Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2005

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 8. März 2004 vorgelegten Tätigkeitsbericht 2003 an und deckt erstmals einen zweijährigen Zeitraum vom 1. Januar 2004 bis zum 31. Dezember 2005 ab.

Die „Dokumente zu Datenschutz und Informationsfreiheit“ für die Jahre 2004 und 2005, auf die in diesem Bericht verwiesen wird, hat die Landesbeauftragte gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit als gesonderten Anlagenband veröffentlicht. Tätigkeitsbericht und Anlagenband sind auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abrufbar.

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: Gallus Druckerei KG, Berlin

Inhaltsverzeichnis Seite

Anlagen

Verzeichnis der öffentlichen Stellen **Gliederungspunkt**

Einleitung

Die beiden zurückliegenden Berichtsjahre 2004 und 2005 zeigen deutlich die stetig wachsende Bedeutung des technischen Datenschutzes durch immer neuere und schnellere technische Entwicklungen. Auf der rechtlichen Seite stehen zwei sehr unterschiedliche Tendenzen, einerseits zahlreiche Entscheidungen des Bundesverfassungsgerichts, das das Recht auf informationelle Selbstbestimmung des Einzelnen durch die Forderung zur Wahrung rechtsstaatlicher Grundsätze gestärkt hat und andererseits eine zunehmende Zahl von Gesetzen, die die Daten verarbeitenden Stellen zur Vorratsdatenverarbeitung verpflichten.

Die Weiterentwicklung technischer Produkte sowie die Entwicklung neuer Produkte ist nie zuvor in so schnellem Tempo erfolgt. Inzwischen spricht man von „Ubiquitous Computing“, was so viel wie „allgegenwärtiges Rechnen“ bedeutet, d. h. unsere Alltagsgegenstände werden durch das Anbringen von Sensoren und Chips mit Rechnerqualitäten ausgestattet. Gegenstände können in Zukunft miteinander vernetzt werden. Die Technik der Zukunft wirft für den Datenschutz viele neue Fragen auf. Neue Technologien wie RFID oder Voice over IP, d. h. die so genannte Internet-Telefonie, haben Eingang in unseren alltäglichen Sprachgebrauch gefunden und zeigen ebenfalls eine Veränderung unseres Alltags auf. Mit diesen Techniken sind nicht nur Chancen verbunden, sie bergen für die Nutzer auch Risiken in sich, die leicht übersehen oder zumindest unterschätzt werden. Zunehmend wichtiger werden damit auch Datensicherheit und Datenschutzinformationen für die Nutzer dieser Technologien. Datenschutz muss in Zukunft als Qualitätsfaktor erkannt werden; er steht der technischen Entwicklung nicht entgegen, sondern muss sie begleiten. Nur so werden die technischen Entwicklungen akzeptiert und nicht als Bedrohung der eigenen Privatsphäre empfunden.

Das Urteil des Bundesverfassungsgerichts zum „Großen Lauschangriff“ vom 3. März 2004 hat erstmals in großer Deutlichkeit die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung festgeschrieben. In diesen letzten Rückzugsraum dürfen staatliche Strafverfolgungsbehörden nicht vordringen. Auch in seiner Entscheidung zur präventiven Telefonüberwachung im Rahmen der Überprüfung des Polizeigesetzes des Landes Niedersachsen hat das Bundesverfassungsgericht im Sommer 2005 zum wiederholten Male auf die von den Datenschutzbeauftragten eingeforderten rechtsstaatlichen Maßstäbe hingewiesen.

Die eindeutige Rechtssprechung des Bundesverfassungsgerichts hat bisher nicht dazu geführt, dass diese Maßstäbe bei Gesetzesvorhaben ausreichend berücksichtigt werden. Zahlreiche Entscheidungen des Gesetzgebers in den beiden letzten Jahren ließen datenschutzrechtliche Fragen offen oder beant-

worteten sie nur unzureichend. So enthält der Reisepass in Deutschland seit dem 1. November 2005 erstmals einen per Funk auslesbaren RFID-Chip, auf dem u. a. biometrische Daten gespeichert sind. Deutschland hat damit als Vorreiterland die Vorgaben einer EU-Verordnung umgesetzt. Die Bedenken der Datenschutzbeauftragten hinsichtlich der Sicherheit der eingesetzten Technologien wurden hintenangestellt. Kontrollen müssen nun zeigen, welche datenschutzrechtlichen Probleme in der Praxis tatsächlich auftreten. In der Presse wird bereits über Missbrauchsmöglichkeiten berichtet.

