst erforderlich sind. Der Akteneinsicht oder einer Veröffentlichung steht dann nichts im Weg.

13.3 Einführung von Ratsinformationssystemen

Ratsinformationssysteme werden mit dem Ziel eingesetzt, den Mitgliedern einer Gemeindevertretung Dokumente und Unterlagen – Tagesordnungen, Vorlagen, Anträge, Anfragen und Niederschriften – der Sitzungen elektronisch bereitzustellen. Weiterhin fördern Ratsinformationssysteme die Transparenz der Verwaltung, da Dokumente zu öffentlichen Sitzungen allgemein zugänglich gemacht werden können.

Sollen Ratsinformationssysteme zum Einsatz kommen, sind wegen des unterschiedlichen Schutzbedarfs der verarbeiteten Daten die Dokumente zu kategorisieren:

- Für datenschutzgerecht erstellte Dokumente aus öffentlichen Sitzungen (Tagesordnungen, öffentliche Vorlagen, Anträge, Anfragen, Niederschriften) sind keine besonderen Maßnahmen zur Verhinderung unberechtigter Zugriffe bzw. zur Sicherung der Vertraulichkeit bei der Übertragung über das Internet notwendig.

- Nicht-öffentliche Dokumente ohne personenbezogene Daten bzw. mit personenbezogenen Daten niedriger oder mittlerer Sensitivität (normaler Schutzbedarf) sind vor unberechtigter Kenntnisnahme zu schützen. Hierbei ist der Zugriff auf berechtigte Nutzer, die sich gegenüber dem System identifizieren und authentisieren müssen, zu beschränken. Die Authentisierung kann z. B. durch die Angabe von Benutzername und Passwort erfolgen. Zusätzlich sind die Dokumente bei ihrer Übertragung über das Internet zu verschlüsseln (Leitungsverschlüsselung). Die beteiligten Rechner sind durch Maßnahmen nach den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik abzusichern.

- Nicht-öffentliche Dokumente mit personenbezogenen Daten höherer Sensitivität (hoher Schutzbedarf, z. B. Personal-, Sozial- oder Steuerdaten) erfordern bei der Übertragung über das Internet eine Ende-zu-Ende-Verschlüsselung auf der Anwendungsebene. Darüber hinaus sind strenge Anforderungen an die Absicherung der Endsysteme zu stellen wie beispielsweise eine abgestufte benutzerspezifische Rechteverwaltung, die Verhinderung des Zugriffs auf externe Datenträger (z. B. Diskette oder USB-Speichermedien), die Protokollierung ausgewählter Aktivitä-

ten, die Verschlüsselung der auf einem Datenträger gespeicherten Dokumente oder die sichere Löschung nicht mehr benötigter Daten.

Vor Einführung eines Ratsinformationssystems muss geprüft werden, welche Kategorien von Dokumenten über das System bereitgestellt werden sollen und welche technischen und organisatorischen Maßnahmen umzusetzen sind, um dem Schutzbedarf gerecht zu werden.

13.4 Öffentliche Übertragung von Gemeindevertretersitzungen

Kommunale Vertretungen denken immer wieder darüber nach, ihre Sitzungen aufzuzeichnen oder gar live im Internet zu übertragen.

Die Kommunalverfassung des Landes Brandenburg regelt in § 36 Abs. 3 die Voraussetzungen für die Zulässigkeit von Ton- und Bildübertragungen sowie Ton- und Bildaufzeichnungen von Gemeindevertretersitzungen.

Grundsätzlich gilt zunächst, dass alle anwesenden Mitglieder der Gemeindevertretung einer Übertragung oder Aufzeichnung zustimmen müssen. Der Gesetzgeber räumt jedoch die Möglichkeit ein, durch einfachen Beschluss in der Geschäftsordnung die Bedingungen für die Zulässigkeit von Übertragungen oder Aufzeichnungen generell zu regeln und an die örtlichen Verhältnisse anzupassen. Auch wenn ein Gemeindevertreter dem Beschluss widerspricht, muss er als Inhaber eines öffentlichen Amtes die Beeinträchtigung, dass er gegen seinen Willen gefilmt wird, hinnehmen.

Etwas anderes gilt jedoch, wenn etwa Mitarbeiter der Verwaltung oder interessierte Bürger an der öffentlichen Sitzung teilnehmen. Eine Übertragung oder Aufzeichnung kann hinsichtlich dieser Personen nur dann erfolgen, wenn sie eingewilligt haben. Alternativ ist denkbar, die Zuhörer auszublenden oder aber bei Wortbeiträgen die Aufzeichnung bzw. Übertragung zu unterbrechen.

Nicht-öffentliche Sitzungen dürfen per Video weder aufgezeichnet noch übertragen werden. Tonaufzeichnungen zum Zweck der Erstellung von Niederschriften sind dagegen zulässig.

Öffentliche Gemeindevertretersitzungen dürfen im Internet übertragen werden, soweit das informationelle Selbstbestimmungsrecht der Anwesenden gewahrt bleibt.

13.5 Mobile Bürgerdienste

Landkreise, Städte und Gemeinden bieten inzwischen viele Dienstleistungen wie beispielsweise die An-, Ab- und Ummeldungen oder die Ausgabe von Personalausweisen auch außerhalb ihrer Verwaltungen an. Für diese Angebote nutzen sie beispielsweise die Räume von Universitäten, Gemeindezentren oder auch öffentlichen Plätzen mit einem mobil eingerichteten Arbeitsplatz. Welche technischen und organisatorischen Maßnahmen sind erforderlich, um solche Angebote datenschutzgerecht zu erbringen?

Die für solche Bürgerdienste genutzten mobilen Arbeitsplätze verfügen über ein so genanntes „Koffersystem“, das beispielsweise ein Notebook, einen Drucker und Lesegeräte für Fingerabdrücke sowie für ec-Karten enthält. Mit diesen Geräten greifen die Bürgerdienste über öffentlich zugängliche Funknetze auf Daten ihrer Verwaltungen zu und verarbeiten dabei teilweise personenbezogene Daten mit hohem Schutzbedarf. Die datenschutzrechtlichen Anforderungen an die technischen und organisatorischen Maßnahmen sind entsprechend hoch: Es bedarf einer physischen Sicherung vor Verlust und Diebstahl, eines effektiven Schutzes der funkbasierten und leitungsgebundenen Netzkommunikation (Verschlüsselung, Sicherung der Integrität) sowie einer restriktiven Rechteverwaltung für den Zugriff auf die Daten.

Das Ministerium des Innern und der Brandenburgische IT-Dienstleister haben im Rahmen eines Pilotprojekts eine zentrale Infrastruktur entwickelt, um den Kommunen von mobilen Arbeitsplätzen aus einen sicheren Zugriff auf die Daten in den Verwaltungen zu ermöglichen. Dabei wird per Funk die Verbindung zum Landesverwaltungsnetz hergestellt. Ein Transferkonzept soll sicherstellen, dass der Einrichtungsaufwand für Kommunen, die diese Infrastruktur erstmalig nutzen möchten, minimiert wird. Ein entsprechendes Pilotprojekt der Stadt Wittstock/Dosse haben wir im Berichtszeitraum begleitet. Die Stadt nutzt für ihre mobilen Bürgerdienste einen speziell hierfür ausgestatteten Kleinbus.

Die Nutzung der von der Landesverwaltung bereitgestellten Infrastruktur für mobile Bürgerdienste erweist sich aus unserer Sicht zurzeit noch als problematisch. Zwar stellt der Brandenburgische IT-Dienstleister die Infrastruktur zur Verfügung, allerdings bleibt die Kommune als Daten verarbeitende Stelle für die Einhaltung der Anforderungen des Datenschutzes und der Datensicherheit verantwortlich. Da sie selbst keinen Einfluss auf die Kommunikationsinfrastruktur im Landesverwaltungsnetz hat, kann sie in ihrem IT-Sicherheitskonzept lediglich die in ihrer eigenen Verantwortung liegenden Systeme berücksichtigen, also beispielsweise das „Koffersystem“ und den eigenen IT-Verbund. Vollständig ist ein solches Sicherheitskonzept aber nur, wenn alle

an dem Verfahren beteiligten Komponenten berücksichtigt werden. Auf diesen Umstand haben wir in mehreren Gesprächen über das genannte Pilotprojekt hingewiesen. Der Brandenburgische IT-Dienstleister hat ein vollständiges Sicherheitskonzept für die von ihm entwickelte Kommunikationsinfrastruktur bislang zwar noch nicht vorgelegt, aber zugesagt, diese Dokumentation nach der Umstellung des Landesverwaltungsnetzes auf eine neue Version[42] zu vervollständigen. Die Stadt Wittstock/Dosse hat dennoch entschieden, das zunächst im Probebetrieb befindliche Verfahren freizugeben und mobile Bürgerdienste trotz der bestehenden Sicherheitsrisiken – vorerst befristet – im Echtbetrieb anzubieten.

Einen im Vergleich zum zentralen Pilotprojekt anderen Ansatz verfolgt beispielsweise die Landeshauptstadt Potsdam. Sie hat in eigener Verantwortung eine Infrastruktur für die mobilen Bürgerdienste geschaffen und bietet diese beispielsweise in städtischen Gebäuden, Hochschulen oder Altersheimen an. Der wesentliche Unterschied besteht darin, dass die Funkkommunikation vom mobilen Arbeitsplatz bis zum Netz der Stadtverwaltung reicht und das Landesverwaltungsnetz nicht genutzt wird. Wir haben das Vorhaben begleitet und bewerten die erreichte Lösung als datenschutzgerecht.

Zentrale Voraussetzung für das Angebot mobiler Bürgerdienste ist eine sichere Kommunikation zwischen dem mobilen Arbeitsplatz und den DV-Verfahren in den internen Netzen der jeweiligen Kommunalverwaltung.

13.6 Das Projekt Maerker Brandenburg

Wilde Abfalldeponien, zugewachsene Fahrradwege oder defekte Straßenbeleuchtungen – das Internetportal Maerker Brandenburg[43] ermöglicht es, kommunale Verwaltungen auf Infrastrukturprobleme aufmerksam zu machen. Auf derselben Webseite informiert die jeweils zuständige Behörde über den Stand der Bearbeitung dieser Hinweise. Wie wird sichergestellt, dass durch diese Veröffentlichungen keine personenbezogenen Daten ins Netz gestellt werden?

Die zentrale Plattform Maerker Brandenburg wird vom Brandenburgischen IT-Dienstleister betrieben; den beteiligten Kommunen obliegt die Zuständigkeit für die Bearbeitung der eingehenden Meldungen. Hinweise können über ein Online-Formular übermittelt werden. Dabei sind unter anderem Angaben zum Ort sowie eine Beschreibung des vorgefundenen Missstands erforderlich. Wer möchte, kann auch Fotografien übermitteln, auf denen der Stein des Anstoßes zu erkennen ist. Sowohl die genauen Angaben zur Adresse als

42 vgl. A 10.3

43 siehe http://maerker.brandenburg.de

auch die auf den Fotos erkennbaren Grundstücke, Gebäude, Personen oder Kfz-Kennzeichen stellen möglicherweise personenbezogene Daten dar.

Um die Nutzer über die Rechtslage zu informieren, bietet Maerker Brandenburg auf dem Online-Formular zur Übermittlung der Angaben einen „Rechtshinweis“ an. Dieser enthält unter anderem Erläuterungen zum Schutzbedarf für personenbezogene Daten. Erst nachdem wir die Projektbetreiber mehrfach aufgefordert hatten, ergänzten sie die Erläuterungen um einen Hinweis auf den Personenbezug von Kfz-Kennzeichen. Auch solche Kennzeichen lassen schließlich Rückschlüsse auf natürliche Personen zu und dürfen deshalb selbst als „Beiwerk“ nicht auf den veröffentlichten Fotos zu erkennen sein. Außerdem haben wir darauf hingewiesen, dass Schulungen und Einweisungen der Verwaltungsmitarbeiter wichtige Voraussetzungen für den datenschutzgerechten Betrieb von Maerker Brandenburg sind.

Vor der Veröffentlichung müssen Redakteure der jeweiligen kommunalen Verwaltung die für ihren Zuständigkeitsbereich eingehenden Meldungen einzeln überprüfen und personenbezogene Textpassagen oder Abbildungen entfernen, um den Schutz der personenbezogenen Daten zu gewährleisten. Im Ergebnis einer stichprobenartigen Überprüfung der veröffentlichten Meldung hatten wir keinen Zweifel daran, dass die Behörden dieses datenschutzrechtliche Erfordernis in ausreichender Weise umsetzen. Originalmeldungen, die den Kommunalverwaltungen über Maerker Brandenburg zur Verfügung gestellt werden, dürfen die Behörden nur so lange aufbewahren, wie dies für die Bearbeitung der Meldungen erforderlich ist.

Hinweise auf Missstände in der kommunalen Infrastruktur dürfen auf der Plattform Maerker Brandenburg nur veröffentlicht werden, wenn ein etwaiger Personenbezug zuvor entfernt wurde. Dies gilt sowohl für den Text der Meldungen als auch für Fotografien.

14 Meldewesen

14.1 Einführung des neuen Personalausweises

Am 1. November 2010 wurde der neue Personalausweis deutschlandweit eingeführt. Neben den bereits auf dem Ausweis gespeicherten Identifikationsmerkmalen enthält er nun zusätzlich ein biometrisches Passbild des Inhabers. Neu ist ein elektronischer Chip, auf dem die persönlichen Angaben und das Bild gespeichert sind. Außerdem ermöglicht er – optional – die Identifikation des Ausweisinhabers im elektronischen Ge-

schäftsverkehr, die Nutzung einer qualifizierten Signatur und die Speicherung biometrischer Fingerabdrücke.

Voraussetzung für die Nutzung der Identifikation im elektronischen Geschäftsverkehr (eID-Funktion) ist, dass der Ausweisinhaber diese Funktion nicht hat ausschalten lassen. Er kann sich damit unter Eingabe einer PIN im Internet genauso eindeutig ausweisen, wie dies bisher nur durch die tatsächliche Vorlage des Ausweises möglich war. Um den Personalausweis für eine – allerdings noch nicht verbreitete – qualifizierte elektronische Signatur zu nutzen, muss ein Signaturzertifikat im Nachhinein von einem zertifizierten Anbieter erworben und nachgeladen werden. Soweit der Ausweisinhaber die Speicherung biometrischer Fingerabdrücke wünscht, dürfen diese ausschließlich für hoheitliche Zwecke (z. B. von Polizeivollzugsbehörden, Zollverwaltung und Steuerfahndung) verwendet werden.

Die Einführung des neuen Personalausweises stellte an die Kommunalverwaltungen hohe Anforderungen bezüglich der Infrastruktur und Sicherheit der erforderlichen Informationstechnik. Es galt, das gesamte Verfahren datenschutzgerecht zu gestalten – von der Beantragung des Ausweises über die Weitergabe deren Daten an die Bundesdruckerei bis hin zur Ausgabe des fertigen Ausweises im Bürgerbüro. Zunächst verzögerte sich allerdings die Bereitstellung von Teilen der technischen Infrastruktur durch das Bundesministerium des Innern. Auch die Anwendung des von diesem im Vorfeld zur Verfügung gestellten Leitfadens zur Erstellung eines Sicherheitskonzepts bereitete erhebliche Probleme. Die Umsetzung des Sicherheitskonzepts nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik sowie die erforderlichen Testverfahren konnten deshalb erst kurz vor Einführung des neuen Personalausweises abgeschlossen werden.

Die Landeshauptstadt Potsdam führte als Testkommune vor dem offiziellen Einführungstermin Feldtests für den neuen Personalausweis durch. In diesem Rahmen berieten wir die Stadtverwaltung ausführlich zur Fortschreibung und Umsetzung des IT-Sicherheitskonzepts. Das Ergebnis konnte mithilfe der Kommunalen Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg (TUIV-AG) auch anderen Kommunalverwaltungen in Form eines Musterkonzepts zur Verfügung gestellt werden. Im Zusammenhang mit der Einführung des neuen Personalausweises erreichten uns nur vereinzelte Beschwerden. Die in diesem Zusammenhang aufgetretenen datenschutzrechtlichen Probleme bezogen sich auf die Datenübermittlung an die Bundesdruckerei; ihnen konnte vollständig abgeholfen werden.

Neben den Verwaltungen kommt aber auch den Inhabern der neuen Personalausweise eine eigene Verantwortung für den Schutz ihrer Daten zu. Für die Verwendung z. B. der eID-Funktion benötigen diese ein Kartenlesegerät.

Bei sogenannten Basislesern (Lesegeräte der Klasse 1) wird die PIN über die Tastatur des Computers eingegeben. Solche Geräte sind aus Sicherheits- und Datenschutzgründen nicht zu empfehlen, da Schadsoftware die Ausweis-PIN ausspionieren kann. Zu empfehlen ist hingegen der Einsatz von zertifizierten Standardlesegeräten (Klasse 2) mit einer integrierten Tastatur oder besser noch von Komfortlesegeräten (Klasse 3) mit integrierter Tastatur und Display. Diese ermöglichen die Eingabe der PIN in einer gesicherten Hardwareumgebung und minimieren das Risiko des Ausspähens durch Dritte. Auch bedarf es bei der Nutzung der neuen Funktionen des Personalausweises eines sicherheitsbewussten Umgangs des Einzelnen mit der PIN und dem Ausweis selbst.

Wer den neuen Personalausweis für den elektronischen Geschäftsverkehr nutzen möchte, sollte sich ein möglichst sicheres Kartenlesegerät zulegen, um das Ausspähen seiner PIN zu verhindern.

14.2 Zulässigkeit von Pass- und Ausweiskopien

Unter welchen Umständen dürfen öffentliche Stellen oder Unternehmen zwecks Identifizierung von Bürgern oder Kunden Kopien des Personalausweises oder Reisepasses erstellen oder zu den Unterlagen nehmen?

Durch das Fotokopieren von Personalausweis oder Reisepass werden personenbezogene Daten verarbeitet. Das gilt unabhängig davon, ob die Kopie auf Papier oder in elektronischer Form erfolgt. Sowohl öffentliche Stellen als auch Unternehmen unterliegen bei dieser Datenverarbeitung einem strikten Erlaubnisvorbehalt. Sie dürfen Kopien nur anfertigen bzw. zu ihren Unterlagen nehmen, wenn dies gesetzlich vorgesehen ist.

In der Praxis verlangen beispielsweise Auskunfteien jedoch häufig die Zusendung einer Kopie des Personalausweises zur Identitätsüberprüfung im Rahmen der Selbstauskunft Betroffener.[44] Sie bezwecken damit die Verhinderung eines Missbrauchs durch Unbefugte. Die Verweigerung der Herausgabe einer Kopie durch die Auskunft ersuchende Person kann die Ablehnung ihres datenschutzrechtlichen Auskunftsanspruchs nach § 34 Bundesdatenschutzgesetz (BDSG) zur Folge haben. Auch andere Unternehmen fertigen teilweise Ausweiskopien zum Zweck der Identitätsprüfung. So hatten wir beispielsweise die Anfrage eines Schrotthändlers zu beantworten, der die Herkunft des von ihm angekauften Altmetalls dokumentieren wollte. Er beabsichtigte, sich damit für den eventuellen Fall eines später aufgedeckten Diebstahls abzusichern.

[44] vgl. A 5.1.3

Zulässig ist die Vervielfältigung von Reisepässen und Personalausweisen nach unserer Auffassung in allen nicht gesetzlich geregelten Fällen ausschließlich unter folgenden engen Voraussetzungen:

- Die Erstellung einer Kopie muss erforderlich sein. Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises oder des Reisepasses und ggf. die Anfertigung eines entsprechenden Vermerkes ausreichend ist.

- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.

- Die Kopie muss als solche erkennbar sein.

- Daten, die nicht zu Identifizierungszwecken benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.

- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.

- Eine automatisierte Speicherung der Pass-/Ausweisdaten ist nach dem Passgesetz und dem Personalausweisgesetz unzulässig.

Das Recht des Betroffenen, sich eine Sicherheitskopie zum Zweck der leichteren Wiederbeschaffung zu machen, bleibt davon unberührt.

Die Vervielfältigung von Reisepässen oder Personalausweisen durch Kopieren, Scannen o. Ä. unterliegt strengen Bedingungen. Sie ist nur insoweit zulässig, als die Datenverarbeitung zum Zweck der Identifikation unerlässlich ist. Darüber hinausgehende personenbezogene Daten sind auf den Ausweiskopien unkenntlich zu machen.

14.3 Einführung des Landesmelderegisters

In unserem letzten Tätigkeitsbericht[45] schilderten wir die gesetzlichen Grundlagen zur Einführung eines elektronischen Landesmelderegisters. Inzwischen entwickelte der Brandenburgische IT-Dienstleister als Registerbehörde das erforderliche Datenverarbeitungsverfahren.

45 vgl. Tätigkeitsbericht 2008/2009, A 4.4.1

Aufgrund der gesetzlichen Festlegung fungiert der Brandenburgische IT-Dienstleister (ZIT-BB) hier selbst als Daten verarbeitende Stelle. Er hat daher zwei grundlegende datenschutzrechtliche Forderungen zu erfüllen:

Erstens ist ein tragfähiges IT-Sicherheitskonzept zu erarbeiten und umzusetzen, welches den hohen Schutzbedarf der verarbeiteten personenbezogenen Daten und die zentrale Speicherung der Daten aller Meldebehörden des Landes berücksichtigt. Zweitens fordert § 38 Abs. 3 Brandenburgisches Meldegesetz eine Trennung der Daten nach Meldebehörden, ohne das genaue Verfahren festzulegen. Denkbar ist eine logische Trennung, bei der letztlich allein die Applikationslogik sowie das Rollen- und Berechtigungskonzept unzulässige Zugriffe erschweren, oder eine physische Trennung, bei der die Speicherung an verschiedenen Orten oder mit unterschiedlicher Verschlüsselung Datenmissbrauch verhindert. Die Art der Datenspeicherung und -trennung hat erheblichen Einfluss auf die Datenbankarchitektur des Verfahrens und die erforderlichen technischen und organisatorischen Maßnahmen nach § 10 Brandenburgisches Datenschutzgesetz (BbgDSG).