Die Tendenz zur Vorratsdatenspeicherung setzt sich weiter fort. So hat das EU-Parlament nach längeren Diskussionen eine Richtlinie beschlossen, die die Anbieter von Telekommunikations- und Internetdiensten verpflichtet, umfangreiche Verkehrsdaten auf Vorrat für die Sicherheitsbehörden zu speichern, ohne dass ein konkreter Verdacht oder Hinweise auf eine bevorstehende Gefahr vorliegen. Es wird nun Aufgabe der Datenschutzbeauftragten sein, sich dafür einzusetzen, dass die von der Richtlinie vorgesehenen Spielräume für die Umsetzung in innerstaatliches Recht soweit wie möglich genutzt werden, um dem Grundrecht auf informationelle Selbstbestimmung und damit dem Datenschutz ausreichend Geltung zu verschaffen. Leider werden Sicherheit und Datenschutz zunehmend als unvereinbare Gegensätze betrachtet und Sicherheitsaspekte im Ergebnis häufig zulasten des Datenschutzes bevorzugt. Die Frage aber, was ein Mensch ohne Freiheit ist, bleibt unbeantwortet. Sicherheit und Datenschutz schließen sich keineswegs aus. Der Datenschutz wird es jedoch zunehmend schwerer haben, wenn internationale Bedrohungen das Denken und Handeln in der Gesetzgebung bestimmen. Jedenfalls haben die vergangenen Jahre gezeigt, dass es ein Freiheitsrecht schwer hat, wenn Ängste im Spiel sind. Möge der Satz „Die Freiheit stirbt zuletzt“ am Ende doch stimmen.

Im Sommer 2005 hat die Europäische Kommission gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren eingeleitet. Nach Auffassung der Kommission ist die derzeitige Organisation der für die Überwachung der Datenverarbeitung im nicht öffentlichen Bereich zuständigen Kontrollstellen nicht mit dem Gemeinschaftsrecht vereinbar. Sie verstößt gegen die Forderung der EU-Datenschutzrichtlinie von 1995 nach „völliger Unabhängigkeit“ der Aufsichtsstellen. Dies betrifft auch die Organisation der Datenschutzaufsicht über den nicht öffentlichen Bereich im Land Brandenburg. In Brandenburg übt das Innenministerium die Aufsicht über den privaten Bereich aus. Nach Auffassung der Europäischen Kommission fehlt es bei dieser Organisationsform an der völligen Unabhängigkeit der Aufsicht, da die Aufsichtsbehörde in die Organisationsstruktur des Ministeriums eingebunden ist. Unabhängig von der rechtlichen Bewertung der Europäischen Kommission wird eine geteilte Aufsicht über den privaten und den öffentlichen Bereich von Rat Suchenden offensichtlich nicht erwartet. Meine Behörde leitet jeden Monat zahl-

reiche Anfragen, die die Aufsicht über den nicht öffentlichen Bereich betreffen, zur weiteren Bearbeitung an das Innenministerium weiter. Gerade vor dem Hintergrund des viel diskutierten Bürokratieabbaus und auch der Bürgerfreundlichkeit stellt sich die Frage, ob eine einheitliche Aufsichtsbehörde hier nicht sinnvoller wäre. Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Oktober 2005 in einer Entschließung für eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit ausgesprochen.[1]

Die Entwicklung des Datenschutzes im Land Brandenburg hat gezeigt, dass dem Einsatz moderner Technik immer mehr Bedeutung zukommt. Einige Stichworte sind E-Government, IT-Sicherheitsleitlinie, Meldedaten-Online oder die Einführung der Kosten- und Leistungsrechnung. Neue Technologien erfordern den Einsatz modernster Sicherheitstechnik. Gemeinsame Positionen der Verwaltungen sind nicht immer zu erkennen, wenn die Erfordernisse des Datenschutzes von einigen Verwaltungen als bürokratischer Hemmschuh abgetan werden. Trotz dieser Schwierigkeiten sehe ich hier aber trotzdem den Wunsch der Landesregierung, an einer gemeinsamen Linie zu arbeiten und werde mich dafür einsetzen, dass Datenschutz als Qualitätsfaktor eines modernen E-Governments einen angemessenen Stellenwert erhält.

Ein Fall, der 2005 durch die Presse ging, hat im Land Brandenburg ganz unerwartet Fragen der Datensicherheit in die Diskussion gebracht. Ein Student ersteigerte bei einem Internetauktionshaus eine Festplatte, die polizeiliche Daten enthielt. Ein inzwischen ehemaliger Mitarbeiter der Polizei hatte Festplatten entwendet. Dieser Fall hat deutlich gemacht, dass Angriffe auf die Datensicherheit nicht nur von außen zu erwarten sind, sondern auch die Mitarbeiterinnen und Mitarbeiter der Verwaltungen ein Gefährdungspotenzial darstellen können. Verschlüsselung, Zugriffsbefugnisse und Protokollierungen sind, um nur einige Maßnahmen zu nennen, keine übertriebenen Sicherheitsmaßnahmen, sondern tragen dazu bei, ein immer bestehendes Restrisiko zu minimieren.

Ein weiteres, den Datenschutz bestimmendes Thema war in Brandenburg wie in der ganzen Bundesrepublik Deutschland die Einführung des Arbeitslosengeldes II, d. h. die Umsetzung des sog. Hartz IV-Gesetzes. Hier lagen Licht und Schatten dicht nebeneinander. Die Mängel des Zweiten Buches Sozialgesetzbuch stellten für die neu eingerichteten Job-Center und die optierenden Kommunen, die diese Aufgabe übernommen haben, eine wahre Herausforderung dar. Gerade der Schutz von Sozialdaten hat für die betroffenen Menschen eine große Bedeutung; dies wurde durch die konstant hohe Zahl der Anfragen und Beschwerden, die uns hierzu erreichten, bestätigt. Eine gute Erfahrung war das schnelle Reagieren einiger Verwaltungen auf festge-

[1] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 3

stellte Mängel; bei anderen gestaltete sich dagegen die Beseitigung der Mängel schwierig. Wir haben uns in diesem Zusammenhang mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und anderen Landesdatenschutzbeauftragten und erstmals im Dialog mit der Bundesagentur für Arbeit zusammen um eine gemeinsame Lösung datenschutzrechtlicher Probleme bemüht. Es liegt jedoch noch viel Arbeit vor uns.

Die Anforderungen an den Datenschutz sind in den beiden vergangenen Jahren immer größer geworden. Es wird künftig entscheidend sein, ob die Datenschutzbeauftragten die Bedeutung des Datenschutzes und damit seinen Wert für den Einzelnen und auch die Gemeinschaft hinreichend deutlich machen können. Ich werde jedenfalls als Beauftragte für den Datenschutz und für das Recht auf Akteneinsicht nicht nachlassen, in Brandenburg Verbündete für dieses Vorhaben zu suchen. Dies gilt auch für das Recht auf Akteneinsicht, das darauf wartet, zu einem ganz selbstverständlichen Recht zu werden. Informationsfreiheit muss schließlich genutzt werden, um das Ziel der Transparenz zu erreichen. Hier ist noch weitere Öffentlichkeitsarbeit zu leisten. Wir bieten den Verwaltungen außerdem bei Bedarf Unterstützung an, um dieses Recht des Bürgers routiniert umzusetzen.

Der Rückblick auf die beiden vergangenen Jahre zeigt, dass sowohl für den Datenschutz als auch für das Recht auf Akteneinsicht weiterhin viel Arbeit auf meine Behörde wartet.

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Biometrische Merkmale in Pässen

Seit dem 1. November 2005 werden in Deutschland neue Reisepässe ausgegeben. Diese enthalten einen zusätzlichen Funkchip, auf dem neben den herkömmlichen Passdaten erstmals auch biometrische Merkmale des Passinhabers gespeichert sind. Die Datenschutzbeauftragten des Bundes und der Länder haben in diesem Zusammenhang wiederholt auf eine Reihe rechtlicher, technischer und gesellschaftlicher Probleme hingewiesen.

Die Bundesregierung ist eine der ersten Regierungen Europas, die mit der Ausgabe elektronisch auslesbarer, biometriegestützter Reisepässe eine entsprechende EU-Verordnung aus dem Jahr 2004 umsetzt. Die wesentlichen Ziele, die mit dem Projekt ePass verfolgt werden, sind einerseits die weitere Erhöhung der ohnehin schon sehr hohen Fälschungssicherheit der Pässe durch einen Speicherchip als zusätzliches Sicherheitsmerkmal und andererseits der Schutz vor Missbrauch eines Passes durch andere Personen als den eigentlichen Passinhaber. Letzteres soll durch den zusätzlichen automatisierten Vergleich der auf dem Chip gespeicherten biometrischen Merkmale mit denen der kontrollierten Person erfolgen. Bei der konkreten Ausgestaltung der Pässe, der Festlegung der zu verwendenden biometrischen Merkmale und der technischen Realisierung der Speicherung auf dem Chip folgte die EU den Empfehlungen einer Arbeitsgruppe der Internationalen Organisation für zivile Luftfahrt (ICAO), die sich mit der Standardisierung und Gewährleistung der Interoperabilität maschinenlesbarer Reisedokumente befasst. Nur durch die Einhaltung der Empfehlungen kann gesichert werden, dass die internationale Reisefreiheit nicht bereits an technischen Schranken scheitert.

1.1.1 Verwendete biometrische Merkmale und Verfahren

Bei den aktuell ausgegebenen Pässen wird neben den herkömmlichen Passdaten das Gesichtsbild des Passinhabers auf dem Chip gespeichert. Die ICAO betrachtet das Gesichtsbild als primäres und obligatorisches biometrisches Merkmal auf Grund der Kompatibilität mit existierenden Verfahren, der weltweit hohen Akzeptanz und der zu erwartenden niedrigen Ausfallrate bei der Datenerhebung. Weitere, sekundäre biometrische Merkmale, die aus Sicht der ICAO optional gespeichert werden können, sind z. B. Fingerabdrü-

cke oder Irismuster. Die EU-Verordnung sieht vor, dass im Bereich der EU-Staaten Fingerabdrücke als zusätzliches Merkmal im Chip abgelegt werden; Deutschland will damit bei den ab März 2007 ausgestellten Pässen beginnen.