Aus datenschutzrechtlicher Sicht favorisierten wir den Einsatz einer physischen Trennung, wohingegen der ZIT-BB die logische Trennung als ausreichend erachtete. Wir haben die Verantwortlichen deshalb aufgefordert, die mit der nur logischen Trennung der Datenbestände verbundenen Risiken im IT-Sicherheitskonzept explizit zu betrachten und ggf. ergänzende oder zur physischen Trennung alternative Sicherheitsmaßnahmen abzuleiten. Da der ZIT-BB darüber hinaus angab, wegen des „hohen Aufwandes“ auch auf eine verschlüsselte Speicherung der Meldedaten zu verzichten, verlangten wir die Vorlage konkreter und belastbarer Zahlen, durch die dieser „hohe Aufwand“ nachgewiesen wird (z. B. erhöhte Kosten für Hard- und Software, Abschätzung von Laufzeit- oder Performanceeinbußen). Beides lag bis zum Redaktionsschluss des Berichtes noch nicht vor.

Kritik haben wir auch an dem uns übersandten IT-Sicherheitskonzept geäußert. Es enthielt sowohl Fehler bezüglich des Umfangs der im Landesmelderegister gespeicherten Daten. Außerdem fehlte ein Realisierungsplan für noch nicht umgesetzte IT-Sicherheitsmaßnahmen. Es ist damit nicht abschätzbar, in welchem Zeitraum noch bestehende Lücken in der IT-Sicherheit bei der Registerbehörde geschlossen werden sollen und wer hierfür verantwortlich ist. Weiterhin verzichtete der ZIT-BB im Sicherheitskonzept trotz des hohen Schutzbedarfs für das Verfahren auf die Durchführung einer ergänzenden Risikoanalyse gemäß den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und BSI-Standard 100-3. Es ist damit aus unserer Sicht zurzeit nicht nachgewiesen, dass die von der Datenverarbeitung ausgehenden Risiken hinreichend beherrscht werden.

Aus unserer Sicht gibt es weiter erheblichen Diskussionsbedarf zur Umsetzung ergänzender IT-Sicherheitsmaßnahmen im Verfahren sowie zur Weiterentwicklung der IT-Infrastruktur in der Registerbehörde, um die hohen Sicherheitsanforderungen zum Schutz der zentral gespeicherten Daten aller Meldebehörden des Landes zu erfüllen.

15 Polizei

15.1 Kennzeichnungspflicht für Polizeibedienstete in Brandenburg

Mit dem Siebenten Gesetz zur Änderung des Brandenburgischen Polizeigesetzes[46] tritt zum 1. Januar 2013 eine Neuregelung zur Legitimations- und Kennzeichnungspflicht von Polizeivollzugsbediensteten in Kraft. Die Landesbeauftragte hat zu diesem Vorhaben eine Stellungnahme abgegeben.

Nach § 9 Brandenburgisches Polizeigesetz (BbgPolG) müssen die Polizeivollzugsbediensteten künftig ein Namensschild an der Dienstkleidung tragen. Beim Einsatz geschlossener Einheiten wird das Namensschild durch eine Kennzeichnung ersetzt, die eine nachträgliche Identitätsfeststellung erlaubt. Nur wenn und soweit durch die Kennzeichnung überwiegend schutzwürdige Belange der Betroffenen oder der Zweck einer polizeilichen Maßnahme beeinträchtigt würden, besteht keine Pflicht sich zu legitimieren oder zu kennzeichnen.

Aus unserer Sicht bestehen keine datenschutzrechtlichen Bedenken, weil der Gesetzgeber eine normenklare und verhältnismäßige Regelung geschaffen hat. Die namentliche Kennzeichnungspflicht stellt zwar einen Eingriff in das grundgesetzlich und durch die Landesverfassung von Brandenburg geschützte Recht auf informationelle Selbstbestimmung dar, indem sie die Betroffenen zwingt, ihren Namen äußerlich sichtbar an eine Vielzahl von Personen bekannt zu geben. Diese Einschränkung ist jedoch im überwiegenden Allgemeininteresse an einer Kennzeichnung zulässig. In einem modernen Rechtsstaat sollen sich Exekutivorgane und Bürger grundsätzlich offen begegnen. Eine Kennzeichnung schafft angemessene Transparenz und unterstreicht das eigenverantwortliche Handeln der Polizeibediensteten.

46 Siebentes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 9. Juni 2011 (GVBl. I, Nr. 10)

Die Tätigkeit von Polizeibediensteten, die aufgrund ihrer gesetzlichen Befugnisse das Gewaltmonopol des Staates vielfach in besonders einschneidender Weise durchsetzen, muss hinsichtlich ihrer Rechtmäßigkeit überprüfbar sein. Voraussetzung ist, dass eine möglicherweise rechtswidrige Dienstausübung einer einzelnen Person jederzeit zurechenbar ist. Wer in Rechte Dritter auch durch Ausübung unmittelbaren Zwangs eingreifen darf, muss daher einer effektiven Kontrolle unterworfen sein, die sich mit einer individuellen Kennzeichnung verbessern lässt. Dies ist besonders bei „anonymen Einsatzsituationen“ wichtig, wenn aufgrund äußerlich einheitlicher Kleidung und Schutzhelmen das Erscheinungsbild der Polizeibediensteten regelmäßig keine Identifizierung einzelner Personen zulässt. Im Übrigen trägt die Kennzeichnung auch umgekehrt dazu bei, falsche Anschuldigungen gegen Einsatzkräfte zügig aufklären zu können.

Die Pseudonymisierung, die z. B. durch eine Kennzeichnung mittels Nummern oder Buchstaben erfolgen kann, schützt die Polizeibediensteten geschlossener Einheiten, bei denen pauschalierend von einer höheren Gefährdung ausgegangen wird als bei anderen Bediensteten. Darüber hinaus ermöglicht der Ausnahmetatbestand des § 9 Abs. 3 BbgPolG, von der Kennzeichnung ganz abzusehen. Im Einzelfall muss zwischen den schutzwürdigen Belangen der Einsatzkräfte und dem Bedürfnis nach Identifizierbarkeit und Transparenz bei den von einer polizeilichen Maßnahmen Betroffenen abgewogen werden.

Wie die namentliche oder pseudonyme Kennzeichnung konkret ausgestaltet wird, soll durch eine Verwaltungsvorschrift des Innenministers festgelegt werden. Der Landtag hat darüber hinaus beschlossen, dass ihm zwei Jahre nach Einführung der Kennzeichnungspflicht ein Erfahrungsbericht vorgelegt wird.

Die Kennzeichnungspflicht von Polizeivollzugsbediensteten setzt ein sichtbares Zeichen für Transparenz und persönliche Verantwortung bei polizeilichem Handeln. Die gesetzliche Regelung ist hinsichtlich der Normenklarheit bei Eingriffen in das informationelle Selbstbestimmungsrecht der Polizeibediensteten zu begrüßen.

15.2 Telekommunikationsüberwachung und Kennzeichenfahndung durch die Polizei

Der Brandenburgische Landtag hat im Dezember 2011 das Achte Änderungsgesetz zum Polizeigesetz[47] verabschiedet und sich damit für den Erhalt der präventiven Telekommunikationsüberwachung und anlassbezogenen Kennzeichenfahndung entschieden. Beide Maßnahmen waren mit dem Vierten Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 18. Dezember 2006 in das Polizeigesetz eingeführt worden.

In § 33b Abs. 6 Brandenburgisches Polizeigesetz (BbgPolG) gestattete der Gesetzgeber der Polizei neben dem Abhören von Inhalten auch sog. Verkehrsdatenabfragen. Diese betreffen die Umstände der Kommunikation, also Informationen ob, wann, wie oft und von welchen Anschlüssen Kommunikation stattgefunden hat. Zudem regelt dieser Absatz die Mitwirkungspflichten der Anbieter von Telekommunikationsdiensten, um diese Datenerhebungen zu ermöglichen. Zur Identifikation und Lokalisation von Nutzern wurde in § 33b Abs. 3 BbgPolG die Befugnis geschaffen, spezifische Kennungen, insbesondere Geräte- und Kartennummern sowie den Standort von Mobilfunkendgeräten zu ermitteln. Darüber hinaus durfte nach dieser Norm die Telekommunikationsverbindung nicht nur überwacht, sondern auch unterbrochen werden. § 36a BbgPolG erlaubte die automatisierte Kennzeichenfahndung für bestimmte gesetzlich definierte Zwecke.

Die genannten Befugnisnormen waren 2006 zunächst auf zwei Jahre und 2008 um weitere drei Jahre bis 31. Dezember 2011 befristet worden. Die praktische Anwendung sollte einer abschließenden Evaluation unterzogen und laufende Entwicklungen in der Rechtsetzung bei Bund und Ländern sowie Rechtsprechung berücksichtigt werden.

Die geforderte Evaluation legte das beauftragte Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg im Mai 2011 vor. Das Institut kam dabei zu dem Ergebnis, dass in der Praxis keine Probleme mit den neuen Maßnahmen erkennbar seien. Der Bericht empfahl, die Voraussetzungen für die Abfrage von Verkehrsdaten der Telekommunikation eigenständig zu regeln, klarstellende und begrenzende Änderungen einzufügen und die befristeten Befugnisse dauerhaft zu übernehmen. Der im Oktober

[47] Achtes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 19. Dezember 2011 (GVBl. I, Nr. 31)

2011 vorgelegte Entwurf für das Achte Änderungsgesetz[48] zum Brandenburgischen Polizeigesetz setzte diese Empfehlungen um.

Wir haben uns bereits 2006 bei Einführung der Normen in unserer Stellungnahme für den Innenausschuss des Landtags und in unserem 14. Tätigkeitsbericht[49] kritisch zu den Befugnissen nach § 33b und § 36a BbgPolG geäußert. Zum einen rügten wir die mangelnde Normenklarheit der Regelung zur präventiven Telekommunikationsüberwachung zum anderen bestanden Zweifel an der Verfassungsgemäßheit der Kennzeichenfahndung, die als weiteres automatisches System zur Verdachtsgewinnung auch Daten vieler Personen erhebt, die durch ihr eigenes Verhalten keinen Anlass zur Fahndung gegeben haben.

Die brandenburgische Rechtsgrundlage für die automatische Kennzeichenfahndung hat das Bundesverfassungsgericht zwar 2008 in seiner Entscheidung über die Zulässigkeit der entsprechenden hessischen und schleswig-holsteinischen Vorschriften für verhältnismäßig befunden, weil die Eingriffsvoraussetzungen des § 36a Abs. 1 BbgPolG den weit gefassten Verwendungszweck hinreichend begrenzen.[50] Die grundlegenden Zweifel an der Notwendigkeit dieser Maßnahme, die für sich allein genommen lediglich die Feststellung erlaubt, dass Fahrzeuge, die auf bestimmte Halter zugelassen sind, einen Einsatzort der Fahndung passieren, sind damit nicht beseitigt. Die Begutachtung der Anwendungspraxis durch das Max-Planck-Institut hatte zudem ergeben, dass die Kennzeichenfahndung zu 95% bei Kraftfahrzeugdiebstählen – also zur Verfolgung von Straftaten – eingesetzt wird und damit nicht auf eine präventive Rechtsgrundlage sondern auf strafprozessuale Befugnisse gestützt wird. Die Trefferquote beim Datenabgleich lag dabei unter 5%, wobei keine Erkenntnisse vorliegen, ob tatsächlich die Gefahrenabwehr oder die Aufklärung einer Straftat deshalb erfolgreich waren. Die in Frage stehende präventive Befugnis, technische Mittel für die Standortbestimmung von Mobilfunkendgeräten einzusetzen, wurde insgesamt nur zweimal von der Polizei genutzt.

In der Anhörung vor dem Innenausschuss haben wir die Auffassung vertreten, dass § 33b Abs. 3 BbgPolG auf die Erlaubnis zur Standortbestimmung bei Gefährdung für Leib und Leben eines Menschen reduziert oder ersatzlos gestrichen werden sollte. Auf die präventive Befugnis zur Kennzeichenfahndung sollte darüber hinaus verzichtet werden, da angesichts der Eingriffsintensität und der Abschreckungswirkung dieser Maßnahme einerseits und den

48 Gesetzentwurf der Landesregierung zum Achten Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 24. Oktober 2011, Landtags-Drucksache 5/4163

49 vgl. Tätigkeitsbericht 2006/2007, A 1.3.3

50 vgl. Urteil des Bundesverfassungsgerichts, 1 BvR 2074/05, 1 BVR 1254/07 vom 11. März 2008, Absatz-Nr. 183

Anwendungsfällen andererseits keine zwingende Notwendigkeit für den Einsatz erkennbar ist.

Im Ergebnis wurde durch die Entscheidung des Landtags die Geltung der Maßnahmen der Telekommunikationsüberwachung gemäß § 33b Abs. 3 (unverändert) und der automatischen Kennzeichenfahndung gemäß § 36a BbgPolG bis zum 31. Dezember 2015 verlängert. Die von uns bereits 2006 geforderte Nachbesserung des § 36a dahin gehend, dass bei einem „Trefferfall“ unverzüglich eine Datenübereinstimmung geprüft und nicht erforderliche Daten sofort gelöscht werden müssen, wurde nach entsprechenden Vorgaben des Bundesverfassungsgerichts in Absatz 2 eingefügt.

Die mit dem Gesetz verabschiedete Änderung zur präventiven Abfrage von Verkehrsdaten der Telekommunikation orientiert sich an Vorgaben des Bundesverfassungsgerichts. Dieses hat in seinem Urteil zur anlasslosen Vorratsdatenspeicherung[51] eine normenklare Begrenzung der Zwecke der möglichen Datenverwendung durch den Gesetzgeber verlangt und einen präventiven Zugriff nur zur Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen. Daneben wird in den neu gefassten § 33b Abs. 6 BbgPolG auch der vom Bundesverfassungsgericht für die Gewährleistung effektiven Rechtsschutzes erforderliche Richtervorbehalt für die hier zu regelnden Verkehrsdatenabfragen aufgenommen. Die neu gefassten Beschränkungen sind grundsätzlich zu begrüßen. Unsere Bedenken hinsichtlich der unklaren Bestimmung der betroffenen Zielpersonen einer Telekommunikationsüberwachung bleiben hingegen bestehen.

Durch das Achte Gesetz zur Änderung des Polizeigesetzes werden polizeiliche Befugnisse im Bereich der Telekommunikationsüberwachung und Kennzeichenfahndung für weitere vier Jahre in das Polizeigesetz übernommen. Dies betrifft zum einen den Einsatz von Geräten, mit denen Kennungen und Standorte von Mobilfunkgeräten ermittelt sowie Telekommunikationsverbindungen unterbrochen oder verhindert werden können. Zum anderen bleibt die automatische Kennzeichenfahndung für präventive Zwecke zulässig. Unsere Zweifel, dass der präventive Einsatz dieser Maßnahmen, der auch zu Eingriffen bei rechtstreuen Betroffenen führt, erforderlich ist, bestehen weiterhin. Immerhin werden mit dem Gesetzentwurf wenigstens die Voraussetzungen der präventiven Abfrage von Verkehrsdaten der Telekommunikation eingeschränkt und präzisiert.

[51] vgl. Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BVR 256/08

15.3 Überprüfbarkeit des Messverfahrens bei Geschwindigkeitsübertretungen

Ein Landkreis und die Zentrale Bußgeldstelle der Polizei des Landes Brandenburg fragten uns zum Akteneinsichtsrecht von Prozessbevollmächtigten in Ordnungswidrigkeitenverfahren wegen Geschwindigkeitsüberschreitung. Zu entscheiden war, ob ein Anspruch auf Herausgabe des vollständigen Originalmessfilms besteht.

Wer einen Bußgeldbescheid erhält, kann gegen diesen Einspruch einlegen und die Korrektheit der Messung überprüfen lassen. Üblicherweise erfolgt dies erst in der Hauptverhandlung vor Gericht durch gerichtlich bestellte Sachverständige. Zunehmend bestellen Prozessbevollmächtigte jedoch bereits im Einspruchsverfahren Sachverständige zur Begutachtung der Messergebnisse, um die Erfolgsaussichten eines gerichtlichen Verfahrens beurteilen zu können.

Geschwindigkeitsüberschreitungen werden je nach Einsatzort und Zielverkehr mit unterschiedlichen Radarmessgeräten und Verfahren nachgewiesen. In der Vergangenheit wurden überwiegend rotlichtempfindliche Messfilme verwendet (analoge Messverfahren), bei denen zu Beginn und am Ende jedes Messeinsatzes sog. Kalibrierungsfotos angefertigt werden. Diese geben Informationen zum Messprozess. Fehlerquellen bei der Messung, die regelmäßig dazu führen, dass ein Messergebnis nicht verwertbar ist, können sich zum Beispiel daraus ergeben, dass zahlreiche Leerbilder auf dem Messfilm vorhanden sind, Unregelmäßigkeiten bei der Dateneinblendung auftreten oder die Kalibrierungsfotos nicht gefertigt wurden. Überprüfbar ist dies nur, wenn der gesamte Messfilm begutachtet wird.

Die Behörden hatten zu entscheiden, ob sie dem Antrag eines Verteidigers auf Übersendung des vollständigen Originalmessfilms stattgeben. Bisher wurde dies aus datenschutzrechtlichen Gründen abgelehnt, da eine Filmrolle nicht nur die relevanten Beweisfotos zu dem Einspruchsverfahren, sondern mehrere hundert Bildaufnahmen zu Verfahren gegen Unbeteiligte enthalten kann.

Dennoch musste der Landkreis in diesem Fall den gesamten Messfilm dem Verteidiger zur Einsichtnahme überlassen. Als Rechtsgrundlage für die Datenübermittlung an Prozessbevollmächtigte oder von diesen beauftragte Sachverständige dient § 16 Abs. 1 Buchstabe b i. V. m. § 13 Abs. 2 Buchstabe a des Brandenburgischen Datenschutzgesetzes. Danach ist eine zweckfremde Nutzung personenbezogener Daten zulässig, wenn eine Rechtsvorschrift dies erlaubt.

Im Ordnungswidrigkeitenverfahren gelten die für das Strafverfahren entwickelten Grundsätze zur Akteneinsicht der Verteidigung (§ 46 Abs. 1 Gesetz über Ordnungswidrigkeiten i. V. m. § 147 Strafprozessordnung, StPO). Zu den Akten des Bußgeldverfahrens gehören sämtliche verfahrensbezogenen Unterlagen der Verwaltungsbehörde, die zu den Akten genommen sind, einschließlich der polizeilichen Ermittlungsvorgänge und unmittelbaren Beweismittel, auf die der Vorwurf in tatsächlicher oder rechtlicher Hinsicht gestützt wird. Die Verteidigung ist daher berechtigt, die vollständigen Akten, die regelmäßig einem Sachverständigen vorgelegt werden – mit Bildaufnahmen des gesamten Messfilms – einzusehen. Eine Schwärzung oder Verpixelung der Gesichter und Kraftfahrzeugkennzeichen aller nicht im Verfahren betroffener Personen und Fahrzeuge auf dem Film oder in der Messserie scheidet schon wegen des unverhältnismäßigen Arbeitsaufwands als nicht praktikabel aus.

Anders ist eine Versendung bei digitalisierten Messverfahren zu beurteilen (z. B. ES 3.0. oder PoliScan Speed), die überwiegend von der Zentralen Bußgeldstelle bearbeitet werden. Es gibt keine Messfilme mit Einzelbildern und keine Kalibrierungsfotos mehr, sondern einzelne Bilddateien, die zu einer Messserie gehören. Im gesamten Verfahren wurden umfangreiche technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes umgesetzt (verschlüsselte und signierte Speicherung der Beweisfotos, strenge Zugangs- und Zugriffskontrollen). Wird Akteneinsicht in die komplette Messserie beantragt, müssen die Originaldateien mit Spezialprogrammen und Kryptoschlüsseln sichtbar gemacht werden. Die zentrale Bußgeldstelle bietet dafür einen Akteneinsichtsraum an. Bei Bedarf können hier die nicht zu dem konkreten Verfahren gehörenden beweiserheblichen Einzelbilder Dritter zur Bußgeldakte genommen werden, wobei die Personen und Kennzeichen durch Abdeckungen unkenntlich gemacht werden. Aus unserer Sicht würden die umfangreichen Sicherungsmaßnahmen für Bilddateien und der verbesserte Schutz personenbezogener Daten Unbeteiligter unterlaufen, wenn die Messserien, sowie dafür erforderliche Zugangsschlüssel an die Antragstellenden versandt werden. Die Einschränkung, dass die Akteneinsicht und Begutachtung bei der Bußgeldstelle ggf. durch beauftragte Rechtsanwälte erfolgen muss, halten wir bei diesem Verfahren für erforderlich und verhältnismäßig.

Wer einen Bußgeldbescheid wegen Geschwindigkeitsübertretung angreifen will, benötigt zur Beurteilung der Erfolgsaussichten Kenntnisse über mögliche Fehler im Messverfahren. Die Bußgeldbehörde muss Prozessbevollmächtigten Einsicht in den gesamten Messfilm oder die komplette Messserie gewähren. Die zwangsläufig damit verbundene Übermittlung von Beweisfotos Unbeteiligter ist wegen des Akteneinsichtsrechts der Verteidigung nach § 147 Strafprozessordnung zulässig. Bei analogen Verfahren kann dies durch Übersendung des Messfilms geschehen. Dagegen ist bei digitalisierten Verfahren der Zugang zu der kompletten Messserie durch eine Akteneinsicht vor Ort zu gewährleisten.