Aus Sicht des Datenschutzes wäre die Speicherung von Templates, die durch Extraktion spezifischer Merkmale aus den biometrischen Daten gewonnen werden, der Speicherung der vollständigen Rohdaten (z. B. als Bilddatei) vorzuziehen. Diese datensparsame Variante wurde jedoch von der ICAO mit der Begründung abgelehnt, dass eine globale Nutzung der Daten bei weltweit möglichen Kontrollen und ein späterer Austausch bei Verfügbarkeit besserer Erkennungsmethoden proprietäre Verfahren der Gewinnung und Verwendung der Templates ausschließen.

In den vergangenen Jahren wurde eine Reihe von Studien zur Einschätzung der Leistungsfähigkeit biometrischer Verfahren durchgeführt. In Deutschland waren daran u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) beteiligt. In allen Studien wurden gespeicherte biometrische Daten mit den aktuell aufgenommenen verglichen. Die Häufigkeit einer fehlerhaften Zurückweisung des Kontrollierten lagen je nach Nutzergruppe und technischer Ausgestaltung des Systems bei Gesichtserkennungssystemen zwischen 2 % und 10 %, bei Fingerabdrucksystemen zwischen 1 % und 7 %. Die höheren Fehlerraten waren insbesondere bei Wenignutzern festzustellen. Für diese Nutzergruppe ist deshalb im Vergleich zu geübten Vielnutzern bei automatisierten Grenzkontrollen mit häufigeren (unberechtigten) Abweisungen und einem zusätzlichen Zeitaufwand für genauere Kontrollen durch Grenzbeamte zu rechnen. Bei den Tests wurde auch eine hohe Abhängigkeit der Fehlerraten von den Umgebungsbedingungen (z. B. Lichtverhältnisse) während der Kontrolle festgestellt.

Weiterhin liegen keine gesicherten Erkenntnisse zur Überwindungssicherheit der getesteten Systeme vor. Einzelne durchgeführte Labortests lassen nur vorläufige Aussagen zu. Gerade vor dem Hintergrund der teilweise sehr öffentlichkeitswirksam dargestellten Möglichkeiten, mit relativ einfachen Mitteln Fingerabdruck- und Gesichtserkennungssysteme zu überlisten, sollten auch die Datenschutzbeauftragten bereits vorliegende Ergebnisse erhalten und in weitere Untersuchungen einbezogen werden.

Kritisch zu beurteilen ist auch die Erprobung der Verfahren für einen nur begrenzten, nicht repräsentativen Personenkreis. Eine Übertragung der Studienergebnisse auf große Bevölkerungsgruppen ist deshalb nicht ohne weiteres möglich. Die Studienautoren verweisen darauf, dass sich bis zur flächendeckenden und routinemäßigen Nutzung biometrischer Verfahren sowohl die Erkennungstechnik selbst als auch deren Benutzerfreundlichkeit verbessern

werden. Offen bleibt die Frage nach den Auswirkungen für diejenigen Betroffenen, die bereits heute die Technik nutzen müssen.

1.1.2 Funkchips und Kommunikation mit den Passlesegeräten

Die ICAO empfiehlt die Nutzung eines kontaktlos auslesbaren Chips zur Speicherung der biometrischen Daten des Passinhabers. Andere Varianten der Speicherung (z. B. kontaktbehaftete Chipkarten, Magnetstreifen, optische Speicher oder zweidimensionale Strichcodes) wurden zwar betrachtet, erwiesen sich jedoch als nicht kompatibel zu existierenden Dokumentformaten oder als zu anfällig gegenüber Verschmutzungen.

In den aktuell ausgegebenen Pässen kommen RFID-Chips[2] zum Einsatz, die nur aus einer geringen Entfernung von einigen Zentimetern auslesbar sind. Ein zusätzliches Merkmal ist die wechselnde Seriennummer: Bei jeder Kommunikation mit einem Lesegerät antworten die verwendeten Chips mit einem anderen Identifikator, sodass die Bildung von Profilen des Passinhabers allein aus der Kenntnis dieses Datums erschwert wird. Alle auf dem Chip gespeicherten Daten sind von der den Pass ausstellenden Behörde digital signiert.

Trotz der geringen Reichweite der Funkkommunikation bestehen bei den verwendeten RFID-Chips Gefahren durch das unberechtigte Auslesen der gespeicherten Daten und durch das Mithören und Decodieren der Kommunikation zwischen Chip und Lesegerät. Um diesen Gefahren zu begegnen, wurden unter maßgeblicher Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik Sicherheitsmaßnahmen entwickelt, die unter dem Namen „Basic Access Control“ zusammengefasst werden und der Zugriffskontrolle auf die gespeicherten Daten dienen. Danach ist zunächst der optische Zugriff des Lesegeräts auf die maschinenlesbare Zone des Passes erforderlich. Aus den von dort gelesenen Daten berechnet das Lesegerät einen Zugriffsschlüssel, mit dem die nachfolgende Funkkommunikation zwischen RFID-Chip und Lesegerät verschlüsselt wird. Kritisch anzumerken ist, dass die in der maschinenlesbaren Zone des Passes vorhandenen Daten relativ frei verfügbar (z. B. auf Antragsformularen für Tickets zur Fußball-WM 2006) oder teilweise sogar aus Zusatzinformationen zu erraten sind. Auch ist die Stärke des errechneten kryptografischen Schlüssels nicht besonders hoch. Die Verantwortlichen im Bundesinnenministerium und im Bundesamt für Sicherheit in der Informationstechnik halten das gewählte Verfahren jedoch für ausreichend, da nur schwach sensible Daten des Passinhabers (Stammdaten und Gesichtsbild) betroffen sind. Ob diese Aussage berechtigt ist, wird die Praxis zeigen.