16 Rundfunk

15. Rundfunkänderungsstaatsvertrag

Im Dezember 2010 haben die Ministerpräsidenten der Länder den 15. Rundfunkänderungsstaatsvertrag unterzeichnet. Die Regelungen des Vertrages sollen die Finanzierung des öffentlich-rechtlichen Rundfunks in der Zukunft sichern. Dazu wird ab 2013 das bisherige gerätebezogene Modell der Gebührenerhebung durch ein wohnungs- bzw. betriebsstättenbezogenes Beitragsmodell abgelöst.

Mit dem vorgelegten 15. Rundfunkänderungsstaatsvertrag soll ein grundlegender Systemwechsel bei der Erhebung der finanziellen Mittel für die Tätigkeit des öffentlich-rechtlichen Rundfunks in Deutschland vollzogen werden. Die bisherige, an den Besitz eines Empfangsgerätes gekoppelte Rundfunkgebühr soll durch die Erhebung eines an das Innehaben einer Wohnung oder Betriebsstätte anknüpfenden Beitrages ersetzt werden. Ziel des neuen Beitragsmodells ist außer einer höheren Beitragsgerechtigkeit auch eine deutlich datenschutzgerechtere Beitragserhebung. Das letztgenannte Ziel droht der vorliegende Staatsvertrag zu verfehlen.

Die Umstellung auf eine wohnungsbezogene Abgabe wird zwar wahrscheinlich zu einer geringeren Zahl zu speichernder Beitragszahler führen. Den öffentlich-rechtlichen Rundfunkanstalten werden allerdings umfangreiche Befugnisse zur Erhebung der Daten der Beitragspflichtigen eingeräumt. Zunächst unterliegen die Wohnungs- oder Betriebsstätteninhaber einer Meldepflicht gegenüber den Rundfunkanstalten. Darüber hinaus können die Anstalten, soweit sie es für nötig halten, personenbezogene Daten potenzieller Beitragsschuldner auch bei Dritten – beispielsweise dem Vermieter – erheben. Ihnen wird per Gesetz der Zugriff auf weitere unbestimmte öffentliche und nicht-öffentliche Quellen eröffnet. Dies kann in der Praxis bedeuten,

dass die Rundfunkanstalten personenbezogene Daten ohne Wissen der betroffenen Bürger bei Adresshändlern, Versicherungen oder Arbeitgebern beschaffen. Der datenschutzrechtliche Grundsatz, Daten unmittelbar beim Betroffenen zu erheben, wird hier durchbrochen. Auch ist im 15. Rundfunkänderungsstaatsvertrag nicht hinreichend geregelt, welchen inhaltlichen Umfang die eingeräumten Datenerhebungsbefugnisse haben.

In dem Verfahren zur Rundfunkgebührenbefreiung bestehen darüber hinaus nach wie vor drei Möglichkeiten, den Nachweis des Bezugs von Sozialleistungen zu erbringen: durch die entsprechende Bestätigung der Behörde oder des Leistungsträgers im Original (Drittbescheinigung) oder durch den entsprechenden vollständigen Bescheid im Original oder in beglaubigter Kopie. Aus datenschutzrechtlicher Sicht ist allein die Vorlage der Drittbescheinigung als datensparsame Variante verhältnismäßig, da bei beiden anderen Varianten Daten an die GEZ (Gebühreneinzugszentrale) übermittelt werden, die diese für ihre Aufgabenerfüllung nicht benötigt.[52]

Aus datenschutzrechtlicher Sicht widersprechen die Datenverarbeitungsbefugnisse des Staatsvertrags durch zu umfangreiche Ermächtigungen der Rundfunkanstalten und ihrer Hilfsorgane den Grundsätzen der Verhältnismäßigkeit und Datensparsamkeit sowie den Grundsätzen der Normklarheit und Transparenz.

17 Schule

17.1 Novellierung der Datenschutzverordnung Schulwesen

Gut Ding will Weile haben! Der langwierige Prozess der Novellierung der Datenschutzverordnung Schulwesen (DSV) steht nun vor seinem Abschluss.

In unserem letzten Tätigkeitsbericht[53] haben wir ausführlich über unsere beratungsintensive Arbeit für die erste Novellierung der Datenschutzverordnung Schulwesen berichtet. Im Ergebnis der mit uns im Sommer 2008 begonnenen Abstimmung hat der Verordnungsgeber im November 2010 die Erste Verordnung zur Änderung der Datenschutzverordnung Schulwesen[54] auf den Weg gebracht. Schwerpunkt war u. a. die Umsetzung der Regelun-

52 vgl. Tätigkeitsbericht 2008/2009, A 3.1

53 vgl. Tätigkeitsbericht 2008/2009, A 6.1

54 Erste Verordnung zur Änderung der Datenschutzverordnung Schulwesen vom 12. November 2010 (GVBl. II, Nr. 76)

gen des § 65a Brandenburgisches Schulgesetz. Insbesondere wurden die Vorschriften der neuen §§ 13 bis 15 DSV zu Schulstatistiken, automatisierter Schülerdatei und Schülerlaufbahnstatistiken erarbeitet.

In einem zweiten Schritt ist nun die Verordnung noch einmal umfassend der aktuellen Rechtslage angepasst und neben kleineren materiellen Änderungen vor allem redaktionell überarbeitet worden. Das Ministerium für Bildung, Jugend und Sport hat uns hierzu rechtzeitig eingebunden und unsere Hinweise nach konstruktiver Zusammenarbeit entsprechend umgesetzt.

Es liegt nun ein datenschutzrechtlich konformer Entwurf der Datenschutzverordnung Schulwesen vor, der spätestens mit Beginn des Schuljahres 2012/2013 in Kraft treten soll.

Durch das rechtzeitige Einbinden unserer Dienststelle und die konstruktive Zusammenarbeit mit dem Bildungsministerium gelang es, einen Verordnungsentwurf zu erarbeiten, der den datenschutzrechtlichen Anforderungen entspricht.

17.2 Öffentliche und private Schulen: zweierlei Datenschutzrecht?

Wenn zwei dasselbe tun, müssen nicht unbedingt dieselben Regeln gelten. Dies zeigt sich auch bei den datenschutzrechtlichen Bestimmungen für Schulen in öffentlicher und freier Trägerschaft im Land Brandenburg. Deshalb bestehen in der Praxis Unsicherheiten bei der Rechtsanwendung.

Im Berichtszeitraum beschwerten sich Petenten, dass in der Schülerakte ihres Sohnes, der eine Schule in freier Trägerschaft besucht, Unterlagen enthalten seien, die aus datenschutzrechtlichen Gründen hätten entfernt werden müssen. Hätte es sich im beschriebenen Fall um eine Schule in öffentlicher Schulträgerschaft gehandelt, wäre der Sachverhalt eindeutig gewesen. In der Datenschutzverordnung Schulwesen ist abschließend geregelt, welche Daten Eingang in die Schülerakte finden dürfen. Eine solche Regelung fehlt jedoch für Schulen in freier Trägerschaft.

Das Brandenburgische Schulgesetz (BbgSchulG) legt in § 1 Abs. 2 fest, dass seine Vorschriften für Schulen in freier Trägerschaft nur dann anwendbar sind, wenn dies ausdrücklich im Gesetz bestimmt ist. Für die Regelungen des § 65 BbgSchulG zum Datenschutz fehlt eine solche Bestimmung. Damit ist auch die Datenschutzschutzverordnung Schulwesen nicht für Schulen in freier Trägerschaft anwendbar. Dies bedeutet, dass die Datenverarbeitung in jedem Einzelfall auf der Grundlage des Bundesdatenschutzgesetzes zu

prüfen ist. Um diese Prüfung zu erleichtern, haben wir empfohlen, sich in solchen Fällen grundsätzlich an den Vorgaben der Datenschutzverordnung Schulwesen zu orientieren.

In Ermangelung schuldatenschutzrechtlicher Vorschriften für Schulen in freier Trägerschaft sollte die Datenschutzverordnung Schulwesen zur Orientierung herangezogen werden.

17.3 Aktenfund in einer ehemaligen Schule

Erst anlässlich des Einbruchs in ein altes Schulgebäude stellte sich heraus, dass Schulakten dort ungesichert im Keller lagerten. Sie enthielten auch personenbezogene Daten der Schüler, Eltern und Lehrer.

Im Zuge der Neuorganisation der Schulstrukturen wurden bereits im Jahre 2002 eine Grundschule im Landkreis Prignitz geschlossen und die Räumlichkeiten an einen Dritten vermietet. Als im Berichtszeitraum in das alte Schulgebäude eingebrochen wurde, stellte sich heraus, dass dort weiterhin alte Schulakten in erheblichem Umfang gelagert wurden.

Als wir über den Vorfall unterrichtet wurden, kontrollierten wir die Räumlichkeiten vor Ort und stellten fest, dass die Akten unter anderem sensitive, personenbezogene Daten ehemaliger Schüler, Eltern und Lehrer enthielten. Die Unterlagen reichten bis in das Jahr 1963 zurück und lagerten ungesichert im Keller des alten Schulgebäudes.

Als Sofortmaßnahme wurde zunächst die Verwahrung der Akten in einer verschließbaren, ausgedienten Kühlzelle der Gemeinde veranlasst. Außerdem forderten wir die Amtsverwaltung sowie das zuständige staatliche Schulamt auf, den Bestand der Altakten vollständig zu erfassen und gemäß den Regeln der Verwaltungsvorschrift über Akten an Schulen im Land Brandenburg aufzubewahren bzw. im Falle einer abgelaufenen Aufbewahrungsfrist datenschutzgerecht zu entsorgen.

Schulakten müssen datenschutzgerecht aufbewahrt werden. Die Verwaltungsvorschrift über Akten an Schulen im Land Brandenburg muss auch beim Umgang mit alten Unterlagen im Falle der Schließung oder Zusammenlegung von Schulen beachtet werden.

18 Verkehr

18.1 Das Projekt INNOS – Einführung elektronischer Fahrscheine im Verkehrsverbund Berlin-Brandenburg

Mit dem Verkehrsprojekt INNOS sollen elektronische Tickets für den Verkehrsverbund Berlin-Brandenburg (VBB) in Form von RFID-Chipkarten eingeführt werden. Seit September 2011 läuft ein Praxistest für das E-Ticket mit einer begrenzten Anzahl freiwilliger Abonnementkunden. Ab Frühjahr 2012 soll schrittweise der Echtbetrieb für Abonnement- und Jahreskarteninhaber starten. Auf brandenburgischer Seite beteiligen sich die Verkehrsunternehmen in Potsdam, Brandenburg an der Havel und Frankfurt (Oder) sowie die Havelbus und die Oberhavel Verkehrsgesellschaft an dem Projekt.

Auf der Chipkarte werden nur solche Daten gespeichert, die auch jetzt bereits den entsprechenden Fahrkarten zu entnehmen sind. Bei den übertragbaren Zeitkarten sind das der Gültigkeitszeitraum und die Gültigkeitszonen, bei personengebundenen Karten der Name, ggf. das Geburtsdatum und der Kartentyp (z. B. Schülerticket). Auf der personengebundenen Karte kann zusätzlich ein Foto des Inhabers aufgebracht werden. Das Foto wird nur mit ausdrücklicher Zustimmung der Kunden in der Abonnentendatenbank gespeichert. Die Kunden können den Inhalt ihrer Chipkarte an speziellen Terminals der Verkehrsunternehmen auslesen und überprüfen.

Bei Einstieg in entsprechend ausgerüstete Verkehrsmittel (z. B. Busse) müssen die Kunden die Chipkarte an ein Kontrollterminal halten, das die Gültigkeit oder Ungültigkeit der Karte durch ein grünes oder rotes Licht und ein entsprechendes akustisches Signal bescheinigt. Auf dieselbe Weise werden die Karten bei einer Fahrscheinkontrolle mittels mobiler Lesegeräte durch das Kontrollpersonal überprüft. Während des Kontrollvorgangs werden keine personenbezogenen Daten übertragen oder in den Kontrollgeräten gespeichert.

Das bisherige Auswechseln der Wertmarken am Monatsende entfällt, da die Karte bei einem Dauerabonnement auch dauerhaft gültig bleibt, solange sie nicht gesperrt ist. Bei Kartenverlust können die Kunden die Chipkarte sperren lassen und erhalten gegen eine Gebühr eine neue Karte.

Die Listen mit den Nummern gesperrter Karten werden einmal täglich auf die Kontrollterminals der Busse und die Handgeräte des Kontrollpersonals übertragen. Die Sperrlisten enthalten außer den Kartennummern keine weiteren personenbezogenen Daten.

Die derzeit noch getrennten und unterschiedlichen Abonnementvertriebssysteme einiger Verkehrsunternehmen sollen durch ein gemeinsames, mandantenfähiges System eines zentralen Dienstleisters ersetzt werden, in dem jedes Unternehmen seine Kundendaten in einem eigenen Mandanten verarbeitet. Jedes Unternehmen muss einen Vertrag zur Auftragsdatenverarbeitung mit dem Dienstleister abschließen. Weiterhin sind jeweils IT-Sicherheitskonzepte für alle beteiligten Komponenten zu erstellen und umzusetzen, die die notwendigen technischen und organisatorischen Maßnahmen für die technische Infrastruktur, die Schnittstellen, die Speicherorte und Datenübertragungsstrecken und die Rollen und Berechtigungen von Benutzern und Administratoren enthalten. Da die Abonnementsysteme auch sensitive Kundendaten wie z. B. Bankdaten enthalten, sind Maßnahmen zu ergreifen, die dem hohen Schutzbedarf der Daten gerecht werden (wie z. B. eine Verschlüsselung in Datenbanken und bei der Datenübertragung). Darüber hinaus sind eine strikte Zweckbindung der Kundendaten und die Trennung der Daten zwischen den einzelnen Verkehrsunternehmen zu realisieren.

In dem gegenwärtigen Projekt INNOS werden keine Bewegungsdaten der Karteninhaber verarbeitet. Die Bildung von Bewegungsprofilen (wer ist wann mit welchem Verkehrsmittel wohin gefahren) ist deshalb nicht möglich.

Die Einführung von elektronischen Tickets im Verkehrsverbund Berlin-Brandenburg ist ein komplexes Projekt, das hohen datenschutzrechtlichen und sicherheitstechnischen Anforderungen genügen muss. Die Ausgestaltung der Chipkarten und Kontrollterminals erfüllt diese Anforderungen. Wir werden den Prozess weiter beratend begleiten.

18.2 Angaben zum Piloten im Hauptflugbuch

Ein Pilot beschwerte sich darüber, dass sein Name im elektronisch geführten Hauptflugbuch eines brandenburgischen Regionalflugplatzes auftauchte.

§ 70 Abs. 1 Luftverkehrsgesetz (LuftVG) enthält eine abschließende Auflistung jener Angaben, wie beispielsweise Daten zum Luftfahrzeug, zum Flug und zur Anzahl der Fluggäste und Besatzungsmitglieder, die im Hauptflugbuch zu speichern sind. Der Name des Piloten gehört nicht dazu. Auch der vom Betreiber des Flugplatzes angegebene Grund, prüfen zu wollen, ob gegen den verantwortlichen Piloten ein Strafverfahren wegen des Verstoßes gegen das Luftverkehrsgesetz einzuleiten ist, ändert nichts am Fehlen der Befugnis zur Speicherung des Namens im Hauptflugbuch. Eine Rechtsgrundlage ergibt sich auch nicht aus der Luftverkehrs-Ordnung. Die Speicherung darf daher nur mit dem Einverständnis des Betroffenen erfolgen.

Wir haben den Betreiber des Flugplatzes auf die Rechtslage hingewiesen und zur Löschung der Eintragung aufgefordert. Erst nach umfangreichen Diskussionen auch mit der zuständigen Luftfahrtaufsichtsbehörde kam der Betreiber dieser Forderung nach. Zusätzlich hat er nun eine Dienstanweisung erstellt, in der eine von § 70 Abs. 1 LuftVG abweichende Datenverarbeitung ausdrücklich untersagt wird. Die Kenntnisnahme dieser Anweisung war von allen Beteiligten per Unterschrift zu bestätigen. Außerdem wurde im elektronischen Hauptflugbuch softwareseitig das ursprüngliche Feld zur Eintragung des Pilotennamens gelöscht, um künftig auch versehentliche Eintragungen zu verhindern.

Die Namen der Piloten dürfen im elektronischen Hauptflugbuch nicht gespeichert werden. Um versehentliche Eintragungen zu verhindern, sollten die Namensfelder in der Software gelöscht werden.

19 Wirtschaft

19.1 Datenschutzrechtliche Zuständigkeit für das Unternehmen eBay

Immer wieder haben sich Nutzer der Internetangebote eBay, PayPal oder mobile.de mit datenschutzrechtlichen Fragen und Problemen an uns gewandt. Da es sich bei den Betreibern dieser Angebote um international tätige Unternehmen unter einem gemeinsamen Dach handelt, mussten wir zunächst die Zuständigkeit für die Datenschutzaufsicht prüfen.

Die eBay GmbH (Deutschand) mit Sitz und Handelsregistereintrag im Land Brandenburg ist im Zusammenhang mit dem Betrieb der Internetplattform www.ebay.de tätig. Eigentlicher Betreiber der Website und verantwortlicher Vertragspartner der deutschen und europäischen eBay-Nutzer ist jedoch die Firma eBay Europe S. à r. l. mit Sitz in Luxemburg. Die eBay GmbH (Deutschland) handelt, auch im Bereich der Datenverarbeitung, nur weisungsabhängig im Auftrag des luxemburgischen Unternehmens. Eine selbstständige Verarbeitung personenbezogener Daten findet in der deutschen Niederlassung nicht statt. Lediglich vorformulierte Standardantworttexte für häufig gestellte Fragen der eBay-Nutzer werden hier versandt. Auf Grundlage dieser Funktionszuweisungen innerhalb des eBay-Konzerns ergibt sich für die datenschutzrechtliche Aufsicht eine Zuständigkeit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg lediglich für den gesamten Arbeitnehmerdatenschutz in der Firma eBay GmbH (Deutschland), sowie eine Randzuständigkeit für die oben genannte Versen-

dung der Mustertexte für Standardanfragen. Die eigentliche Aufsichtspflicht für die datenschutzgerechte Verarbeitung der personenbezogenen Daten der eBay-Nutzer liegt bei der Nationalen Kommission für den Datenschutz (CNPD), der nationalen Datenschutzbehörde Luxemburgs. Diese ist zuständig für die Kontrolle der Datenverarbeitung im Zusammenhang mit dem Betrieb der Internetplattform www.eBay.de und die Bearbeitung von Anfragen und Beschwerden der Nutzer.

PayPal (Europe) S. à r. l. & Cie, S.C.A., das Tochter- und Serviceunternehmen der eBay-Gruppe mit Sitz in Luxemburg, das als Dienstleister bei der Zahlungsabwicklung der eBay-Kunden auftritt, verfügt mit der PayPal Deutschland GmbH über eine Niederlassung in Brandenburg. Hier findet jedoch auch keine relevante Verarbeitung personenbezogener Nutzerdaten statt, sodass eine Aufsichtsbefugnis der Landesbeauftragten nur insoweit gegeben ist, als Arbeitnehmerdaten betroffen sind. Es handelt sich bei der PayPal Deutschland GmbH um eine interne Unternehmensberatungsgesellschaft. Allein zuständig für datenschutzrechtliche Fragestellungen und Probleme der Nutzer aus Deutschland ist die CNPD in Luxemburg.

Die gleichfalls zum eBay-Konzern gehörende mobile international GmbH hat ihren Sitz im Land Brandenburg. Sie betreibt die Internetportale www.mobile.de, www.automobile.fr und www.automobile.it, die den Nutzern die Möglichkeit zum An- und Verkauf von Kraftfahrzeugen eröffnen. Die Firma verarbeitet selbstständig personenbezogene Daten von Nutzern der Internetportale sowie die Beschäftigtendaten ihrer Mitarbeiter. Sie ist damit verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes und unterliegt vollumfänglich dessen Regelungen. Dies bedeutet, dass die datenschutzrechtliche Aufsicht über die mobile international GmbH von der Landesbeauftragten wahrgenommen wird. Sie ist Ansprechpartnerin für Fragen und Probleme der Nutzer hinsichtlich der Verarbeitung ihrer personenbezogenen Daten beim Betrieb der Internetplattformen www.mobile.de, www.automobile.fr und www.automobile.it.

Für die Einhaltung des Datenschutzes bei den Internetangeboten von eBay und PayPal ist die luxemburgische Datenschutzbehörde zuständig. Die Landesbeauftragte übt die datenschutzrechtliche Aufsicht über die Angebote von mobile international aus.

19.2 Weitergabe von Adressdaten durch eine Stadtverwaltung?

Ein Unternehmen beabsichtigte, zur Vorbereitung von Verkaufsverhandlungen an eine Reihe von Grundstückseigentümern heranzutreten. Von der Stadtverwaltung erhielt es die Anschriften der Bürger eines ganzen Stadtteils und verschickte einen ausführlichen Fragebogen. Einige Einwohner beschwerten sich über die Weitergabe ihrer Daten durch die Stadt.

Die Adressdaten der Einwohner sind personenbezogene Daten, die nicht ohne Rechtsgrundlage weitergegeben werden dürfen. Eine solche lag jedoch nicht vor, sodass die Herausgabe der Anschriften unzulässig war. Das bedeutet jedoch nicht, dass die Stadt das Begehren des Unternehmens von vornherein hätte ablehnen müssen. Denkbar sind in solchen Fällen die drei folgenden Alternativen:

- Das Unternehmen verteilt die Fragebögen mithilfe eines Boten ohne Adressierung an sämtliche Haushalte. Dies kommt vor allem infrage, wenn, wie dies hier der Fall war, nur ein begrenztes Gebiet betroffen ist. Die Stadtverwaltung ist in einem solchen Verfahren nicht involviert; datenschutzrechtliche Fragen spielen dann bei der Zustellung der Fragebögen keine Rolle.

- Die Stadtverwaltung übernimmt den Versand der Fragebögen in eigener Regie, ohne die Adressdaten an das Unternehmen zu übermitteln („Adressmittlungsverfahren“). Letzteres stellt dabei die Fragebögen und die frankierten Kuverts zur Verfügung, die von der Verwaltung mit den Anschriften versehen und auf den Postweg gebracht werden. Aus den übersandten Unterlagen müssen die Adressaten erkennen können, dass ihre Daten nicht weitergegeben wurden.

- Nach § 32 Abs. 3 Brandenburgisches Meldegesetz kann die Stadtverwaltung eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) erteilten, wenn diese im öffentlichen Interesse liegt. Die Meldebehörde muss den Antrag aber zuvor dem Ministerium des Innern zur Feststellung des öffentlichen Interesses vorlegen.

Die Stadtverwaltung sagte zu, diese Hinweise in Zukunft zu berücksichtigen.

Aus dem Fragebogen muss deutlich hervorgehen, dass seine Beantwortung in jedem Fall freiwillig erfolgt und keine Auskunftspflicht für die Bewohner besteht. Dies gilt insbesondere im Fall einer Adressmittlung durch die Stadt-

verwaltung, da hier durch das Tätigwerden einer hoheitlichen Stelle leicht der gegenteilige Eindruck entstehen könnte. Die Fragebogenaktion ist zudem nur zulässig, wenn die Befragten ausdrücklich in die damit einhergehende Datenverarbeitung schriftlich einwilligen. Aus der Einwilligungserklärung nach § 4a Bundesdatenschutzgesetz muss eindeutig zu erkennen sein, zu welchem Zweck die Daten erhoben und in welcher Weise sie genutzt werden. Die Erklärung kann in den Fragebogen integriert werden. Unzulässig ist es, durch die Fragen Angaben zu Dritten – beispielsweise zu Mietern oder weiteren im Haushalt lebenden Personen – zu erfragen. Solche personenbezogenen Daten dürfen ausschließlich bei den Betroffenen selbst erhoben werden.

Die Herausgabe von Adressdaten ist nur zulässig, wenn hierfür eine Rechtsgrundlage besteht. Das Brandenburgische Meldegesetz erlaubt zwar eine Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner – dies setzt aber voraus, dass das Ministerium des Innern hierfür ein öffentliches Interesse feststellt.

19.3 Erfassung der Wohnungstemperatur per Funk?

Ein Mieter erkundigte sich nach der Zulässigkeit des Funkabrufs und der Verarbeitung von Heizmessdaten aus seiner Wohnung. Dabei ging es um ein System, das die Innentemperatur der Wohnräume per Funk übermittelt und unter Berücksichtigung der Außentemperatur den Energiebedarf des Gebäudes errechnet.

Wir haben den Betreiber des Erfassungssystems – einen vom Vermieter beauftragten Dienstleister – gebeten, zu dem Sachverhalt Stellung zu nehmen. Er erläuterte zwei voneinander unabhängige Verfahren zur Datenverarbeitung: die Ermittlung des Wärmebedarfs zwecks Energieeinsparung und die Verbrauchsabrechnung.

Mit dem Ziel, Energie einzusparen, wird der Wärmebedarf eines Gebäudes ermittelt. Die Heizkostenverteiler in den einzelnen Wohnungen messen dort zunächst die Raumtemperatur sowie die Oberflächentemperatur der Heizkörper. Per Funkabruf werden diese Angaben an eine technische Vorrichtung übertragen, die den gesamten Zustand der Wärmeversorgung eines Gebäudes errechnet. Den sich daraus ergebenden Korrekturwert überträgt diese Vorrichtung an ein Modul, das die Vorlauftemperatur der Heizung entsprechend dem Wärmebedarf anpasst. Beide Geräte verarbeiten keine personenbezogenen Daten – die Temperaturangaben lassen sich nicht einer einzelnen Wohnung zuordnen.

Darüber hinaus wird der Energieverbrauch für Zwecke der Abrechnung erfasst. Die so erfassten Verbrauchsdaten beziehen sich auf die einzelnen

Wohneinheiten und sind somit personenbezogen. Sie werden einmal täglich verschlüsselt an das Rechenzentrum des Dienstleisters übertragen und am Ende des Abrechnungszeitraums addiert. Diese individuellen Verbrauchsdaten dienen ausschließlich der Abrechnung und werden nicht für andere Zwecke verwendet.

Aus datenschutzrechtlicher Sicht ist dieses Verfahren nicht zu beanstanden. § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz erlaubt dem Vermieter die Verarbeitung personenbezogener Daten, soweit dies zur Begründung, Durchführung oder Beendigung des bestehenden Mietverhältnisses erforderlich ist. Unter der Voraussetzung, dass die Zweckbindung der erhobenen Daten eingehalten wird, gilt dies auch für einen vom Vermieter beauftragten Dienstleister. Die anteilige Erfassung des Verbrauchs wird zudem durch die Verordnung über die verbrauchsabhängige Abrechnung der Heiz- und Warmwasserkosten (Heizkostenverordnung) vorgeschrieben. Dabei obliegt die Auswahl der Geräte zur Verbrauchserfassung dem Gebäudeeigentümer – davon ist grundsätzlich auch die im vorliegenden Fall gewählte Funkübertragung der Messdaten umfasst.[55] Aus Gründen der Transparenz sollten die Mieter vor der Einrichtung eines solchen Systems umfassend über die Datenverarbeitung informiert werden.

Die funkgestützte Übertragung von Temperaturmesswerten zwecks Wärmeregulierung von Gebäuden ist datenschutzrechtlich unproblematisch, solange kein Bezug zu einzelnen Wohnungen hergestellt werden kann. Die Funktionsweise des Messsystems sollte den Mietern möglichst frühzeitig erläutert werden.

20 Wissenschaft

20.1 Wählerverzeichnis der Studierenden im Internet?

Zur Durchführung von Wahlen der Gremien der akademischen Selbstverwaltung sind die Wählerverzeichnisse der Studierenden in den jeweiligen Hochschulen auszulegen. Ein studentisches Gremienmitglied machte uns darauf aufmerksam, dass Mitarbeiter des Wahlbüros einer Hochschule die Angaben aus dem Verzeichnis allgemein zugänglich ins Internet gestellt hatten.

Die einschlägigen Wahlordnungen schreiben das hochschulöffentliche Auslegen der Wählerverzeichnisse zur Durchführung der Wahlen zu den Gremien

[55] vgl. Urteil des Bundesgerichtshofs vom 28. September 2011, VIII ZR 326/10

der akademischen Selbstverwaltung vor. Studierende können sich vergewissern, dass sie der richtigen Hochschuleinrichtung zugeordnet sind. Nur mit diesem Wissen können sie dann ihr Wahlrecht wahrnehmen. Die Angaben umfassen neben Namen und Matrikelnummern auch Angaben zur Semesterzahl und Studienrichtung und damit schutzbedürftige personenbezogene Daten. Das Einstellen der Verzeichnisse ins Internet ist deshalb nicht zulässig.

Durch die zügige Reaktion der Hochschulverwaltung wurde die Zugriffsmöglichkeit nach ihrem Bekanntwerden unverzüglich beseitigt. Die Hochschule hat zur Vermeidung künftiger Fehler dieser Art Vorkehrungen getroffen, die Mitarbeiter des Wahlamts eingehend belehrt und zugesagt, datenschutzrechtliche Schulungen durchzuführen.

Hochschulinterne Wählerverzeichnisse dürfen nicht im Internet veröffentlicht werden.

20.2 Das Projekt-Portal im Deutschen Biobanken-Register

Das Fraunhofer-Institut für Biomedizinische Technik in Potsdam (Fraunhofer IBMT) bat uns um eine datenschutzrechtliche Prüfung des geplanten Projekt-Portals im Deutschen Biobanken-Register.

In Biobanken wird biologisches Material wie beispielsweise Körperflüssigkeiten oder Gewebeproben aufbewahrt. Diesen Stoffen sind sensitive medizinische Daten der Spender dieser Proben zugeordnet, zum Beispiel Angaben zu Krankheiten oder Lebensgewohnheiten. Solche Biobanken werden dezentral geführt – vor allem in Universitätskliniken und ähnlichen Einrichtungen.

Ziel des Projekt-Portals im Deutschen Biobanken-Register ist es, Meta-Informationen zu diesen Proben zusammenzuführen. Die Proben selbst bleiben in den Kliniken vor Ort, das Portal bietet lediglich strukturierte Informationen über die Standorte und Art der dezentralen Probenbestände an. Dies soll den Forschern die Auffindbarkeit der Proben und den Kliniken die Akquise von Forschungsprojekten erleichtern. Redundante Forschungsprojekte sollen dadurch vermieden werden. Das von dem Fraunhofer IBMT betriebene Projekt-Portal ist in das Deutsche Biobanken-Register der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) integriert. Projektpartner sind verschiedene Biobanken.

Die Plattform stellt lediglich eine Vermittlungsstelle zwischen Forschern und den eigentlichen Biobanken dar und ermöglicht eine Online-Suche nach Proben, Partnern und Forschungsprojekten. Soweit sie die Proben anonym,

d. h. ohne Bezug zu den Spendern, beschreibt und lediglich auf ihren Standort verweist, bestehen gegen dieses Vorhaben keine datenschutzrechtlichen Bedenken. Die datenschutzrechtliche Verantwortung der Biobanken für den Umgang mit den Angaben zu den Spendern der Proben bleibt vom Aufbau des Projekt-Portals unberührt.

Ein Vermittlungsportal, das lediglich auf den Standort von Gewebeproben hinweist, greift nicht in das Recht der Spender auf informationelle Selbstbestimmung ein.

Teil B

Akteneinsicht und Informationszugang

1 Entwicklung der Informationsfreiheit

1.1 Untätigkeit der Landesregierung?

In ihrem letzten Tätigkeitsbericht[56] bemängelte die Landesbeauftragte unter anderem die zunehmende Rechtszersplitterung der Regelungen zum Informationszugang. In ihrer Stellungnahme[57] zum Tätigkeitsbericht vertrat die Landesregierung im Hinblick auf die höchst unterschiedliche Ausgestaltung der einzelnen Informationszugangsrechte die Auffassung, dass diese unbefriedigende Situation auch künftig hinzunehmen sei. Insbesondere die Zusammenführung des Akteneinsichts- und Informationszugangsgesetzes mit dem Umweltinformationsgesetz führe – „bei Anerkennung teilweise unterschiedlicher Interessenlagen“ – nicht zu einem handhabbaren Ergebnis, wie ein entsprechender Versuch, der gescheitert war, zeige. Dieser Feststellung ist zwar grundsätzlich zuzustimmen. Keine Anerkennung finden hier jedoch die von der Landesregierung genannten unterschiedlichen Interessenlagen. Dies würde bedeuten, dass Transparenz mit zweierlei Maß gemessen wird: Dort, wo das Land verpflichtet ist, transparenzfreundliches, europäisches Recht umzusetzen (Umweltinformationsrecht), wird ein Mehr an Informationsfreiheit umgesetzt, dort, wo es eine eigene Regelungskompetenz hat (Akteneinsichts- und Informationszugangsgesetz), bleibt es trotz einer verfassungsrechtlichen Verankerung bei seinen restriktiven Vorschriften.

Unabhängig von ihrer Einschätzung zur Rechtszersplitterung teilte die Landesregierung jedoch mit, dass vorgesehen sei, das Akteneinsichts- und Informationszugangsgesetz zu novellieren und mit den Vorarbeiten bereits begonnen worden sei. Unter anderem sei eine Abfrage im Bereich der Landesregierung zu einem möglichen Änderungsbedarf an den Regelungen durchgeführt worden. Anlässlich eines Gesprächs zwischen dem Ministerium des Innern und der Landesbeauftragten im Frühjahr 2010 zeigte sich, dass seitens der Regierung durchaus die Notwendigkeit einer Novellierung gesehen wird, wenn auch in geringerem Maße als von der Landesbeauftragten empfohlen. Rückäußerungen der befragten Ressorts seien bereits eingegan-

---

56 vgl. Tätigkeitsbericht 2008/2009, B 2.2, B 2.3

57 vgl. Stellungnahme der Landesregierung zum Tätigkeitsbericht für die Jahre 2008 und 2009 der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, Landtags-Drucksache 5/1804 vom 13. August 2010

gen; die weitere Einbindung der Landesbeauftragten wurde zugesichert. Bereits im Herbst 2010 teilte das Ministerium mit, die in Aussicht gestellte Vorbereitung der Novellierung könne im laufenden Jahr nicht mehr in Angriff genommen werden. Im Dezember 2010 fasste der Landtag dann einen Beschluss,[58] mit dem die Landesregierung aufgefordert wird, im Zuge der Novellierung des Akteneinsichts- und Informationszugangsgesetzes darin einen ausdrücklichen Rechtsanspruch zur Herausgabe von Kopien zu verankern. Ein ähnlich lautender Beschluss war zum Ende der letzten Legislaturperiode der Diskontinuität anheimgefallen.

Das Land Brandenburg war mit seiner fortschrittlichen Verfassung aus dem Jahre 1992, die als erste und noch immer einzige in der Bundesrepublik Deutschland ein Akteneinsichtsrecht enthält, Vorreiter auf dem Gebiet der Informationsfreiheit. Sechs Jahre später verabschiedete der Landtag dann das Akteneinsichts- und Informationszugangsgesetz – wiederum das erste seiner Art in Deutschland. Erst im Jahre 2005 hat der Gesetzgeber auf Bundesebene das Informationsfreiheitsgesetz auf den Weg gebracht. Auch zehn Länder gaben sich Informationsfreiheitsgesetze. Die meisten Gesetzgeber sind bei ihren Regelungen von denen der anderen Länder abgewichen. Sie konnten von deren Erfahrungen profitieren, bewährte Regelungen übernehmen und Ergänzungen vornehmen. Der ehemalige brandenburgische Pionier – das Akteneinsichts- und Informationszugangsgesetz – wurde über die Jahre seines Bestehens hingegen kaum verbessert. Als Beispiel, von dem andere profitieren könnten, dient es deshalb schon lange nicht mehr. Die Musik spielt inzwischen auf anderen Bühnen.

1.2 Europa, Bund und Länder

Um grundsätzlich alle amtlichen Dokumente in den Mitgliedstaaten, die keinem berechtigten Schutzbedarf unterliegen, öffentlich zugänglich zu machen, hat der Ministerausschuss des Europarats bereits im Jahre 2008 eine entsprechende Konvention beschlossen. Diese Vereinbarung würde die Vertragsstaaten verpflichten, ein voraussetzungsloses Recht auf Informationszugang zu gewähren und bestehende Informationszugangsregelungen gegebenenfalls zu erweitern. Voraussetzung für das In-Kraft-Treten der Konvention ist die Ratifizierung durch die Vertragsstaaten. Die Bundesrepublik Deutschland hat sich bislang nicht einmal zur Unterzeichnung entschließen können. Hintergrund sind nicht zuletzt Bedenken einiger Länder. Brandenburg plädierte beispielsweise dagegen, weil es unter anderem mit der in der Konvention vorgesehenen Kostenfreiheit für den Informationszugang nicht einverstanden war.

[58] vgl. Beschluss des Landtages Brandenburg vom 17. Dezember 2010, Landtags-Drucksache 5/2409-B

Durch das In-Kraft-Treten des Vertrags von Lissabon ist die Charta der Grundrechte zu einem rechtsverbindlichen Instrument geworden. Das Recht auf Zugang zu Dokumenten ist darin verankert. Es gilt sowohl gegenüber den Organen und Einrichtungen der Union als auch gegenüber den Mitgliedsstaaten, soweit sie EU-Rechtsvorschriften umsetzen. Auch der Vertrag über die Arbeitsweise der Europäischen Union enthält eine entsprechende Transparenzverpflichtung. Die Verordnung, in der Einzelheiten hierzu geregelt sind, wird gegenwärtig einer Überprüfung unterzogen.

Auch auf Bundesebene wird über Verbesserungen des Informationsfreiheitsgesetzes nachgedacht. Der Innenausschuss des Deutschen Bundestags hat dem Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer den Auftrag zur Bewertung des Gesetzes erteilt. Die Evaluation soll im Frühjahr 2012 abgeschlossen sein. Ein vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Auftrag gegebenes Gutachten empfiehlt ausdrücklich die Einführung von Abwägungsklauseln bei Betriebs- und Geschäftsgeheimnissen.

Im Koalitionsvertrag haben die Parteien der Bundesregierung angekündigt, Informationsansprüche des Bürgers in einem einheitlichen Gesetz regeln zu wollen. Im Dezember 2010 präsentierten Netzwerk Recherche e. V., Greenpeace e. V. und die Deutsche Gesellschaft für Informationsfreiheit e. V. den Entwurf für ein Bürgerinformationsgesetz. Er fasst die im Informationsfreiheitsgesetz des Bundes, im Verbraucherinformationsgesetz und im Umweltinformationsgesetz verstreuten Regelungen zusammen und erweitert den Informationsanspruch auf Unterlagen von Unternehmen, die für die öffentliche Hand tätig sind. Dieser Verbändeentwurf für ein Modellgesetz zeigt deutlich: Wo ein Wille ist, ist auch ein Weg. Nachdem die Koalitionsparteien in Kiel die Zusammenfassung des Umweltinformationsgesetzes und des Informationsfreiheitsgesetzes vereinbart hatten, wird derzeit im schleswig-holsteinischen Landtag ein entsprechender Gesetzentwurf diskutiert. In Nordrhein-Westfalen gab das Innenministerium ein Gutachten in Auftrag, das die Möglichkeiten zur Schaffung eines einheitlichen Informationszugangsgesetzes des Landes ausloten sollte. Die beauftragte Forschungsgruppe hielt eine solche Kodifikation der verstreut geregelten Informationsrechte und Parallelregelungen grundsätzlich für möglich und sinnvoll.

In zahlreichen Bundesländern, die über ein Informationsfreiheitsgesetz verfügen, konnten sich im Berichtszeitraum Verbesserungen durchsetzen. Das Berliner Informationsfreiheitsgesetz wurde durch eine erfolgreiche Volksabstimmung um Sonderregelungen für die Offenlegung von Verträgen der öffentlichen Grundversorgung ergänzt. Die Gesetzgeber im Saarland und in Mecklenburg-Vorpommern kamen im Rahmen von Evaluationen zum Ergebnis, dass sich die dortigen Informationsfreiheitsgesetze bewährt haben und

verlängerten deren Geltung. Darüber hinaus hat die Bremische Bürgerschaft das Bremer Informationsfreiheitsgesetz um ein Abwägungserfordernis beim Vorliegen von Betriebs- und Geschäftsgeheimnissen, um eine Vorschrift zur Offenlegung von Verträgen über die Daseinsvorsorge sowie um Regelungen zur aktiven Veröffentlichung von Informationen ergänzt. Rheinland-Pfalz verfügt zwar seit dem Jahre 2009 über ein Informationsfreiheitsgesetz, hatte hierfür aber ebenso wie der Freistaat Thüringen keinen Beauftragten vorgesehen. Der rheinland-pfälzische Landtag verabschiedete eine Gesetzesänderung, nach der nunmehr auch in Mainz der Datenschutzbeauftragte mit der Wahrung des Rechts auf Informationszugang betraut wird. Die Ergebnisse einer darüber hinausgehenden wissenschaftlichen Evaluation des Informationsfreiheitsgesetzes Rheinland-Pfalz sollen im Jahre 2012 vorliegen. Die Koalitionäre der Thüringer Landesregierung haben vereinbart, das Informationsfreiheitsgesetz zu evaluieren, die Informationsfreiheitsrechte zu stärken und die Aufgaben des Thüringer Datenschutzbeauftragten ebenfalls um die Funktion eines Informationsfreiheitsbeauftragten zu erweitern. Die Regierungsparteien in Baden-Württemberg haben sich zur Schaffung eines Informationsfreiheitsgesetzes bekannt. So weit ist es im Freistaat Bayern zwar noch nicht. Auch dort zeigt sich jedoch sehr deutlich, wie groß der Bedarf an einer entsprechenden Regelung ist: Während seitens des Landesgesetzgebers keine Initiative zu erkennen ist, haben inzwischen etliche Kommunen, darunter auch große Städte wie München, Nürnberg oder Regensburg, für ihren eigenen Wirkungskreis eine Informationsfreiheitssatzung erlassen. Dasselbe gilt auch für die niedersächsische Stadt Göttingen. Auch in hessischen und baden-württembergischen Kommunen wird diskutiert, die Informationsfreiheit „von unten“ zu fördern.

1.3 Verbraucherinformationen, Agrarsubventionen und Geodaten

Nach den ersten Erfahrungen mit dem seit dem Jahre 2008 geltenden Verbraucherinformationsgesetz erfolgte eine umfangreiche Evaluation. Im Ergebnis ihrer Auswertung brachte die Bundesregierung im Oktober 2011 einen Gesetzentwurf zur Novellierung ein, der mit einigen Veränderungen am 2. Dezember 2011 vom Deutschen Bundestag verabschiedet wurde. Das Ergebnis der Befassung des Bundesrates mit dem Entwurf steht noch aus. Das novellierte Gesetz stärkt die Informationsrechte der Verbraucher in wesentlichen Punkten: Der Informationsanspruch wird auf technische Verbraucherprodukte wie Haushaltsgeräte, Heimwerkerartikel oder Möbel ausgedehnt. Außerdem werden die Anhörungsverfahren gestrafft. Die Berufung auf Betriebs- und Geschäftsgeheimnisse ist künftig nicht mehr möglich, wenn bestimmte amtliche Kontrollergebnisse erfragt werden oder das öffentliche Interesse an der Herausgabe überwiegt. Gebühren für einfache Anfragen

entfallen; entsteht durch einen Antrag auf Verbraucherinformationen ein höherer Verwaltungsaufwand, muss die Behörde stets einen Kostenvoranschlag erstellen. Durch eine Ergänzung des Lebensmittel- und Futtermittelgesetzbuches werden die Behörden zudem verpflichtet, alle Rechtsverstöße durch Grenzwertüberschreitungen zu veröffentlichen. Nachdem in einem Modellprojekt des Berliner Stadtbezirks Pankow erste Erfahrungen mit dem so genannten „Smiley-System“ gewonnen werden konnten, befürworteten die Verbraucherschutzminister des Bundes und der Länder im Berichtszeitraum eine bundesweit einheitliche Veröffentlichung von Hygienestandards in Restaurants.