---

[2] vgl. A 1.2

Für das Auslesen der ab 2007 in den Pässen gespeicherten Fingerabdrücke werden zusätzliche Sicherheitsmaßnahmen vorgesehen („Extended Access Control“). Insbesondere sind die Verwendung starker kryptografischer Verfahren, die Authentifizierung des Lesegerätes gegenüber dem Chip und eine strenge Einschränkung des Zugriffs auf Fingerabdrücke für einzelne, vertrauenswürdige Länder geplant. Nach dem aktuellen Stand soll das Auslesen der Fingerabdrücke nur den so genannten Schengen-Staaten gestattet werden.

1.1.3 Forderungen der Datenschutzbeauftragten zu biometrischen Pässen

Die Datenschutzbeauftragten des Bundes und der Länder haben im Vorfeld der Einführung biometriegestützter, elektronisch auslesbarer Reisepässe in Deutschland eine gemeinsame Entschließung[3] verabschiedet, in der sie wesentliche Fragen und Kritikpunkte an dem Projekt zusammenfassen. Bis zum heutigen Tag sind die aufgeführten Probleme nur in Ansätzen gelöst.

Insbesondere fordern die Datenschutzbeauftragten die strenge Zweckbindung der biometrischen Daten der Passinhaber. Die Daten sind ausschließlich bei Passkontrollen für hoheitliche Zwecke zu nutzen. Auf ihre Speicherung in zentralen oder vernetzten Datenbanken ist zu verzichten. Während der letzte Punkt in Deutschland zurzeit rechtlich ausgeschlossen ist, planen andere EU-Staaten offiziell die Einrichtung nationaler Datenbanken mit den Daten aller ausgegebenen Pässe einschließlich der biometrischen Daten. Generell ist auf internationaler Ebene nicht garantiert, dass Staaten darauf verzichten, die Stammdaten und biometrischen Merkmale der Passinhaber nach dem Auslesen der Pässe in Datenbanken zu speichern.

Darüber hinaus ist zu verhindern, dass in Pässen gespeicherte Daten als Referenzdaten für die Verknüpfung mit Daten aus anderen Systemen oder Kontexten genutzt werden. Prinzipiell würden sich biometrische Daten zwar auch als eindeutiges Personenkennzeichen eignen, ihre derartige Verwendung oder gar die Nutzung zur Bildung von Bewegungs- und Verhaltensprofilen der Passinhaber wäre datenschutzrechtlich jedoch unzulässig.

Ein weiterer wesentlicher Kritikpunkt ist die bislang nur unzureichende Festlegung und Umsetzung von technischen und organisatorischen Maßnahmen, die die Wahrung des Rechts auf informationelle Selbstbestimmung des Passinhabers sicherstellen. Die oben aufgeführten Maßnahmen zur Absicherung der Funkkommunikation zwischen RFID-Chip und Lesegerät sowie zur Kontrolle des Zugriffs auf die gespeicherten Daten helfen zwar, die Vertraulichkeit zu sichern, beschränken sich jedoch nur auf einen kleinen Teil des Gesamtsystems. Ein umfassendes Datenschutz- und Sicherheitskonzept ist noch

[3] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 2

nicht verfügbar. Dieses muss u. a. auch einen Missbrauch bei der Erfassung der biometrischen Daten sowie bei der Herstellung des Passes verhindern und eine Zertifizierung der verwendeten Geräte auf der Basis internationaler Standards vorsehen.

Sämtliche Forderungen gelten auch für die Aufrüstung von Personalausweisen mit elektronisch auslesbaren Speicherchips und biometrischen Daten. Dieses Projekt ist von der Bundesregierung für den Zeitraum ab Ende 2007 geplant.

Die Einführung biometriegestützter Reisepässe in Deutschland erfolgt zu einem Zeitpunkt, zu dem viele Fragen noch nicht abschließend geklärt sind. Auch ist bislang nicht erwiesen, dass durch die neue Technik ein echter Sicherheitsgewinn erzielt wird. Auf eine breite gesellschaftliche Diskussion zum Thema ePass wurde leider verzichtet. Unter Fachleuten ist umstritten, ob die mit der Verarbeitung biometrischer Daten verbundenen Risiken mit heutigen Herangehensweisen und Techniken überhaupt beherrschbar sind.

1.2 Von funkenden Mikrochips zur allgegenwärtigen Datenverarbeitung

In den letzten Jahren ist eine rasante Entwicklung in der Forschung und Anwendung von RFID-Chips zu verzeichnen. Bezüglich Datenschutz und Datensicherheit beim Einsatz von RFID-Systemen sind ähnlich große Fortschritte jedoch nur in einzelnen Teilbereichen zu beobachten.