Im letzten Tätigkeitsbericht[59] haben wir ausführlich über die europarechtlich vorgeschriebene Veröffentlichung der Empfänger von Agrarsubventionen im Internet berichtet. Der Europäische Gerichtshof hat inzwischen die vollständige Veröffentlichung gestoppt und damit der Klage zweier Landwirte, die Datenschutzrechte geltend gemacht hatten, stattgegeben. Im Wesentlichen bemängelte das Gericht, dass durch die pauschale Veröffentlichung der Daten zu natürlichen Personen (Einzellandwirte) unzulässigerweise in deren Persönlichkeitsrechte eingegriffen werde und verlangte für die künftige Praxis eine Differenzierung. Weiterhin uneingeschränkt zulässig ist hingegen die Veröffentlichung von Empfängern, die als juristische Personen auftreten (Unternehmen). Die Bundesregierung hat die Veröffentlichung zunächst vollständig ausgesetzt; inzwischen sind die Daten zu juristischen Personen wieder einsehbar. Eine Neuregelung für den Umgang mit personenbezogenen Daten bleibt noch abzuwarten. Im Ergebnis aber bleibt es dabei: Jeder soll konkret erfahren können, wofür immerhin vierzig vom Hundert der EU-Haushaltsmittel ausgegeben werden.

Zur Umsetzung der Richtlinie zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft in nationales Recht traten bereits im Jahre 2009 das Geodatenzugangsgesetz des Bundes und im Jahre 2010 das brandenburgische Geodateninfrastrukturgesetz in Kraft. Ziel der Richtlinie ist es, die grenzübergreifende Nutzung von Geodaten in Europa zu erleichtern und dadurch vorausschauende Planungen und Maßnahmen zum Beispiel auf dem Gebiet des Umwelt- oder Katastrophenschutzes leisten zu können. Hierfür soll nicht nur eine Infrastruktur zur Bereitstellung von Geodaten aufgebaut, sondern auch deren schnelle und einfache Zugänglichkeit gewährleistet werden. Dabei ist der Schutz öffentlicher und sonstiger Belange zu berücksichtigen; Gebühren können erhoben werden. Das Land Brandenburg bietet inzwischen mit seinem Geoportal Brandenburg einen zentralen Zugang auf dezentral – nicht zuletzt auch kommunal – geführte Geodatenbestände an.

---

59 vgl. Tätigkeitsbericht 2008/2009, B 1

1.4 Open Data

Die aktive, nicht durch den Antrag eines Bürgers veranlasste Veröffentlichung von Informationen durch staatliche Stellen wird inzwischen auf vielen Gebieten diskutiert. In der Debatte geht es nicht mehr nur um Verbraucherinformationen, Angaben zu Agrarsubventionsempfängern oder Geodaten. Vielmehr wird der Bedarf an einem übergreifenden Informationsangebot zunehmend deutlich. Mit dem Ansatz „Open Data“ finden zahlreiche Initiativen aus unterschiedlichen Richtungen einen gemeinsamen Nenner. Dieses Konzept, das auf nicht personenbezogene Informationen beschränkt ist, sieht vor, dass Daten der öffentlichen Hand für jedermann frei und in technisch standardisierter und maschinenlesbarer Form zur Verfügung gestellt werden. Nachdem beispielsweise in den Vereinigten Staaten von Amerika oder im Vereinigten Königreich von Großbritannien und Nordirland bereits Open-Data-Plattformen im Internet erfolgreich eingerichtet wurden, findet Open Data auch auf europäischer Ebene allmählich Eingang in Verwaltungspraxis und Gesetzgebung: Im Rahmen der Digitalen Agenda – einer Leitinitiative der Kommission zur Förderung des sozialen und wirtschaftlichen Potenzials des digitalen Binnenmarktes – soll der Anwendungsbereich der bestehenden Richtlinie zur Weiterverwendung von Informationen des öffentlichen Sektors ausgeweitet werden. Die Kommission beabsichtigt zudem, die Richtlinie dergestalt zu novellieren, dass künftig Daten der öffentlichen Hand in einfach zu nutzenden Formaten und möglichst kostenlos bereitgestellt werden müssen sowie grundsätzlich für beliebige Zwecke verwendet werden können. Zur Durchsetzung dieser Grundsätze soll eine behördliche Aufsicht geschaffen werden. Bislang zielte die Richtlinie vor allem auf die Nutzung öffentlicher Daten durch die Wirtschaft und beschränkte sich darauf, die Einheitlichkeit von Gebühren und die Diskriminierungsfreiheit bei der Lizenzvergabe zu regeln. Die Kommission plant darüber hinaus ein Datenportal, das Zugang zu den Daten der Europäischen Kommission ermöglicht und fordert die Mitgliedstaaten auf, sich an der Entwicklung eines gesamteuropäischen Portals zu beteiligen. Bereits jetzt halten die Organe der Europäischen Union öffentliche Register auf ihren Webseiten bereit.

Die Bundesrepublik befindet sich beim Thema Open Data noch in einer Orientierungsphase. Der IT-Planungsrat – ein Steuerungsgremium für die Anwendung der Informations- und Kommunikationstechnik in der öffentlichen Verwaltung – hat beschlossen, die Transparenz des Regierungs- und Verwaltungshandelns durch Informationstechnik und E-Government stärker zu fördern. Das Regierungsprogramm „Vernetzte und transparente Verwaltung“ nennt als Ziel, bis zum Jahre 2013 eine gemeinsame Strategie für ein offenes Regierungshandeln zu erarbeiten und umzusetzen, um einen einfachen Zugang zu den Informationen zu ermöglichen. In der Freien Hansestadt Bremen wird der Open-Data-Grundsatz bereits praktiziert: Auf der Grundlage

einer gesetzlichen Verpflichtung im Bremer Informationsfreiheitsgesetz muss die Verwaltung wichtige Dokumente in einem zentralen Informationsregister im Internet allgemein zugänglich machen.

1.5 Konsequenzen für Brandenburg

Seit der Verabschiedung des brandenburgischen Akteneinsichts- und Informationszugangsgesetzes im Jahre 1998 hat sich die Welt der Informationsfreiheit grundlegend gewandelt. Die Änderung der Rahmenbedingungen und die Anforderungen an die Informationsfreiheit sind auch an Brandenburg nicht vorbeigegangen. Dabei spiegelt die oben beschriebene, dynamische Entwicklung sowohl der Zugangsrechte als auch der Verwaltungspraxis lediglich die beiden Jahre des Berichtszeitraums wider. Das Akteneinsichts- und Informationszugangsgesetz muss dringend und umfassend novelliert werden, um Brandenburg in Sachen Transparenz von den hinteren Rängen wieder auf eine vordere Position zu bringen. Einem Antragsteller ist es kaum zu vermitteln, dass er während des laufenden Verfahrens oder im Falle der Ausübung einer Aufsicht durch eine übergeordnete Stelle – also dann, wenn es am interessantesten ist – keinen Anspruch auf Informationszugang hat oder dass ihm kein ausdrücklicher Rechtsanspruch auf Fotokopien der von ihm eingesehenen Papiere zusteht, auch wenn er bereit ist, die Auslagen zu ersetzen. Das Gesetz fragt nicht danach, ob sich ein Antrag auf Akteneinsicht auf Unterlagen richtet, die im Zusammenhang mit der Erledigung einer öffentlichen Aufgabe entstanden sind, sondern beschränkt sich schlicht auf die „klassischen“ Behörden. Zahlreiche andere öffentliche Einrichtungen sowie in öffentlichem Eigentum oder unter öffentlicher Kontrolle stehende Unternehmen werden von der Informationsfreiheit in Brandenburg gar nicht erst erfasst. Ob Unternehmensdaten herausgegeben werden können, hängt im Wesentlichen von der Zustimmung des Unternehmers ab. Erteilt er sie nicht, muss die Behörde die Information geheim halten, auch wenn ihr Bekanntwerden nicht im Geringsten geeignet wäre, die wirtschaftlichen Interessen des Unternehmens zu beeinträchtigen. Verträge, mittels derer öffentliche Stellen sich bei der Wahrnehmung ihrer Aufgaben häufig privater Unternehmen bedienen, sind daher in Brandenburg zumeist Geheimverträge. Eine Abwägungsklausel, die dazu beitragen würde, einen angemessenen Ausgleich zwischen dem Einsichtsinteresse der Öffentlichkeit und dem öffentlichen oder privaten Geheimhaltungsinteresse zu erzielen, fehlt in weiten Teilen des Gesetzes ebenso wie ein Gebot zur aktiven Veröffentlichung von Informationen.

In ihrem täglichen Kontakt zu Antragstellern, die sich über die Verweigerung des Informationszugangs beschweren, muss die Landesbeauftragte häufig darauf hinweisen, dass die Behörden gar nicht anders können, als den Antrag abzulehnen. Verständliche Frustrationen – „Wozu ist das Gesetz eigent-

lich da?“ – sind das Ergebnis. Ebenso wenig wie die brandenburgischen Amtsstuben nach In-Kraft-Treten des Akteneinsichts- und Informationszugangsgesetzes im Jahre 1998 unter einem befürchteten Ansturm der Antragsteller zusammenbrachen, wird die Verwaltung heute kollabieren, wenn eine Novellierung die Informationszugangsrechte der Bürger stärkt. Im Gegenteil: das Vertrauen und die Akzeptanz von Verwaltungshandeln steigen im selben Maße wie die Transparenz der Behörden.

2 Schwerpunkte der Beschwerden über verweigerte Akteneinsicht

Repräsentative Aussagen zum Stand der Informationsfreiheit in Brandenburg sind nicht möglich, da die informationspflichtigen Stellen keinerlei Berichts- oder Statistikpflicht unterliegen. Unsere Rückschlüsse ergeben sich daher aus jenen Fällen, die in Form von Anfragen oder Beschwerden an die Landesbeauftragte herangetragen wurden. Dabei handelt es sich nur um einen vergleichsweise kleinen Ausschnitt der gesamten Situation, der aus unserer Sicht jedoch geeignet ist, Tendenzen in der Praxis der Informationsfreiheit im Land Brandenburg einzuschätzen.

Seitdem das Akteneinsichts- und Informationszugangsgesetz im Jahre 1998 in Kraft trat, hat sich in den meisten Verwaltungen ein routinierter Umgang mit Anträgen auf Akteneinsicht eingestellt. Die anfangs zu verzeichnende Aufregung – „Da kann ja jeder kommen!“ – ist einer sachlichen Prüfung der Anträge gewichen. Im Großen und Ganzen ist festzustellen, dass die Qualität der Entscheidungen auf allen Verwaltungsebenen in den vergangenen Jahren deutlich zugenommen hat. Aufgefallen sind uns darüber hinaus folgende Trends:

- Die Zahl der Beschwerden bei der Landesbeauftragten ist im Berichtszeitraum ungeachtet der von uns beobachteten Verbesserung der Qualität der Bearbeitung durch die öffentlichen Stellen wesentlich gestiegen. Dies mag damit zusammenhängen, dass die Informationsfreiheit gerade in den beiden zurückliegenden Jahren häufig Eingang in aktuelle Schlagzeilen gefunden hat. Beispielhaft seien die Debatte um WikiLeaks, der erfolgreiche Volksentscheid zur Offenlegung der „Wasserverträge“ und der Wahlerfolg der Piratenpartei im Nachbarland Berlin oder wegweisende Entscheidungen verschiedener Gerichte zur Informationsfreiheit genannt. Möglicherweise stellte dies einen Anlass auch für die Nutzung des brandenburgischen Akteneinsichts- und Informationszugangsgesetzes dar.

- Gleichzeitig war aber insbesondere im Jahr 2011 zu beobachten, dass vergleichsweise weniger Eingaben zu einem von den Antragstellern erwünschten Erfolg führten. Im Gegenteil stellten wir häufiger als zuvor fest, dass die Behörden den Informationszugang zumindest im Ergebnis zu Recht ablehnten. Ob es sich dabei um einen statistischen Einmaleffekt oder einen verlässlichen Trend handelt, werden die nächsten Jahre zeigen.

- In den seltensten Fällen genügt ein kurzer Blick ins Gesetz, um über Informationszugangsanträge entscheiden zu können – zunächst stellt sich nämlich die Frage, in welches Gesetz man schauen soll. Unsicherheiten aufgrund der Rechtszersplitterung im Informationsfreiheitsrecht führen dazu, dass Anträge oft auf der falschen Rechtsgrundlage bearbeitet werden und mit fehlerhaften Ergebnissen über Informationsbegehren entschieden wird.

- Den weitaus größten Anteil der Einsichtsbegehren, mit denen wir uns im Rahmen der Beratung und Bearbeitung von Beschwerden befassen, richtet sich auf Unterlagen aus dem Bau- und Planungswesen. Sowohl klassische Baugenehmigungen als auch unterschiedliche Aspekte der Flächennutzungs- und Verkehrsplanung stehen offenbar im Mittelpunkt des Interesses sehr vieler Antragsteller. Aber auch Informationen über andere umweltrelevante Maßnahmen öffentlicher Stellen werden häufig nachgefragt. Überschneidungen mit dem Umweltinformationsrecht treten hier naturgemäß am deutlichsten zutage.

- Im Berichtszeitraum häuften sich erneut Beschwerden und Anfragen zur Geheimhaltung unternehmensbezogener Daten. Zumeist interessierten sich Bürger in solchen Fällen für Vereinbarungen öffentlicher Stellen mit privaten Unternehmen. Auch wenn Betriebs- und Geschäftsgeheimnisse dabei gar keine Rolle spielten, stellt das Akteneinsichts- und Informationszugangsgesetz die Offenlegung beispielsweise von Verträgen weitgehend in das Belieben des betroffenen Unternehmens.

- Angestiegen ist die Zahl jener Fälle, in denen wir die Kostenerhebung für den Informationszugang zu prüfen hatten. Strittig waren dabei sowohl die Berechnung der Gebührenhöhe als auch die richtige Wahl der Rechtsgrundlage. Letzteres betraf im Wesentlichen kommunale Verwaltungen, die entweder nicht über eine entsprechende Kostensatzung verfügten oder deren Satzung nicht den Anforderungen des Akteneinsichts- und Informationszugangsgesetzes entsprach. Das durch dieses Gesetz vorgegebene Erfordernis einer nicht abschreckenden Kostenerhebung ist gerade auf kommunaler Ebene von besonderer Bedeutung, weil dort die überwiegende Zahl der Anträge auf Akteneinsicht gestellt wird.

- Einfache Verfahrensfehler stehen einem rechtzeitigen und vollständigen Informationszugang in der Praxis oft entgegen. Deutlich wird das vor allem bei Überschreitungen der maximalen gesetzlichen Bearbeitungsfrist. Aber auch die fehlerhafte Erstellung von Bescheiden und die unzureichende Begründung der Ablehnung von Anträgen auf Akteneinsicht sind scheinbar kleine Ärgernisse, die eine große, negative Wirkung zeitigen. Die überwiegende Mehrzahl der uns bekannt gewordenen Verfahrensfehler könnte durch eine sorgfältige Bearbeitung ohne großen Aufwand vermieden werden.

Antragstellern, die sich nach den Erfolgsaussichten eines Antrags auf Akteneinsicht erkundigen möchten oder eine Überprüfung der Ablehnung eines solchen Antrags wünschen, können sich jederzeit kostenfrei an die Landesbeauftragte wenden. Verwaltungen, die einen Antrag auf Informationszugang ablehnen, sind verpflichtet, die Antragsteller über dieses Anrufungsrecht zu informieren. Beratung und Unterstützung bietet die Landesbeauftragte auch den informationspflichtigen Stellen im Land Brandenburg an.

3 Interne Dienstanweisungen im Sozialbereich

Um Sozialleistungen nach einheitlichen Kriterien zu bemessen, erstellen die Behörden Verwaltungsvorschriften, so zum Beispiel zur Berechnung von Unterkunftskosten. Ein Landkreis verweigerte einem Leistungsempfänger die Offenlegung dieser Vorschriften mit diffusen Gründen.

Obwohl der Antragsteller sein Ersuchen um die Herausgabe der Durchführungshinweise zur Grundsicherung für Arbeitsuchende sowie zur Arbeitsförderung ausdrücklich auf das Akteneinsichts- und Informationszugangsgesetz stützte, bezog sich der Landkreis in seiner Antwort auf das Informationsfreiheitsgesetz des Bundes. Er meinte, seinen Informationspflichten durch die Öffentlichkeitsarbeit im Internet Genüge zu tun, obwohl nicht zu erkennen war, ob die dort vorhandenen Informationen vollständig waren. Die Erstellung eines rechtsmittelfähigen Bescheides lehnte er mit der Begründung ab, bei der Ablehnung der Herausgabe handele es sich nicht um einen Verwaltungsakt. Außerdem weigerte er sich, den Schriftverkehr zum Informationszugang aus der Sozialleistungsakte des Antragstellers zu entfernen.

Verwaltungsvorschriften, die auch als Erlasse, Rundschreiben, Durchführungshinweise oder Ähnliches bezeichnet werden, enthalten in der Regel keine schutzwürdigen Informationen, da sie sich auf eine unbestimmte Vielzahl von Fällen beziehen. Konkrete Sozialdaten, die zweifelsohne zu schützen sind, können schon deshalb gar nicht darin vorhanden sein. Auch ist die

Einstufung dieser Vorschriften als „intern“ informationszugangsrechtlich nicht relevant. Das Akteneinsichts- und Informationszugangsgesetz hat vielmehr gerade zum Ziel, nicht schutzbedürftige Verwaltungsinformationen zugänglich zu machen.

Ein Antrag auf Akteneinsicht löst ein separates Verwaltungsverfahren aus, das keinen rechtlichen Zusammenhang zum Sozialleistungsbezug des Antragstellers aufweist. Die Entscheidung über den Informationszugang enthält alle Merkmale eines klassischen Verwaltungsakts. Schriftverkehr über den Informationszugang, also alle Unterlagen vom Antrag bis zum Bescheid oder ggf. Widerspruchsbescheid, ist dementsprechend in einer separaten Akte zu führen. Er darf nicht Bestandteil der Sozialleistungsakte werden. Mit dem sozialrechtlichen Anspruch auf Löschung unrichtiger Sozialdaten hat die gebotene Trennung der Aktenführung nichts zu tun.

Der Fall ereignete sich im Jahre 2010. Am 1. Januar 2011 trat die Neuorganisation der Grundsicherung für Arbeitsuchende in Kraft. Für die bisher von den Kommunen und der Bundesagentur für Arbeit gemeinsam betriebenen Job-Center ist seitdem in der Regel vollständig der Bund verantwortlich. Rechtsgrundlage für den Informationszugang ist das Informationsfreiheitsgesetz des Bundes; zuständig für die Kontrolle seiner Einhaltung ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Nur die fünf brandenburgischen Landkreise, die sich entschieden haben, die Langzeitarbeitslosen eigenständig zu betreuen – die so genannten „Optionskommunen“ – unterliegen dem Akteneinsichts- und Informationszugangsgesetz und der Aufsicht der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg. Zur Zeit der Erstellung dieses Tätigkeitsberichts handelte es sich bei den brandenburgischen Optionskommunen um die Landkreise Oberhavel, Oder-Spree, Ostprignitz-Ruppin, Spree-Neiße und Uckermark, ab dem 1. Januar 2012 kommen noch die Landkreise Potsdam-Mittelmark und Havelland dazu.

Im Ergebnis gewährte der Landkreis den Informationszugang und sicherte eine getrennte Aktenführung zu. Es stellte sich heraus, dass die Behörde nur wenige Vorschriften selbst erlassen hat, in der Regel aber die Durchführungshinweise der Bundesagentur für Arbeit anwendet. Diese veröffentlicht solche Weisungen im Übrigen regelmäßig und nachvollziehbar auf ihrer Website – ein Beispiel, das auch in Brandenburg Schule machen sollte.

4 Auch eingetragene Vereine können Geschäftsgeheimnisse haben

Das Akteneinsichts- und Informationszugangsgesetz nimmt Unternehmensdaten weitgehend vom Recht auf Informationszugang aus. Bislang vertrat die Landesbeauftragte die Auffassung, dass Informationen öffentlicher Stellen über eingetragene Vereine nicht unter die entsprechende Ausnahmeklausel des Gesetzes fallen.

Diese in ihrem Tätigkeitsbericht 2002[60] dargelegte Rechtsauffassung musste die Landesbeauftragte im Berichtszeitraum revidieren. Anlass war eine umfangreiche Prüfung mehrerer Anfragen von Verwaltungen, wie mit den Daten eingetragener Vereine umzugehen sei.

Zahlreiche eingetragene Vereine („Idealvereine“) betätigen sich wirtschaftlich. Nach herrschender Rechtsprechung ist dies zulässig, solange die wirtschaftliche Tätigkeit nachrangig bleibt und dem eigentlichen (ideellen) Vereinszweck untergeordnet ist („Nebenzweckprivileg“). Die von § 5 Abs. 1 Nr. 3 Akteneinsichts- und Informationszugangsgesetz (AIG) geforderte Voraussetzung, dass es sich um Informationen zum „Geschäftsbetrieb“ eines „Unternehmens“ handelt, ist immer dann gegeben, wenn jemand sich wirtschaftlich betätigt. Eine unternehmerische Tätigkeit ist weder von der Rechtsform noch von der Absicht, einen Gewinn zu erzielen, abhängig. Sie kann also auch von Idealvereinen ausgeübt werden. Auch deren Teilnahme am Wettbewerb ist denkbar.