Die mit dem Begriff Radio Frequency Identification (RFID) bezeichnete Technik zur Identifizierung von Objekten per Funkkommunikation ist bereits über 50 Jahre alt. Ihr Einsatz war lange auf militärische Zwecke beschränkt. Im Zuge der Miniaturisierung, des Preisverfalls und der Leistungssteigerung wurde sie in der jüngeren Vergangenheit auch für andere Bereiche interessant. Insbesondere Warenwirtschaft und Logistik versprechen sich durch die Ausstattung von Einzelprodukten oder Paletten mit RFID-Chips und ihre automatische Identifikation oder Verfolgung erhebliche Kosteneinsparungen sowie Verbesserungen der Lieferprozesse. Auch der Endkunde des Einzelhandels kommt mit den Chips in Berührung, wenn sie auf Konsumgütern als Ersatz der herkömmlichen Strichcodes genutzt werden. Weitere Einsatzgebiete sind z. B. die Zutrittskontrolle oder die Bezahlung von Fahrkarten im Nahverkehr durch kontaktlos auslesbare Chipkarten, das Einbringen von Chips in Eintrittskarten für die Fußball-WM 2006[4] zur Erhöhung der Fälschungssicherheit und Unterbindung des Schwarzhandels, die Speicherung

[4] vgl. A 5.1.2

biometrischer Daten auf RFID-Chips in Pässen[5], die Kennzeichnung von Tieren durch unter die Haut injizierte Chips sowie die Echtheitsprüfung und Verfolgung von Arzneimitteln oder von Ersatzteilen für Wartungsprozesse. Viele der zum Zeitpunkt unseres letzten Tätigkeitsberichts noch geplanten Projekte sind inzwischen bereits Realität oder in der Phase der Umsetzung.

1.2.1 Überblick über technische Grundlagen

Ein RFID-System besteht mindestens aus einem RFID-Chip (auch als RFID-Tag bezeichnet), der an dem zu identifizierenden Objekt angebracht ist, und einem RFID-Lesegerät. Der RFID-Chip, dessen Fläche kleiner als ein Quadratmillimeter sein kann, arbeitet nach dem Transponder-Prinzip: er empfängt mithilfe einer externen Antenne über Funk Signale vom Lesegerät und liefert daraufhin die auf ihm gespeicherten Daten zurück. Im einfachsten Fall einer Diebstahlsicherung für Produkte in einem Warenhaus ist dies ein einzelnes Bit (bezahlt/nicht bezahlt). Die aktuell größte Speicherkapazität von bis zu Hundert Kilobyte haben Chips für Pässe und Ausweise, auf denen biometrische Daten der Inhaber gespeichert werden. Neben RFID-Chips, die nur auslesbar sind, existieren solche, die ein- oder mehrfach beschrieben werden können. Auch bezüglich der Möglichkeiten der Datenverarbeitung direkt auf dem Chip kann zwischen verschiedenen Typen differenziert werden. Die Palette reicht von „dummen“ RFID-Chips, die nur die gespeicherten Daten zurückliefern, bis hin zu Chips, die über eine eigene Verarbeitungskapazität, z. B. zur Verschlüsselung, verfügen.

Weitere Klassifikationskriterien für RFID-Chips sind die Art der Energieversorgung (passive Chips gewinnen ihre Energie aus der Funkkommunikation, aktive Chips verfügen über eine eigene Batterie), die verwendete Übertragungsfrequenz und die Reichweite der Funkkommunikation. Letztere kann entsprechend der verwendeten Chiptypen und der Übertragungstechnik zwischen wenigen Zentimetern und einigen Metern liegen. Befinden sich mehrere RFID-Chips in Reichweite eines Lesegerätes, so lassen sich diese anhand einer eindeutigen Seriennummer unterscheiden.

Als weiterer wichtiger Bestandteil von RFID-Systemen sind die mit dem Lesegerät verbundenen Komponenten zur Weiterverarbeitung der RFID-Daten zu nennen, die so genannten Hintergrundsysteme. Dies können Datenbanken z. B. zur Identifikation des Produktes anhand eines auf dem Chip gespeicherten Codes, Warenwirtschafts- und Logistiksysteme zur Planung von Lieferprozessen oder Steuerungen für Türöffner, Roboter, Förderbänder usw. sein.

[5] vgl. A 1.1

Obwohl RFID-Systeme heute schon relativ weit verbreitet sind und in verschiedenen Szenarien eingesetzt werden, stehen ihrer flächendeckenden Nutzung noch einige Probleme entgegen. Gerade bei der Kennzeichnung einzelner Handelsprodukte erweisen sich der noch relativ hohe Stückpreis (je nach Eigenschaften und Leistungsfähigkeit des Chips zwischen 30 Cent und mehreren Euro), die unzureichende Standardisierung der Datenformate und Funkkommunikation, Schwierigkeiten beim Auslesen in ungünstigen Umgebungsbedingungen (z. B. bei Vorhandensein von Metall oder Flüssigkeiten) und die Pulkerfassung einer großen Menge von Chips als Hemmnisse. Es ist jedoch davon auszugehen, dass die genannten Herausforderungen in naher Zukunft gemeistert werden.

1.2.2 Bedrohungen für den Datenschutz und die Datensicherheit

Auf Grund der großen Anzahl verschiedener Typen von RFID-Chips mit unterschiedlichen Eigenschaften, Leistungsparametern und diversen Nutzungsmöglichkeiten sind für jedes konkrete RFID-System im Vorfeld des Einsatzes die spezifischen Bedrohungen zu analysieren und ggf. geeignete Maßnahmen abzuleiten. Neben Maßnahmen zur Gewährleistung des Datenschutzes für die Betroffenen (d. h. die „Träger“ der RFID-Chips) sind aus der Sicht des Anwenders bzw. Betreibers auch Maßnahmen für die Datensicherheit zu ergreifen. Diese sichern das ordnungsgemäße und zuverlässige Funktionieren des Systems.

Bezüglich des Datenschutzes ist zunächst zu unterscheiden, an welcher Stelle im RFID-System personenbezogene Daten auftreten. Folgende Varianten existieren:

- Personenbezogene Daten werden direkt auf dem RFID-Chip gespeichert. Ein Beispiel hierfür sind die seit November 2005 neu ausgegebenen Reisepässe, bei denen die Daten des Inhabers und ausgewählte biometrische Merkmale auf dem Chip abgelegt sind.
- Auf dem Chip gespeicherte Daten wie z. B. ein elektronischer Produktcode, eine ISBN oder ein Arzneimittelcode werden mit personenbezogenen Daten verknüpft. Dies erfolgt im Allgemeinen durch das Hintergrundsystem, z. B. beim Einkauf mit einer Kunden- oder Kreditkarte. Auch Dritte, mit denen keine direkten (Vertrags-) Beziehungen bestehen, können hier ggf. die Daten einer Person zuordnen.
- Eindeutige auf dem RFID-Chip gespeicherte Daten (wie z. B. seine Seriennummer) werden zunächst ohne konkreten Personenbezug erfasst und gespeichert. Wenn man annimmt, dass bestimmte Objekte stets von derselben Person mitgeführt werden (z. B. Brille, Armbanduhr, Schuhe), lassen sich über das Auslesen der eindeutigen Identifikatoren der an solchen Objekten angebrachten Chips Bewegungs- und Konsumprofile des Träger er-

stellen. Weiterhin ist auch die spätere Verknüpfung mit konkreten Personendaten wie Name, Adresse usw. möglich.

Beim Einsatz von RFID-Chips im Einzelhandel ist zu berücksichtigen, dass die Speicherkapazität der Chips ausreicht, nicht nur Produkttyp, Produktgruppe und Hersteller zu codieren, sondern jedes einzelne konkrete Produkt. Gekaufte Artikel können so u. U. dauerhaft dem Käufer zugeordnet werden, falls keine geeigneten Gegenmaßnahmen ergriffen werden.

Die wesentlichen Gefahren, die beim Einsatz von RFID-Systemen für die Privatsphäre der Betroffenen entstehen können, sind insbesondere:

- das versteckte Anbringen sowie das unbefugte oder verdeckte Auslesen von Daten entweder direkt aus dem RFID-Chip oder durch Mithören und Decodieren der Kommunikation zwischen Chip und Lesegerät,
- das für den Träger des Chips unbemerkte Ausspähen von Daten auf Grund der kontaktlosen Kommunikation mit dem Lesegerät,
- die Verknüpfung von ausgelesenen Chipdaten mit personenbezogenen Daten des Chipinhabers ohne Rechtsgrundlage oder Vorliegen der Einwilligung des Betroffenen,
- die Speicherung von mit RFID-Chips erhobenen Daten auf Vorrat und ohne konkrete Zweckbindung,
- die Erzeugung und Speicherung von Verhaltens-, Nutzungs- und Bewegungsprofilen der Betroffenen.

Auch aus der Sicht des Betreibers oder Anwenders eines RFID-Systems (z. B. eines Warenhauses) existieren eine Reihe von Bedrohungen, die zu einer Beeinträchtigung der korrekten Funktion des Systems führen können. Exemplarisch seien hier genannt: das unbefugte Manipulieren von auf beschreibbaren Chips gespeicherten Daten, das unkontrollierte Einbringen von zusätzlichen Chips mit gefälschten Daten, das unbefugte Ablösen von RFID-Chips von den zu identifizierenden Objekten, das Fälschen der Identität von Lesegeräten oder das Blockieren bzw. Stören der Funkkommunikation zwischen Lesegerät und Chip. Bereits die Aufzählung verdeutlicht, dass zwischen den beteiligten Parteien – dem Betreiber eines RFID-Systems und dem Träger der mit RFID-Chips versehenen Objekte – zum Teil unterschiedliche Interessen bestehen. So ermöglicht das Ablösen des Chips von einem Warenobjekt offensichtlich dem Betroffenen, die weitere Verfolgung des Objekts und die Verknüpfung mit seinen Kundendaten zu unterbinden. Der Betreiber des Systems ist jedoch auf die zuverlässige Kennzeichnung der Ware zumindest bis zur Kasse und evtl. auch für die Abwicklung von Gewährleistungsansprüchen angewiesen.