Für die Bearbeitung eines Antrags auf Informationszugang ist es nicht erforderlich, die Einhaltung der Grenzen des Nebenzweckprivilegs zu prüfen. Es genügt, festzustellen, ob die wirtschaftliche Betätigung stattfindet und in welchem Umfang sie sich in den zur Einsicht beantragten Akten widerspiegelt. In diesem Fall gilt dasselbe wie für „klassische“ Unternehmen: § 5 Abs. 1 Nr. 3 AIG sieht vor, dass die entsprechenden Informationen nur offen gelegt werden können, wenn das Unternehmen – hier: der Verein – nach § 5 Abs. 2 Nr. 4 AIG zustimmt.

Dies bedeutet jedoch nicht, dass sämtliche Informationen, die eine öffentliche Stelle über einen eingetragenen Verein führt, unter die Schutzbestimmungen des § 5 Abs. 1 Nr. 3 AIG fallen. Davon sind vielmehr lediglich solche Informationen betroffen, die im Zusammenhang mit der unternehmerischen Tätigkeit des Vereins stehen.

[60] vgl. Tätigkeitsbericht 2002, B 2.7

Soweit eingetragene Vereine sich wirtschaftlich betätigen und die sich daraus ergebenden Informationen in den Akten einer öffentlichen Stelle vorhanden sind, gelten dieselben Regeln wie im Falle „klassischer“ Unternehmen: keine Herausgabe ohne Einverständnis des Vereins.

5 Informationen zum Führungssystem der Polizei

Die Landesregierung veröffentlicht Verwaltungsvorschriften, die früher als rein interne Dokumente galten, seit einigen Jahren im Internet. Als es um Informationen zu einem Erlass über die Umsetzung von Dienstvorschriften für die Polizei ging, war das Ministerium des Innern aber plötzlich recht zugeknöpft.

In das brandenburgische Vorschriftensystem (BRAVORS) auf der Website des Landes war der Erlass nicht eingestellt worden. Der Antragsteller wandte sich daher mit seinem Antrag auf Informationen zur Form der Umsetzung des Erlasses direkt an das zuständige Ministerium. In ihrem Bescheid teilte die Behörde dem Antragsteller mit, dass dem Begehren entsprochen werde, und erläuterte in knappen Zeilen die Form der Umsetzung und wenige Aspekte des Inhalts des Erlasses für die brandenburgische Polizei. Hierfür stellte sie Gebühren und Auslagen in Rechnung. Die Gebührenerhebung begründete das Ministerium unter anderem mit dem Erfordernis einer umfassenden rechtlichen Prüfung.

Dass die Behörde die aufwendigere Erteilung einer Auskunft der wesentlich einfacheren Übersendung einer Kopie des Erlasses vorzog sowie die Geltendmachung eines umfassenden Prüfungsbedarfs ließen uns daran zweifeln, dass dem Begehren des Antragstellers tatsächlich vollständig Rechnung getragen wurde. Die Aussonderung schutzbedürftiger Informationen bzw. die Reduzierung des Akteneinsichtsrechts auf ein Auskunftsrecht wäre nämlich als teilweise Verweigerung des Informationszugangs einzustufen. Anderenfalls hätte auch der ohnehin vorgeschriebenen Veröffentlichung in der Vorschriftensammlung des Landes nichts entgegengestanden. Auf diese allgemein zugängliche Quelle hätte der Antragsteller dann kostenfrei verwiesen werden können.

In der von uns erbetenen Stellungnahme berief sich das Ministerium auf den Wortlaut des Informationszugangsantrags, in dem der Antragsteller die Übersendung der Vorschriften nicht ausdrücklich wünschte. Außerdem sei eine solche Übermittlung aufgrund sicherheitsrelevanter Informationen nicht möglich und damit auch die Veröffentlichung im Internet ausgeschlossen. Das Ministerium zog zwar indirekt die Kontrollkompetenz der Landesbeauftragten

in gebührenrechtlichen Fragen in Zweifel. Es teilte aber mit, der teilweise in Rechnung gestellte Arbeitsaufwand habe sich aus der Notwendigkeit ergeben, Informationen aus dem Erlass zu bestimmen, die offengelegt werden können, ohne die Geheimhaltung dieser schutzbedürftigen Angaben zu gefährden.

Im Ergebnis der Prüfung hielten wir den von der Behörde geltend gemachten Schutzbedarf für plausibel. Auch eine Veröffentlichung von Verwaltungsvorschriften, der Geheimhaltungsinteressen entgegenstehen, hat zu unterbleiben. Auf die brandenburgische Vorschriftensammlung im Internet konnte somit zu Recht nicht verwiesen werden. Im Hinblick auf die Kostenerhebung konnten wir keinen Verstoß gegen die Vorschriften des Akteneinsichts- und Informationszugangsgesetzes erkennen.

Wir informierten das Ministerium über die Kompetenzen der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht: Sie ist für die Wahrung des Grundrechts auf Informationszugang zuständig. Zu ihren Aufgaben gehört die Kontrolle der Einhaltung des Akteneinsichts- und Informationszugangsgesetzes. Dieses regelt im Hinblick auf die Gebührenerhebung, dass die Höhe der Kosten keine abschreckende Wirkung haben darf. Eine Entscheidung über die Kostenerhebung für den Informationszugang geht somit stets über rein gebührenrechtliche Fragen hinaus. Sie hat vielmehr eine unmittelbare Auswirkung darauf, ob das Grundrecht auf Akteneinsicht und Informationszugang wirksam in Anspruch genommen werden kann und ist somit von der Kontrollkompetenz der Landesbeauftragten umfasst. Der von der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht geprüfte Fall bot keinen Anlass, die Angemessenheit der erfolgten Gebührenerhebung zu bezweifeln.

Verwaltungsvorschriften (z. B. Erlasse, Rundschreiben, Durchführungshinweise) enthalten in der Regel keine schutzbedürftigen Informationen. Sie werden in der brandenburgischen Vorschriftensammlung BRAVORS (www.bravors.brandenburg.de) veröffentlicht. Nur in wenigen Ausnahmefällen stehen der Offenlegung berechtigte Geheimhaltungsinteressen entgegen.

6 Fördermittel für ein grenzüberschreitendes Projekt

Mit öffentlichen Mitteln wurden eine Kreisstraße innerhalb Brandenburgs sowie eine grenzüberschreitende Brücke nach Polen gefördert. Eigentlich kein Geheimnis, sollte man meinen. Die zuständige Kreisverwaltung lehnte Informationen zur Förderung des Baus der Brücke dennoch ab.

Der Antragsteller beantragte Einsicht in den Fördermittelantrag des Landkreises und den entsprechenden Bewilligungsbescheid der Investitionsbank des Landes Brandenburg zum Bau der Kreisstraße. Außerdem interessierten ihn die entsprechenden Fördermittelunterlagen aus dem Projekt des brandenburgischen Landkreises und seines polnischen Nachbarkreises zum Bau der Brücke sowie das Protokoll einer gemeinsamen Erörterung des Projektes durch die Vorhabenträger. Die Behörde teilte dem Antragsteller ihre Absicht mit, die beteiligten Stellen nach ihrem Einverständnis mit dem Informationszugang zu fragen und bat um eine Konkretisierung und um eine Begründung seines Begehrens.

Daraufhin machten wir den Landkreis darauf aufmerksam, dass die den Antragsteller interessierenden Unterlagen hinreichend bestimmt sind und allenfalls mit Unterstützung der Behörde noch weiter eingegrenzt werden können. Diese hat insoweit eine Beratungspflicht dem Antragsteller gegenüber. Die Gründe für die Akteneinsicht spielen bei der Prüfung des Einsichtsbegehrens keine Rolle und dürfen grundsätzlich nicht erfragt werden.

Das Akteneinsichts- und Informationszugangsgesetz sieht vor, dass ein Antrag auf Akteneinsicht abzulehnen ist, wenn die betroffenen öffentlichen Stellen, die nicht dem Anwendungsbereich des Gesetzes unterfallen, die Zustimmung zur Einsichtnahme verweigern. Es schützt außerdem Akteninhalte, welche die internationalen Beziehungen berühren oder die Beziehungen des Landes zu anderen Staaten oder zwischenstaatlichen Einrichtungen beeinträchtigen könnten. Die Investitionsbank des Landes Brandenburg ist eine Anstalt des öffentlichen Rechts und fällt somit nicht unter den engen Anwendungsbereich des Akteneinsichts- und Informationsgesetzes. Zu Recht hat der Landkreis daher sowohl die Bank als auch die polnischen Partner nach ihrem Einverständnis mit der Offenlegung gefragt.

Im Ergebnis der Beteiligung gewährte der Landkreis die Einsicht in die Fördermittelunterlagen zu der brandenburgischen Kreisstraße. Allerdings verweigerte die zuständige polnische Stelle ihr Einverständnis zur Offenlegung der Unterlagen zu dem gemeinsamen Brückenprojekt mit dem Hinweis, das polnische Recht ermögliche die Einsichtnahme erst nach Abschluss des Fördervertrags. An die Versagung der Zustimmung war der Landkreis gebunden und lehnte diesen Teil des Antrags zu Recht ab.

Unterlagen öffentlicher Stellen, die nicht dem Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes unterliegen, können nur mit deren Einverständnis offengelegt werden. Versagen sie ihre Zustimmung, ist der Antrag auf Informationszugang abzulehnen.

7 Informationen zu Ordnungswidrigkeiten – Kirrungen und Wirrungen

Der Erstatter einer Anzeige wegen unzulässiger Wildfütterungen interessierte sich für das Ergebnis des behördlichen Vorgehens. Er wollte von der unteren Jagdbehörde unter anderem erfahren, wie hoch das gegen den Beschuldigten verhängte Bußgeld war und ob es bezahlt wurde. Sein Begehren stützte er auf das Akteneinsichts- und Informationszugangsgesetz.

Das Jagdgesetz des Landes Brandenburg stellt die Fütterung von Schalenwild – also von Paarhufern wie Hirschen, Rehen oder Wildschweinen – außerhalb der Notzeiten grundsätzlich unter Verbot. Den Verstoß gegen diese Vorschrift ordnet es als Ordnungswidrigkeit ein und sieht hierfür eine Geldbuße von bis zu 5.000 Euro vor.

Ein Antrag auf Akteneinsicht ist nach § 4 Abs. 1 Nr. 5 Akteneinsichts- und Informationszugangsgesetz (AIG) unter anderem dann abzulehnen, wenn durch die Gewährung des Zugangs Inhalte von Akten offenbart würden, die eine Behörde zur Durchführung eines Bußgeldverfahrens erstellt hat. Dieser Ausnahmetatbestand gilt auch, wenn das Verfahren über die Ordnungswidrigkeit abgeschlossen ist. Außerdem wird nach § 2 Abs. 5 AIG in laufenden Verfahren Akteneinsicht nur nach Maßgabe des anzuwendenden Verfahrensrechts gewährt. Die Verhängung eines Bußgeldes erfolgt auf der Grundlage des Gesetzes über Ordnungswidrigkeiten. Diese Rechtsgrundlage geht dem Akteneinsichts- und Informationszugangsgesetz somit im laufenden Verfahren vor. Nach Abschluss eines Bußgeldverfahrens ist der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes zwar grundsätzlich eröffnet, in der Regel dürfte jedoch der erwähnte Ausnahmetatbestand zur Geheimhaltung von Bußgeldakten dem Informationszugang entgegenstehen.

Die Behörde hat demnach zur Prüfung eines Antrags auf Zugang zu Informationen aus einem Bußgeldverfahren das Gesetz über Ordnungswidrigkeiten (OWiG) und – über die Verweise der §§ 46 und 49b OWiG – die Vorschriften der Strafprozessordnung (StPO) heranzuziehen.

Ein Anzeigeerstatter, der weder Beteiligter noch Geschädigter ist, erhält nach der Strafprozessordnung wie folgt Einsicht: Nach § 475 Abs. 1 StPO kann ein Rechtsanwalt für Privatpersonen Auskünfte erhalten, soweit er hierfür ein berechtigtes Interesse darlegt. Auch die Einsichtnahme durch den Rechtsanwalt gemäß § 475 Abs. 2 StPO ist möglich, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern oder zur Wahrnehmung des berechtigen Interesses nicht ausreichen würde. Privatpersonen ohne

anwaltliche Vertretung oder sonstige private Stellen (beispielsweise Versicherungsunternehmen) können nach § 475 Abs. 4 StPO unter denselben Voraussetzungen Auskunft erhalten. Einsicht und Auskunft sind zu versagen, wenn der Betroffene ein schutzwürdiges Interesse hat.

Die Verfolgungsbehörde informiert den Anzeigeerstatter gemäß § 171 StPO über die Nichteinleitung oder Einstellung des Verfahrens.

Die bloße Neugierde des Anzeigeerstatters, was aus seiner von der Behörde bearbeiteten Anzeige geworden ist, stellt in der Regel kein berechtigtes Interesse im Sinne der oben genannten Rechtsgrundlagen dar. Die untere Jagdbehörde hat den Antragsteller im vorliegenden Fall auf die Anwendung des Gesetzes über Ordnungswidrigkeiten hingewiesen und den Informationszugang zu Recht abgelehnt.

Ein Antrag auf Akteneinsicht ist in Verfahren über Ordnungswidrigkeiten in der Regel auf der Grundlage des Gesetzes über Ordnungswidrigkeiten zu prüfen. Nicht am Verfahren Beteiligte können nur unter bestimmten Umständen Informationen erhalten.

Teil C

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

1.1 Entwicklungen der Dienststelle

Hinter der Dienststelle der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht liegen zwei Jahre, die durch Neuorganisation, Mitarbeiterwechsel und eine weiter steigende Zahl von Bürgerbeschwerden gekennzeichnet sind.

Mit der Verabschiedung des Vierten Gesetzes zur Änderung des Gesetzes zum Schutz personenbezogener Daten im Land Brandenburg im Mai 2010 hat der brandenburgische Landtag die Zusammenlegung der öffentlichen und nicht-öffentlichen Datenschutzaufsicht bei der Landesbeauftragten sowie die Verlagerung der Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten nach dem Brandenburgischen Datenschutzgesetz und dem Bundesdatenschutzgesetz auf die Landesbeauftragte zum 1. Juni 2010 beschlossen. Vier Stellen des Ministeriums des Innern, das zuvor die Datenschutzaufsicht über den nicht-öffentlichen Bereich im Land Brandenburg beim Ministerium des Innern ausgeübt hatte, wurden der Landesbeauftragten übertragen.

Mit der Zusammenlegung der Aufsicht ergab sich auch die Notwendigkeit, die Geschäftsverteilung in der Dienststelle neu zu organisieren. Zur Erreichung von Synergieeffekten und Vermeidung unnötiger Abstimmungsprozesse wurden Arbeitsgebiete aus dem öffentlichen und nicht-öffentlichen Bereich thematisch zusammengefasst (z. B. Gesundheit, Personaldaten, Videoüberwachung). Die Prüfung und Durchführung von Ordnungswidrigkeitenverfahren musste als Arbeitsgebiet vollständig neu aufgebaut werden. Für diese Aufgabe hatte die Dienststelle kein Personal erhalten.

Im Mai 2010 habe ich eine langjährige Mitarbeiterin in den Ruhestand verabschiedet. Sie hatte sich seit dem Bestehen der Dienststelle – insbesondere im Bereich der Polizei und des Verfassungsschutzes sowie als Pressesprecherin – für Datenschutz und Informationsfreiheit engagiert. Ihre Stelle konnte nach einem Ausschreibungsverfahren erfolgreich wiederbesetzt werden.

Eine weitere Neubesetzung konnte allerdings erst mit einem halben Jahr Verzögerung stattfinden. Die Zwischenzeit haben wir mit der befristeten

Beschäftigung eines Mitarbeiters überbrückt, der die vakanten Arbeitsgebiete mit großem Einsatz übernommen hat.

Mit der Zusammenlegung der Datenschutzaufsicht in meiner Dienststelle habe ich die Aufgabe, für beide Aufsichtsbereiche gleichermaßen tätig zu sein. Dies führt dazu, dass sich Arbeitsschwerpunkte verlagern. Die zeitintensive Einbindung meiner Dienststelle bei der Begleitung von Projekten öffentlicher Stellen ist mit den gegenwärtig zur Verfügung stehenden personellen Kapazitäten im gewohnten Umfang nicht mehr zu bewerkstelligen. Auch anlassunabhängige Prüfungen bei nicht-öffentlichen Stellen im Land sind aus diesen Gründen fast nicht möglich. Darüber hinaus bin ich gezwungen, andere für die Gewährleistung von Datenschutz und Informationsfreiheit im Land Brandenburg notwendige Aufgaben hintanzustellen. Die Schaffung zusätzlicher Kapazitäten ist daher unabdingbar.

1.2 Erneuerung des IT-Systems

In unserem lokalen Netz (LAN) werden personenbezogene Daten verarbeitet, die zum Teil einem hohen Schutzbedarf unterliegen. Die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität der in unserer Dienststelle verarbeiteten personenbezogenen Daten ist eine wesentliche Forderung, die aus § 10 Brandenburgisches Datenschutzgesetz (BbgDSG) resultiert.

Im Berichtszeitraum wurde das IT-System unserer Behörde an den aktuellen Stand der Technik angepasst. Meine Mitarbeiter haben neue Server, Arbeitsplatzcomputer, Drucker und Netzwerkkomponenten beschafft, installiert und in Betrieb genommen. Im Zuge der Neukonzeption des IT-Systems wurde auch unser IT-Sicherheitskonzept überarbeitet und an den aktuellen Stand der Technik angepasst. Insbesondere erfolgte eine Implementierung entsprechender kryptographischer Verfahren. Personenbezogene Daten, die einem hohen Schutzbedarf unterliegen, werden auf den Servern ausschließlich verschlüsselt gespeichert. Eine von uns administrierte Firewall schottet das LAN vom Landesverwaltungsnetz ab.

1.3 Ordnungswidrigkeiten

Aufgrund der neuen Zuständigkeitsregelungen des § 23 Abs. 8 Brandenburgisches Datenschutzgesetz (BbgDSG) ist die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht seit dem 1. Juni 2010 zuständige Behörde für die Verfolgung von Ordnungswidrigkeiten nach § 38 BbgDSG, § 43 Bundesdatenschutzgesetz (BDSG) sowie anderer datenschutzrechtlicher Regelungen.

Das Arbeitsgebiet musste vollkommen neu aufgebaut werden, da der Dienststelle hierfür im Rahmen der Zusammenlegung der Aufsichtsbehörden kein Personal durch das Ministerium des Innern übertragen wurde. Die Aufgabe wird von einer Mitarbeiterin des Bereichs Recht und Verwaltung wahrgenommen; ihr oblag auch die Erarbeitung und Beschreibung interner Abläufe und Handlungsrichtlinien für die Durchführung von Ordnungswidrigkeitenverfahren.

Bei jedem Rechtsverstoß gegen datenschutzrechtliche Normen ist durch die Landesbeauftragte grundsätzlich zu prüfen, ob und welche Maßnahmen eingeleitet werden. Hierfür sehen das Brandenburgische Datenschutzgesetz bzw. das Bundesdatenschutzgesetz verschiedene Möglichkeiten vor. Neben einer Reihe anderer Instrumente (wie z. B. Belehrung, Beanstandung, Anordnung, Untersagung, Zwangsgeld) kann sie auch ein Ordnungswidrigkeitenverfahren einleiten. Im Ergebnis eines solchen Verfahrens kann eine einfache Verwarnung bzw. eine Verwarnung mit Verwarnungsgeld erteilt oder ein Bußgeld erhoben werden. Im Falle des Verdachts strafbarer Handlungen erfolgt die Abgabe an die Staatsanwaltschaft mit dem Ziel der Einleitung eines Strafverfahrens.

Seit der Übernahme der neuen Aufgabe am 1. Juni 2010 wurden wegen gravierender Verstöße gegen das Datenschutzrecht in mehreren Fällen Bußgelder festgesetzt. Dabei ging es vor allem um unbefugte Abfragen aus polizeilichen Datenbanken sowie Übermittlungen von Sozialdaten an unzuständige Dritte.

Auch hat die Landesbeauftragte im Berichtszeitraum einen Strafantrag bei der Staatsanwaltschaft gestellt. Dieser betraf den unbefugten Verkauf von Kundendaten durch ein Versicherungsunternehmen. Das Strafverfahren ging mit einem Strafbefehl gegen den Unternehmer aus.

2 Zusammenarbeit mit dem Landtag

Auch in den vergangenen beiden Jahren haben wir mit dem Landtag Brandenburg eng und intensiv zusammengearbeitet.

In seiner Sitzung am 8. Dezember 2010 hat der Ausschuss für Inneres den Tätigkeitsbericht 2008/2009 abschließend beraten. Er empfahl dem Landtag, die Landesregierung aufzufordern, auf ein Recht auf Kopien bei der Anwendung des Akteneinsichts- und Informationszugangsgesetzes hinzuwirken und dies bei einer Novellierung dieses Gesetzes auch zu regeln, die Datenschutzverordnung Schulwesen abschließend zu überarbeiten, die Kommunen

bei ihrer Aufgabe des kommunalen Datenschutzes zu unterstützen sowie bei der Konsolidierung der IT-Infrastruktur bei dem Zentralen IT-Dienstleister die Anforderungen an den Datenschutz und die Betriebssicherheit zu gewährleisten. Der Landtag ist der Beschlussempfehlung des Innenausschusses in seiner Sitzung am 17. Dezember 2010 gefolgt.[61]

Die Datenschutzverordnung Schulwesen wurde inzwischen vom Ministerium für Bildung, Jugend und Sport überarbeitet und soll 2012 in Kraft treten. Die Novellierung des Akteneinsichts- und Informationszugangsgesetzes steht noch immer aus. Die Umsetzung der beiden letztgenannten Beschlüsse erfordert einen längeren Zeitraum.

Der Landtag bat im Berichtszeitraum um datenschutzrechtliche Stellungnahmen zu mehreren Gesetzesvorhaben. So habe ich mich unter anderem vor dem Ausschuss für Umwelt, Gesundheit und Verbraucherschutz zu dem Gesetz zur Änderung des Gesetzes zu Hilfen und Schutzmaßnahmen sowie über den Vollzug gerichtlich angeordneter Unterbringung für psychisch Kranke und seelisch behinderte Menschen in Brandenburg geäußert. Auf Bitte des Ausschusses für Inneres gab ich Stellungnahmen zur Kennzeichnungspflicht für Polizisten, zur Handyortung und zur automatisierten Kfz-Kennzeichenfahndung im Rahmen verschiedener Änderungen des Brandenburgischen Polizeigesetzes ab. Weiterhin habe ich mich im Rahmen der Anhörung des Haupt- und des Innenausschusses zu dem Ersten Gesetz zur Änderung des Volksabstimmungsgesetzes zu den damit verbundenen datenschutzrechtlichen Fragen geäußert.

Am 22. Juni 2011 hat mich der Landtag für eine zweite Amtszeit als Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wiedergewählt. Das damit verbundene Vertrauen ehrt mich sehr. Ich freue mich auf die Fortführung der guten Zusammenarbeit in der neuen Amtsperiode.

3 Zusammenarbeit mit den behördlichen Datenschutzbeauftragten

Einer Tradition folgend haben wir auch in den Jahren 2010 und 2011 die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden in unsere Dienststelle eingeladen, um Sachverhalte der täglichen Arbeit der öffentlichen Stellen aus datenschutzrechtlicher Sicht zu erörtern.

[61] vgl. Beschluss des Landtages Brandenburg vom 17. Dezember 2010, Landtags-Drucksache 5/2409-B

Das Interesse an diesen Beratungen ist seitens der behördlichen Datenschutzbeauftragten unverändert groß. Aber auch für die Arbeit der Landesbeauftragten ist es ein Vorteil, wenn aktuelle Probleme aus der Praxis rechtzeitig angesprochen werden. So können bei der Planung oder Durchführung von Daten verarbeitenden Verfahren ggf. notwendige Maßnahmen oder Korrekturen effektiv ergriffen werden.

Inhaltliche Schwerpunkte der Beratungen waren rechtliche Fragen zum Arbeitnehmer-, Gesundheits- und Sozialdatenschutz, technische und organisatorische Aspekte (z. B. Sicherheitsanforderungen an Meldebehörden, elektronischer Personalausweis, Zensus, Virtuelles Bauamt) sowie Probleme zu Akteneinsicht und Informationszugang. Darüber hinaus dienen die Treffen regelmäßig dem Austausch der Beteiligten zu den Aufgabenfeldern der behördlichen Datenschutzbeauftragten sowie zur Umsetzung ihrer Empfehlungen.

4 Zusammenarbeit mit anderen Datenschutzbehörden

Auch 2010 und 2011 fanden wieder halbjährlich Kooperationsgespräche mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit statt. Eine zentrale Rolle spielten dabei erneut Abstimmungen zu rechtlichen Positionen (z. B. soziale Netzwerke), zu Fragen der IT-Sicherheit (z. B. Einführung des E-Tickets beim Verkehrsverbund Berlin-Brandenburg) sowie zu gemeinsamen Prüfungen (z. B. des Amtes für Statistik Berlin-Brandenburg im Projekt Zensus 2011).

Im Jahr 2010 tagte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter dem Vorsitz des baden-württembergischen Kollegen, Jörg Klingbeil, im Frühjahr in Stuttgart und im Herbst in Freiburg. Die Konferenz hat 2010 insgesamt zwölf Entschließungen verabschiedet, die sich unter anderem mit Sicherheitsthemen, Steuerdaten und Beschäftigtendatenschutz befassten. Im Jahr 2011 hatte der bayerische Kollege, Dr. Thomas Petri, den Konferenzvorsitz inne. Die Frühjahrskonferenz fand in Würzburg, die Herbstkonferenz in der Landeshauptstadt München statt. Es wurden vierzehn Entschließungen verabschiedet, von denen sich allein fünf mit dem Thema der inneren Sicherheit und vier mit technischen Fragestellungen befasst haben. Die Konferenz sieht es zunehmend als wichtig an, zu technischen Entwicklungen Orientierungshilfen anzubieten. Dies hat sie zuletzt bei den Themen „Cloud Computing“ und „Krankenhausinformationssysteme“ getan.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat das Eckpunktepapier „Ein modernes Datenschutzrecht für das

21. Jahrhundert“ erarbeitet und im März 2010 vorgestellt. Das Papier soll einen wichtigen Diskussionsbeitrag zu der Frage leisten, wie ein modernes Datenschutzrecht im Internetzeitalter aussehen könnte.

Seit dem 1. Juni 2010 ist die Landesbeauftragte durch die Zusammenlegung der Datenschutzaufsicht auch Mitglied im Düsseldorfer Kreis, dem Zusammenschluss aller Aufsichtsbehörden für den Datenschutz im privaten Bereich. Auch der Düsseldorfer Kreis tagt zweimal im Jahr und fasst Beschlüsse zu aktuellen Datenschutzthemen. Er beschäftigt sich mit Fragen der Auslegung datenschutzrechtlicher Vorschriften und der Abstimmung aufsichtsbehördlicher Praxis. Nachdem der Düsseldorfer Kreis in den letzten Jahren immer einen wechselnden Vorsitz hatte, wird er zurzeit von dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Ulrich Lepper, wieder in seinem Gründungsort in Düsseldorf geleitet. Der Düsseldorfer Kreis hat 2010 und 2011 in den drei Sitzungen, an denen die Landesbeauftragte teilgenommen hat, insgesamt zehn Beschlüsse gefasst.

Im Zusammenhang mit der Entscheidung des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzaufsicht haben inzwischen fast alle Bundesländer die Zusammenlegung der Aufsichtsbehörden für den Datenschutz im öffentlichen und nicht-öffentlichen Bereich vollzogen. Lediglich im Freistaat Bayern werden auch künftig zwei verschiedene Behörden zuständig sein. Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung in München den Präsidenten des Bayerischen Landesamtes für Datenschutz, Thomas Kranig, als Mitglied aufgenommen.

5 Informationsfreiheitsbeauftragte

Im Berichtszeitraum tagte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland insgesamt viermal.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Dr. Alexander Dix, führte im ersten Halbjahr 2010 den Vorsitz in der Konferenz. In dieser Zeit forderte sie in einer Entschließung die Schaffung von Rechtsvorschriften, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind. Unter dem Vorsitz der brandenburgischen Landesbeauftragten, Dagmar Hartge, diskutierte die Konferenz im zweiten Halbjahr 2010 vor allem zwei aktuelle Themen der Informationsfreiheit. Angesichts der weitgehenden Geheimhaltung von Verträgen zwischen Staat und Unternehmen forderte sie hier eine grundsätzliche Offenlegung.

Die Informationsfreiheitsgesetze sollten – ähnlich wie dies teilweise bereits in Berlin anlässlich der Debatte um die „Wasserverträge“ geschah – so geändert werden, dass der Zugang zu Verträgen nicht mehr pauschal zurückgewiesen werden kann. Außerdem machte die Konferenz auf das gestiegene Bedürfnis der Öffentlichkeit nach verbesserter Information und mehr Transparenz staatlichen Handelns aufmerksam. Sie ermutigte die staatlichen Stellen in einer Entschließung ausdrücklich, Informationen im Sinne des Open-Data-Ansatzes umfangreich und auf eigene Initiative auf einer einheitlichen Plattform zur Verfügung zu stellen.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, Dr. Imke Sommer, hatte den Konferenzvorsitz im ersten Halbjahr 2011 inne. Die Informationsfreiheitsbeauftragten veröffentlichten in dieser Zeit zwei Entschließungen: Sie appellierten an die Gesetzgeber in Bund und Ländern, flächendeckend allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informationsfreiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln. Außerdem forderten sie mehr Transparenz für ein geplantes europäisches Nanoproduktregister.

Unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, sprach sich die Konferenz der Informationsfreiheitsbeauftragten im November 2011 in einer Entschließung für die Aufnahme der Informationsfreiheit ins Grundgesetz und in die Landesverfassungen aus.

In zwei gemeinsamen Stellungnahmen zum Verbraucherinformationsgesetz legten die Informationsfreiheitsbeauftragten ihre Auffassung zur weiteren Entwicklung auf diesem Gebiet dar. Im September 2010 beteiligten sie sich an einer öffentlichen Konsultation der Bundesregierung zur Evaluation des Verbraucherinformationsgesetzes und im März 2011 nahmen sie zu einem konkreten Referentenentwurf zur Änderung des Gesetzes Stellung. Schwerpunkte ihrer Forderungen waren die Einheitlichkeit der Regelungen und Kontrollkompetenzen zu den bislang unterschiedlichen Informationszugangsregelungen, die Ausweitung des Anwendungsbereichs des Verbraucherinformationsgesetzes, Abwägungspflichten, die sowohl das Geheimhaltungsinteresse der Hersteller als auch das Zugangsinteresse der Öffentlichkeit angemessen berücksichtigen, sowie eine bürgerfreundliche Gebührenregelung.

6 Öffentlichkeitsarbeit

6.1 Internationales Symposium zu Verbraucherinformationen

Die Landesbeauftragte veranstaltete am 30. und 31. Mai 2011 das siebente Internationale Symposium in Potsdam. Im Zentrum der Konferenz stand der Zugang zu Verbraucherinformationen. Auf der Grundlage des im Jahre 2007 verabschiedeten Verbraucherinformationsgesetzes kann jeder bei den zuständigen Behörden Informationen zu Lebensmitteln, Futtermitteln und Gegenständen des täglichen Bedarfs beantragen. Deutschland hat damit einen rechtlichen Sonderweg gewählt; in anderen Ländern wird das allgemeine Informationsfreiheitsrecht auch für den Zugang zu Verbraucherinformationen genutzt. Als das Internationale Symposium stattfand, war die Diskussion um die Novellierung des Verbraucherinformationsgesetzes gerade in vollem Gange.

Wie die Beiträge zahlreicher Experten aus Brandenburg, Deutschland und Europa sowie die lebhaften Diskussionen der Teilnehmer zeigten, ist das Verbraucherinformationsgesetz nur ein Instrument unter vielen. Verbraucher möchten sich in der Regel unkompliziert, spontan und vor allem ohne ein aufwendiges Antragsverfahren informieren. Hält das Restaurant, dessen Speisekarte so vielversprechend klingt, auch die hygienischen Vorschriften ein? Welche Konservierungsstoffe enthält das Fertiggericht im Kühlregal des Supermarkts? Ist das billig erstandene Kinderspielzeug mit gefährlichen Chemikalien versetzt? Wie kommt man bei grenzüberschreitenden Einkäufen zu den notwendigen Informationen? Wie werden Finanzprodukte oder Dienstleistungen der Telekommunikation für den Verbraucher leichter durchschaubar?

Das Internationale Symposium wurde gemeinsam mit der Alcatel-Lucent Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik organisiert. Welche Instrumente und Modelle zur Verbraucherinformation während des Internationalen Symposiums vorgestellt wurden, geht aus einer Dokumentation hervor, die die Landesbeauftragte sowohl als Druckbroschüre als auch auf ihrer Website veröffentlicht hat.

6.2 Veranstaltungen der Landesbeauftragten

Im Rahmen der Novellierung des Brandenburgischen Datenschutzgesetzes im Frühjahr des Jahres 2010 wurde die Datenschutzaufsicht über private Unternehmen mit Sitz in Brandenburg auf die Landesbeauftragte übertragen. Dass sich daraus nicht zuletzt ein erhöhter Beratungsbedarf ergibt, zeigte sich bereits im September des Jahres 2010, als die Landesbeauftragte mit

ihren Mitarbeitern ein Wochenende lang auf dem Brandenburg-Tag in Schwedt/Oder präsent war. In einem Informationszelt stellte sie ein System zum Einsatz von RFID vor. Zahlreiche Besucher äußerten sich erstaunt darüber, mit welch geringem Mitteleinsatz es technisch möglich ist, Menschen zu kontrollieren und zu überwachen. Ähnliche Reaktionen zeitigte auch eine Präsentation zum „Knacken“ von Windows-Passwörtern. Wer wollte, konnte am Stand der Landesbeauftragten ein (erfundenes) Passwort eingeben, um zu testen, wie sicher diese Zugangskennung ist. Nicht in angemessener Zeit zu knacken waren nur die wenigsten. Ebenfalls auf großes Interesse stießen Informationen zum Adresshandel sowie zu den Datenschutzrechten gegenüber Auskunfteien. Auch zum nächsten Brandenburg-Tag in Lübbenau am 1./2. September 2012 lädt die Landesbeauftragte alle Interessierten wieder an ihren Stand ein.

Gemeinsam richteten die Datenschutzbeauftragten des Bundes und der Länder – unter Beteiligung der brandenburgischen Landesbeauftragten – zentrale Veranstaltungen zum vierten und fünften Europäischen Datenschutztag in Berlin aus. Dieser wird auf Initiative des Europarates jährlich am 28. Januar begangen. Im Jahr 2010 fand aus diesem Anlass eine Podiumsdiskussion mit dem Thema „Gesundheitsdaten im Netz“ statt. Neben dem Dauerbrenner „elektronische Gesundheitskarte“ erörterten Experten aus Medizin, Wissenschaft und Datenschutz die Wahrung der Persönlichkeitsrechte der Patienten beim elektronischen Austausch medizinischer Informationen. Im Folgejahr hieß die Frage: „Datenschutz in Europa – Quo vadis?“. Dabei stand die aktuelle Debatte um eine Modernisierung des Datenschutzrechts auf europäischer Ebene im Fokus, es ergaben sich aber auch wertvolle Anregungen für die Novellierung der Vorschriften zum Datenschutz im Bund und in den Ländern.

Die umfangreichen Stadt-Umland-Verflechtungen führen in der Region Berlin-Brandenburg immer stärker auch auf den landesspezifisch geregelten Gebieten des Datenschutzes und der Informationsfreiheit zu Überschneidungen. Berliner, die ein Grundstück in Brandenburg besitzen oder Brandenburger, die in Berlin einen Arzt aufsuchen, fragen Beratung zu der Rechtslage in dem jeweils anderen Land nach. Eine Einladung ihres Berliner Kollegen zur Teilnahme an dessen Informationsstand zum Tag der offenen Tür des Abgeordnetenhauses von Berlin im Mai des Jahres 2010 nahm die brandenburgische Landesbeauftragte daher gerne an. Zusammen mit ihren Mitarbeitern informierte sie dort unter anderem über die Möglichkeit, bei brandenburgischen Behörden Auskunft über die „eigenen“ dort verarbeiteten Daten zu erlangen und beantwortete beispielsweise Fragen zum Datenschutz bei Auskunfteien. Sie nahm zudem an einer Veranstaltung des Petitionsausschusses zu Hartz IV teil. Der gemeinsam mit dem Berliner Kollegen erstellte Ratgeber zu Hartz IV stieß hier auf großes Interesse.

In den letzten Jahren bot die Landesbeauftragte Sprechstunden in den brandenburgischen Landkreisen und kreisfreien Städten an, um den Bürgern sowie den Verwaltungsmitarbeitern vor Ort einen unkomplizierten Kontakt zu ermöglichen. Im ersten Jahr des Berichtszeitraums fanden vier weitere Bürgersprechstunden statt: in der Landeshauptstadt Potsdam, in Seelow (Märkisch-Oderland), in Senftenberg (Oberspreewald-Lausitz) und in Neuruppin (Ostprignitz-Ruppin). Alle Bürgersprechstunden wurden vonseiten der Stadt bzw. der Landkreise sehr hilfreich unterstützt und sowohl von Bürgern als auch von Beschäftigten der Verwaltungen gut angenommen. Auch für die Landesbeauftragte waren diese Veranstaltungen ausgesprochen nützlich, schließlich zeigt sich im persönlichen Gespräch am besten, wo überhaupt „der Schuh drückt“. Dieses erfolgreiche Konzept kann die Landesbeauftragte vorerst leider nicht weiterführen. Die Übernahme der Datenschutzaufsicht über die nicht-öffentlichen Stellen im Frühjahr 2010 sowie die Verpflichtungen im öffentlichen Bereich lassen hierfür keine Möglichkeit mehr.

6.3 Fortbildungsangebote

Obwohl die personelle Situation in unserer Dienststelle nach der Übernahme der Aufsicht über den Datenschutz im nicht-öffentlichen Bereich sehr angespannt ist, haben Mitarbeiter unserer Behörde wie schon in den vergangenen Jahren auch in diesem Berichtszeitraum zahlreiche Fortbildungen zu Fragen des Datenschutzes durchgeführt. So unterschiedlich die Teilnehmer, ihre Vorkenntnisse und Erwartungen, die thematische Ausrichtung einzelner Veranstaltungen oder die zur Verfügung stehende Zeit auch waren – immer ging es uns darum, einen Beitrag zur Sensibilisierung für die Belange des Datenschutzes sowohl aus rechtlicher als auch aus technisch-organisatorischer Sicht zu leisten. Ziel war es weiterhin, neben der Erläuterung von rechtlichen Grundlagen auch deren Anwendung zu erörtern und so die Verbindung von Theorie und Praxis herzustellen.

Im rechtlichen Bereich waren die Themen unserer Schulungen u. a. Datenschutz in der Justiz (gemeinsam durchgeführt mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit), Sozialdatenschutz bei der Grundsicherung für Arbeitslose, Datenschutz und Kinderschutz, Datenschutz in der Kinder- und Jugendhilfe sowie bei der Kitabetreuung, Datenschutz im Internet und bei der Nutzung Neuer Medien (Web 2.0, Google Street View), Datenschutz und Stärkung der Medienkompetenz, Datenschutz am kommunalen Arbeitsplatz, aktuelle Fragen des Datenschutzes in Kommunen sowie postmortaler Datenschutz.

Auf dem Gebiet der technischen und organisatorischen Aspekte des Datenschutzes wurden Fortbildungen u. a. zu den folgenden Themen durchgeführt: Grundlagen des Datenschutzes und der Datensicherheit (mehrfach für ver-

schiedene Zielgruppen), Datenschutzmanagement, Erstellung von IT-Sicherheitskonzepten, IT-Sicherheitsaudits, Datenschutz beim Cloud Computing, Kriminalität im Internet sowie Technische Risiken, Angriffsszenarien und Schutzmaßnahmen im Internet.

Auch im Bereich des Akteneinsichts- und Informationszugangsrechts besteht nach wie vor ein erheblicher Bedarf, Mitarbeiter in öffentlichen Verwaltungen des Landes Brandenburg in Bezug auf die rechtliche Grundlagen und ihre Anwendung in der täglichen Verwaltungspraxis zu schulen. Ursache für die stetige Nachfrage nach Schulungen ist vor allem die komplizierte und zersplitterte Rechtsmaterie im Bereich der Informationsfreiheit. Aber auch die Anwendung der umfangreichen Ausnahmetatbestände zum Schutz überwiegender öffentlicher und privater Interessen, die in diesem Zusammenhang häufig erforderliche Auslegung unbestimmter Rechtsbegriffe sowie die Bearbeitungsfristen, die Kostenerhebung oder die Durchführung von Anhörungsverfahren für Drittbetroffene bereiten den Verwaltungen in der täglichen Umsetzung der Informationsfreiheit teilweise Schwierigkeiten.

Wegen des großen Bedarfs haben im Berichtszeitraum Mitarbeiter der Behörde Fortbildungen zur Informationsfreiheit in verschiedenen öffentlichen Verwaltungen unterschiedlicher Größe, bei kommunalen Bildungsträgern sowie beim Brandenburgischen IT-Dienstleister durchgeführt. Im Mittelpunkt stand dabei nicht nur die reine Vermittlung von Wissen – stets wurden mit den Teilnehmern auch ausführlich Fallbeispiele diskutiert sowie Erfahrungen bei der Anwendung des Rechts ausgetauscht.

6.4 Neue Publikationen der Landesbeauftragten

Die Neufassung der Broschüre „Technisch-organisatorische Aspekte des Datenschutzes“ berücksichtigt die Vorgaben des seit der ersten und zweiten Auflage inzwischen mehrfach novellierten Brandenburgischen Datenschutzgesetzes sowie den aktuellen Stand der Technik. Neben Erläuterungen zu den rechtlichen Grundsätzen des technischen und organisatorischen Datenschutzes enthält sie ausführliche Empfehlungen zur datenschutzgerechten und sicheren Gestaltung informationstechnischer Systeme und Verfahren. Die Publikation richtet sich in erster Linie an Mitarbeiter der öffentlichen Verwaltung im Land Brandenburg, die sich mit Fragen der IT-Sicherheit und des Datenschutzes befassen.

Die Landesbeauftragte gab nach dem Internationalen Symposium „Verbraucherinformationen - Marktregulierung durch Transparenz?“, das am 30./31. Mai 2011 stattfand, einen Tagungsband mit den Beiträgen der Referenten heraus. Die Dokumentation ist als siebenter Band in der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ erschienen.

In einem Ratgeber informiert die Landesbeauftragte über die Rechtslage zum Adresshandel und zu unerwünschter Werbung. Im Vordergrund stehen Tipps, um die Weitergabe personenbezogener Daten für Werbezwecke zu unterbinden und die Flut unerwünschter Werbung einzudämmen. Die Hinweise aus dieser Broschüre sind in enger Zusammenarbeit des Bundesbeauftragten sowie der Landesbeauftragten für den Datenschutz aus Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Brandenburg erstellt worden.

Angesichts der immer häufigeren Anfragen vor allem aus dem europäischen Ausland haben wir das im Jahre 2010 geänderte Brandenburgische Datenschutzgesetz in seiner aktuellen Fassung ins Englische übersetzen lassen und in elektronischer Form veröffentlicht. Das für Unternehmen mit Sitz in Brandenburg wichtige Bundesdatenschutzgesetz wird vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in englischer Sprache bereitgehalten.

Das Datenscheckheft der Landesbeauftragten ist grundlegend überarbeitet und der in weiten Teilen veränderten Gesetzeslage angepasst worden. Es enthält unter anderem Musterbriefe, mit denen die Bürger ihre Datenschutzrechte – insbesondere das Auskunftsrecht über gespeicherte personenbezogene Daten – leichter wahrnehmen können.

Nach den gesetzlichen Novellierungen hat die Landesbeauftragte sowohl das Brandenburgische Datenschutzgesetz als auch das Bundesdatenschutzgesetz in einer handhabbaren Lesefassung drucken sowie vergriffene Broschüren mit den Regelungen zum Akteneinsichts- und Informationszugangsgesetz und dem Verbraucherinformationsgesetz nachdrucken lassen.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 17./18. März 2010 in Stuttgart ein Eckpunktepapier mit dem Titel „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ verabschiedet und dieses anschließend als Druckbroschüre herausgegeben. Darin wird eine technikneutrale, internettaugliche und die Rechte der Betroffenen in den Vordergrund stellende Novellierung des Datenschutzrechts umrissen und eine bessere Kontrolle sowie leichtere Verständlichkeit der Regelungen gefordert. Die Broschüre wurde vom Konferenzvorsitzenden gedruckt und zur Verfügung gestellt. Die Landesbeauftragte hat die Eckpunkte im Land Brandenburg publik gemacht, um den Diskussionsprozess über eine grundlegende Modernisierung des deutschen Datenschutzrechts voranzubringen.

Für die Gewährleistung der Vertraulichkeit beim Umgang mit den Daten der Patientinnen und Patienten sind zunächst die Krankenhäuser selbst verantwortlich. Um sie dabei zu unterstützen, hat eine Expertengruppe die Orientierungshilfe „Krankenhausinformationssysteme“ mit rechtlichen und techni-

schen Hinweisen erarbeitet. Darin formulieren die Datenschutzbeauftragten erstmals einen bundeseinheitlichen Rahmen zum datenschutzgerechten Umgang mit Patientendaten in Krankenhausinformationssystemen. Die Orientierungshilfe richtet aber auch an die Hersteller von Krankenhausinformationssystemen. Die „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der gesetzlichen Krankenversicherung“ soll die Versicherungen dabei unterstützen, komplexe Verfahren zur Verarbeitung personenbezogener Daten nachvollziehbar zu machen und aussagekräftig zu protokollieren. Die Orientierungshilfe „Cloud Computing“ schließlich richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern. In den Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder, die für die Erstellung der Orientierungshilfen verantwortlich sind, hat die Landesbeauftragte mitgewirkt.

Sämtliche genannten Publikationen stehen in elektronischer Form auf der Website der Landesbeauftragten zur Verfügung.

Anlagen

1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1.1 82. Konferenz am 28./29. September 2011 in München

1.1.1 Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir“-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verant-

wortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

1.1.2 Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie

beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,

2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,

3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,

4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und

5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit

Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

1.1.3 Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

1.1.4 Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

1.1.5 Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der techni-

schen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.

- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.

- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.

- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.

- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.

- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

1.1.6 Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 02. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektro-

nischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

1.1.7 Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

1.2 Entschließung zwischen der 81. und 82. Konferenz vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder

hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

1.3 81. Konferenz am 16./17. März 2011 in Würzburg

1.3.1 Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[62] – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar.

---

62 Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

1.3.2 Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100a, 100b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

1.3.3 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landes-

krankenhausgesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

1.3.4 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html.

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)
- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

1.3.5 Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten

geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

1.3.6 Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90 / DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis

  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,

  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,

  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere

- zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.

- für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,

  - zur privaten Nutzung von Telekommunikationsdiensten,

  - zum Thema Whistleblowing,

  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,

  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,

  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

1.4 80. Konferenz am 3./4. November 2010 in Freiburg

1.4.1 Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,

- die größtmögliche Transparenz der Tätigkeit garantiert ist und

- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

1.4.2 Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

1.4.3 Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

1.5 Entschließungen zwischen der 79. und 80. Konferenz

1.5.1 Entschließung vom 11. Oktober 2010, Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

1.5.2 Entschließung vom 24. Juni 2010, Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer

  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat

  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs

  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept

  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

1.5.3 Entschließung vom 22. Juni 2010, Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu

einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen – weiterhin zu unterbleiben haben.

- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-) Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

1.6 79. Konferenz am 17./18. März 2010 in Stuttgart

1.6.1 Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereini-

gungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

1.6.2 Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),

- die Leistung, Wirkung sowie der Erfolg und die Effizienz,

- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

1.6.3 Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

1.6.4 Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

1.6.5 Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.

- Es darf keine Fach- und Rechtsaufsicht geben.

- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.

- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.

- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

2 Beschlüsse der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) seit dem 1. Juni 2010

2.1 Düsseldorfer Kreis am 22./23. November 2011

2.1.1 Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote - insbesondere Informationsdienste und Medieninhalte - nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das "auf der ganzen Linie" anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener "White Cards" erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. "Micropayment") zu erhalten.[63]

2.1.2 Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines "zugelassenen Wirtschaftsbeteiligten" (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern - und gegebenenfalls Daten Dritter - zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Daten-screenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht

63 vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!“

einheitlich umgesetzt. Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.

- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.

- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

2.2 Beschluss vom 8. Dezember 2011

Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr

dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen. Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten - soweit keine Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und –nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transpa-

renz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugins erhebt. Wenn sie die über ein Plugins mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

2.3 Düsseldorfer Kreis am 4./5. Mai 2011

2.3.1 Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“.

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

- **Transparenz bezüglich der Preisgabe personenbezogener Daten:**

In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- **Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:**

Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

- **Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:**

Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

- **Anonyme und pseudonyme Nutzungsmöglichkeiten:**

Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartpho-

nes; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport).

2.3.2 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Krankenhausinformationssysteme 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 Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Ge-

staltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

2.3.3 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem

1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von

Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

2.4 Beschluss vom 8. April 2011

Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.

- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.

- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

2.5 Düsseldorfer Kreis am 24./25. November 2010

2.5.1 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

2.5.2 Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.

- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer

Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

2.5.3 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Absatz 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle

   - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

   - umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,

- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

   - umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,

   - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),

   - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),

   - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und

   - Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt der Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.

3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.

4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.

5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

2.5.4 Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

3 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

3.1 23. Konferenz am 28. November 2011 in Berlin

Informationsfreiheit ins Grundgesetz und in die Landesverfassungen

Demokratie und Rechtsstaat können sich nur dort wirklich entfalten, wo auch die Entscheidungsgrundlagen staatlichen Handelns offen gelegt werden. Bund und Länder müssen ihre Bemühungen weiter verstärken, für mehr Transparenz staatlichen Handelns zu sorgen. Eine verfassungsrechtliche Verankerung der Informationsfreiheit ist geboten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland tritt dafür ein, den Anspruch auf freien Zugang zu amtlichen Informationen in das Grundgesetz und die Landesverfassungen – soweit noch nicht geschehen – aufzunehmen. Staatliche Stellen müssen die ihnen vorliegenden Informationen grundsätzlich öffentlich zugänglich machen.

3.2 22. Konferenz am 23. Mai 2011 in Bremen

3.2.1 Informationsfreiheit – Lücken schließen!

Der Gedanke der Transparenz staatlichen Handelns ist beim Bund und den meisten Ländern seit einigen Jahren angekommen, wie die Informationsfreiheitsgesetze von Brandenburg (1998), der meisten anderen Länder und auch das Informationsfreiheitsgesetz des Bundes (2005) zeigen.

Vor diesem Hintergrund begrüßt die Konferenz der Informationsfreiheitsbeauftragten die Absicht der neuen Landesregierung von Baden-Württemberg, auch dort ein Informationsfreiheitsgesetz auf den Weg zu bringen. Dabei sollte allerdings, wie in Rheinland-Pfalz vorgesehen, dem Landesbeauftragten für den Datenschutz die Aufgabe der oder des Beauftragten für die Informationsfreiheit übertragen werden. Diese unabhängige Funktion eines oder einer Informationsfreiheitsbeauftragten fehlt gegenwärtig auch noch in Thüringen. Bayern, Hessen, Niedersachsen und Sachsen lehnen dagegen beharrlich jede gesetzliche Regelung für einen Anspruch der Bürgerinnen und Bürger auf Zugang zu behördlichen Informationen ab.

Dies führt zu absurden Ergebnissen: So haben die Bürgerinnen und Bürger gegenüber den Jobcentern mit gemeinsamer Trägerschaft durch Bundesagentur für Arbeit und Kommune auch in den vier Ländern ohne Informationsfreiheitsgesetze einen Anspruch auf der Grundlage des Bundesgesetzes.

Dagegen besteht gegenüber den Jobcentern der Optionskommunen in ausschließlich kommunaler Trägerschaft in diesen Ländern kein Anspruch auf Informationszugang.

Unbefriedigend ist auch, dass die Bürgerinnen und Bürger bei Ersuchen auf Zugang zu Verbraucher- und Umweltinformationen nicht durchgängig die gesetzlich garantierte Möglichkeit haben, sich an die Informationsfreiheitsbeauftragten zu wenden. Eine Ombudsfunktion ist zwar in den meisten Informationsfreiheitsgesetzen vorgesehen, fehlt aber für Umwelt- und Verbraucherinformationen auf Bundesebene und in vielen Ländern.

Deshalb appelliert die Konferenz an die Gesetzgeber in Bund und Ländern, diese Regelungsdefizite zu beseitigen und „flächendeckend“ allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informationsfreiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln.

3.2.2 Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger!

Neue Technologien rufen bei Bürgerinnen und Bürgern nicht nur positive Reaktionen hervor, sondern stoßen häufig auf Skepsis oder lösen Ängste aus. Grund hierfür ist nicht selten eine unzureichende Informationslage bis hin zur Zurückhaltung von Informationen für Verbraucherinnen und Verbraucher. Wer das Potential neuer Technologien ausschöpfen möchte, muss mit offenen Karten spielen. Das bedeutet, dass nicht nur Vorteile, sondern auch Risiken offengelegt werden müssen, um einen demokratischen Diskurs und jedem Menschen eine informierte Willensbildung zu ermöglichen.

Ein aktuelles Beispiel ist der Einsatz von Nanotechnologie: Dabei geht es um künstlich hergestellte winzige Partikel (Nanomaterial), die heute schon in Baustoffen, Textilien sowie Kosmetika und zukünftig immer mehr in verbrauchernahen Produkten wie etwa Lebensmitteln eingesetzt werden. Nanotechnologie soll Produkte zum Beispiel robuster machen. In einem Bericht aus dem Jahre 2009 (nano.DE-Report 2009) geht das Bundesministerium für Wissenschaft und Forschung davon aus, dass nanotechnologisches Know-how in den Bereichen Gesundheit, Informations- und Kommunikations- sowie Energie- und Umwelttechnik immensen Einfluss auf die Wertschöpfung nehmen wird. Ein Weltmarktvolumen von 15 Prozent der globalen Güterproduktion wird prophezeit.

Wenigen ist dies bekannt, denn es besteht derzeit keine Pflicht, Produkte, die Nanomaterial enthalten, zu kennzeichnen. Erst 2013 wird eine solche Pflicht für Kosmetika bestehen. Für Lebensmittel wird die Kennzeichnungspflicht

noch diskutiert. Zugleich – stellt die Nano-Kommission der Bundesregierung in ihrem Aktionsplan Nanotechnologie 2015 fest – fehlen vielfach grundlegende Kenntnisse über die Risiken bei der Exposition mit Nanomaterialien.

Die Informationsfreiheitsbeauftragten in Deutschland fordern die Bundesregierung auf, sich bei den Diskussionen und Verhandlungen auf europäischer Ebene dafür einzusetzen, dass Bürgerinnen und Bürgern ein direkter Zugang zu Informationen über Nanotechnologie in Produkten ermöglicht wird. Deshalb ist es notwendig, dass auch Bürgerinnen und Bürger Zugang insbesondere zu dem auf europäischer Ebene diskutierten Nanoproduktregister erhalten. Beim Einsatz neuer Technologien muss verstärkt auf Aufklärung, Transparenz und Einbindung der Menschen gesetzt werden.

3.3 21. Konferenz am 13. Dezember 2010 in Kleinmachnow

3.3.1 Open Data: Mehr statt weniger Transparenz!

Die WikiLeaks-Debatte zeigt beispielhaft sowohl ein wachsendes Bedürfnis der internationalen Öffentlichkeit nach verbesserter Information und mehr Transparenz staatlichen Handelns als auch nach einem wirksamen rechtsstaatlichen Rahmen für den Zugang zu öffentlichen Informationen. Auch in Deutschland muss die Transparenz des politischen Handelns einen deutlich höheren Stellenwert bekommen, indem die rechtlichen und tatsächlichen Möglichkeiten zum Zugang zu staatlichen Informationen verbessert werden.

Die Informationsfreiheitsbeauftragten haben bereits vor vier Jahren die Verwaltungen aufgefordert, Informationen nicht erst auf Anfrage zu gewähren, sondern auch aus eigener Initiative im Internet zu veröffentlichen. Den Bürgerinnen und Bürgern soll damit der Zugang erleichtert und gleichzeitig der Aufwand für die öffentlichen Stellen mit der Bearbeitung von individuellen Anträgen auf Informationszugang reduziert werden.

Inzwischen ist einiges geschehen: Immer mehr Informationen, zum Beispiel über die Umwelt, Gerichtsentscheidungen, Parlamentsdokumente, amtliche Statistiken oder Vorlagen kommunaler Vertretungen, sind im Internet frei zugänglich. Aber immer noch fehlt ein Wegweiser durch die meist dezentral veröffentlichten Informationen ebenso wie ein einheitlicher technischer Standard, der die Weiterverwendung der Informationen erleichtern würde.

Beispiele aus dem In- und Ausland zeigen bereits heute, dass es möglich ist, eine Vielzahl von Informationen übersichtlich und über eine einheitliche Plattform zur Verfügung zu stellen. So kann Transparenz gleichermaßen einen Beitrag zur Stärkung der Demokratie und auch zur effizienten Aufgabenwahrnehmung der Verwaltung leisten.

3.3.2 Verträge zwischen Staat und Unternehmen offen legen!

Öffentliche Stellen des Bundes, der Länder und der Kommunen bedienen sich bei der Wahrnehmung ihrer Aufgaben vielfach privater Unternehmen: von großen Firmen, die öffentliche Infrastrukturprojekte verwirklichen, bis hin zu kleinen Betrieben, die für eine Gemeinde das Dorffest arrangieren. Dabei nimmt der Umfang des Outsourcing ständig zu und umfasst auch zentrale Felder der staatlichen Daseinsvorsorge. Die wesentlichen Inhalte und Konditionen werden dabei vertraglich fixiert.

Das Interesse der Öffentlichkeit an den Inhalten solcher Verträge ist groß, die Bereitschaft der Vertragspartner, sie offen zu legen, meist gering. Bisweilen wird privaten Geschäftspartnern sogar die Vertraulichkeit der Vertragsbestimmungen ausdrücklich zugesichert, um deren Offenbarung zu vermeiden.

Von besonderem öffentlichem Interesse sind aussagekräftige Informationen über öffentliche Gelder, die für bestimmte Leistungen bezahlt wurden, ob die Leistungen mit den zuvor ausgeschriebenen Anforderungen übereinstimmen und in welcher Höhe Steuermittel dafür aufgewendet werden. Diese Angaben dienen der Haushaltstransparenz und der Verhinderung von Korruption. Transparenz bei derartigen Verträgen ist auch deshalb besonders wichtig, weil hier nicht selten langfristige Weichenstellungen getroffen werden, die auch Parlamente späterer Legislaturperioden nicht mehr ändern können. Angaben hierüber dürfen der politischen Diskussion nicht vorenthalten werden.

Die Informationsfreiheitsbeauftragten fordern deshalb, die Verträge zwischen Staat und Unternehmen grundsätzlich offen zu legen. Die pauschale Zurückweisung von auf solche Verträge gerichteten Auskunftsbegehren unter Hinweis auf Vertraulichkeitsabreden und Betriebs- und Geschäftsgeheimnisse ist nicht länger hinnehmbar. Die Konferenz hält es deshalb für zwingend geboten, den Zugang zu entsprechenden Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies jüngst im Berliner Informationsfreiheitsgesetz (GVBl. Berlin 2010, Seite 358) geschehen ist.

3.4 20. Konferenz am 24. Juni 2010 in Berlin

Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten

Die Informationsfreiheit erfasst grundsätzlich alle Formen und Bereiche öffentlich-rechtlichen Handelns. Ihr Ziel ist es, Verwaltungsvorgänge transparenter zu gestalten und den Menschen die politische Mitgestaltung zu erleichtern. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland

weist deshalb darauf hin, dass das Recht auf Informationszugang auch gegenüber den öffentlich-rechtlichen Rundfunkanstalten als Trägern mittelbarer Staatsverwaltung gilt, sofern nicht deren grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit berührt ist.

Die Rundfunkfreiheit garantiert den Schutz vor staatlicher Kontrolle und Beeinflussung. Eine Öffnung aller Sendeanstalten außerhalb dieses geschützten Kernbereichs für die Informationsbelange der Bürgerinnen und Bürger gefährdet diese Freiheit nicht. Offenheit und Transparenz sind keine Bedrohungen, sondern schaffen Vertrauen in der Bevölkerung. Die Geltung der Informationsfreiheitsgesetze wird die Rundfunkanstalten daher in ihrem demokratischen Auftrag und Selbstverständnis nachhaltig stärken.

Die derzeitige Rechtslage ist aufgrund unterschiedlicher Landesgesetze uneinheitlich. Während in einigen Bundesländern die Anwendbarkeit des Informationsfreiheitsgesetzes ausdrücklich festgeschrieben oder ausgeschlossen ist, ergibt sie sich in anderen Bundesländern nur aus allgemeinen Regeln. Einige Sendeanstalten der ARD sind zudem in Ländern ansässig, in denen noch immer kein Informationsfreiheitsgesetz gilt.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb die Schaffung ausdrücklicher Rechtsvorschriften, sofern nicht schon vorhanden, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind.

4 Abkürzungsverzeichnis

ABl. EU	=	Amtsblatt der Europäischen Union
Abs.	=	Absatz
AfSBB	=	Amt für Statistik Berlin-Brandenburg
AG	=	Arbeitsgruppe
AIG	=	Akteneinsichts- und Informationszugangsgesetz
AO	=	Abgabenordnung
AOK	=	Allgemeine Ortskrankenkasse
ARGE	=	Arbeitsgemeinschaft
Art.	=	Artikel
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BDSG	=	Bundesdatenschutzgesetz
BGBl.	=	Bundesgesetzblatt
BRAVORS	=	Brandenburgisches Vorschriftensystem
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
bzw.	=	beziehungsweise
CNPD	=	Commission Nationale pour la Protection des Données
DIN	=	Deutsches Institut für Normung
DSV	=	Datenschutzverordnung Schulwesen
DV	=	Datenverarbeitung
EDV	=	elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft
eID	=	elektronische Identität
ELENA	=	Verfahren des elektronischen Entgeltnachweises
ELSTER	=	elektronische Steuererklärung
endg.	=	endgültig
EntgFG	=	Entgeltfortzahlungsgesetz
EnWG	=	Energiewirtschaftsgesetz
EU	=	Europäische Union
GEZ	=	Gebühreneinzugszentrale
GmbH	=	Gesellschaft mit beschränkter Haftung
GVBl.	=	Gesetz- und Verordnungsblatt
HBCI	=	Homebanking Computer Interface
IaaS	=	Infrastructure as a Service
IP	=	Internet Protokoll
IPv4	=	Internet Protokoll Version 4
IPv6	=	Internet Protokoll Version 6
IT	=	Informationstechnik
iTAN	=	indizierte Transaktionsnummer
i. V. m.	=	in Verbindung mit

Kfz	=	Kraftfahrzeug
KunstUrhG	=	Kunsturhebergesetz
LAN	=	Lokal Area Network
LBG	=	Landesbeamtengesetz
LPAR	=	Logical Partition
LStR	=	Lohnsteuerrichtlinie
LuftVG	=	Luftverkehrsgesetz
LVN	=	Landesverwaltungsnetz
MdF	=	Ministerium der Finanzen
mTAN	=	mobile Transaktionsnummer
NAT	=	Network Adress Translation
NFM	=	Neues Finanzmanagement
Nr.	=	Nummer
o. Ä.	=	oder Ähnliches
OWiG	=	Ordnungswidrigkeitengesetz
PaaS	=	Platform as a Service
PIN	=	persönliche Identifikationsnummer
QES	=	qualifizierte elektronische Signatur
RFID	=	Radio Frequency Identification
RIO	=	Ressort Information Officer
S.	=	Seite
SaaS	=	Software as a Service
SGB X	=	Zehntes Buch Sozialgesetzbuch
SIS	=	Sicherheitsinformationssystem
SNC	=	Secure Network Communication
SSL	=	Secure Socket Layer
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
TAN	=	Transaktionsnummer
TFA	=	Technisches Finanzamt
TUIV-AG	=	Kommunale Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg
TV	=	Tarifvertrag
u. a.	=	unter anderem
vgl.	=	vergleiche
z. B.	=	zum Beispiel
ZBB	=	Zentrale Bezügestelle des Landes Brandenburg
ZIT-BB	=	Brandenburgischer IT-Dienstleister

5 Stichwortverzeichnis