1.2.3 Forderungen an Hersteller und Anwender von RFID-Systemen

Eine wesentliche Herausforderung bei der Gestaltung von RFID-Systemen besteht somit in der Berücksichtigung der beiden unterschiedlichen Interessenlagen bereits in der Phase der Systemplanung und des Entwurfs. Hersteller und Anwender/Betreiber müssen durch geeignete und angemessene Sicherheitsmaßnahmen die Eigenschaften der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachweisbarkeit der Datenverarbeitung gewährleisten. Bereits heute gibt es hierfür eine Reihe technischer Mechanismen, die direkt in RFID-Chips realisiert werden können (z. B. durch verschlüsselte Speicherung von Daten auf dem Chip, Vergabe von Passwörtern zum Zugriff auf Chipdaten, Chips mit wechselnder Seriennummer) oder die in Lesegeräten und Hintergrundsystemen zur Anwendung kommen (z. B. gegenseitige Authentifizierung von Chip und Systemkomponenten, verschlüsselte Datenübertragung sowohl bei Funk- als auch bei drahtgebundener Kommunikation, strikte Zugriffskontrolle). Einen umfassenden Überblick bietet die Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, die im November 2004 vom Bundesamt für Sicherheit in der Informationstechnik veröffentlicht wurde.[6]

Aus der Sicht des Datenschutzes muss die Aufmerksamkeit der Einhaltung grundlegender Prinzipien wie z. B. der Datensparsamkeit, Zweckbindung und Transparenz gelten. Aus diesem Grund sind Entwickler und Anwender/ Betreiber von RFID-Systemen gefordert, soweit möglich auf die Herstellung eines Personenbezugs in derartigen Systemen zu verzichten oder geeignete Alternativen hierfür zu erarbeiten. Sollte sich die Verarbeitung personenbezogener Daten in einem konkreten RFID-System als unverzichtbar erweisen, so sind insbesondere:

- Betroffene umfassend über den Einsatz von RFID-Chips und Lesegeräten, den Umfang und Inhalt der über sie gespeicherten Daten sowie deren Verwendungszweck zu informieren,
- jegliche personenbezogene Daten nur solange zu speichern, wie es zur Erreichung des jeweiligen Zwecks erforderlich ist,
- Verknüpfungen zwischen Daten nur auf Basis einer bestehenden Rechtsgrundlage oder einer informierten Einwilligung des Betroffenen über die potentielle Datenverarbeitung vorzunehmen,
- Möglichkeiten zur Deaktivierung/Löschung von RFID-Chips zu schaffen, insbesondere dann, wenn die Chipdaten für die spezifischen Zwecke nicht mehr erforderlich sind,
- Möglichkeiten zur wirksamen, fallweisen und nutzergesteuerten Blockierung des unbefugten Auslesens von RFID-Chips zu realisieren und die Betroffenen hierüber zu informieren,

[6] siehe http://www.bsi.bund.de/fachthem/rfid/studie.htm

- Alternativen zur Nutzung von RFID-Chips vorzusehen und auch anonymes Kaufen weiterhin zu ermöglichen,
- die Vertraulichkeit der gespeicherten und übertragenen Informationen durch wirksame Authentisierung der beteiligten Systemkomponenten und durch Verschlüsselung sicherzustellen.

Weitergehende Informationen und Anregungen für die datenschutzgerechte Gestaltung von RFID-Systemen sind dem Arbeitspapier der Artikel 29-Gruppe der europäischen Datenschutzbeauftragten vom Januar 2005 zu entnehmen.[7]

1.2.4 Herausforderungen der allgegenwärtigen Datenverarbeitung

Beobachtet man die Geschwindigkeit, mit der neue Forschungs- und Entwicklungsergebnisse im Bereich der RFID-Technik erzielt werden, so scheint die Vision der allgegenwärtigen, alles durchdringenden Datenverarbeitung (Ubiquitous Computing, Pervasive Computing) nicht mehr fern. Diese Vision wurde bereits vor ca. 20 Jahren entwickelt und geht von der zunehmenden Verschmelzung der realen und der digitalen Welt aus. Dinge des Alltags sind mit winzigen, intelligenten Chips (z. B. RFID-Chips) und Datenverarbeitungsmechanismen versehen, sie beobachten mit Sensoren ihre Umwelt, können sich spontan vernetzen, Informationen austauschen, Nutzern bei der Entscheidungsfindung assistieren oder ihnen lästige Routineaufgaben abnehmen und selbstständig kontextbezogen agieren. Die Technik wirkt diskret im Hintergrund, ist überall verfügbar, jedoch selbst kaum wahrnehmbar.

Systeme aus intelligenten Alltagsgegenständen, die ohne oder mit nur geringer menschlicher Interaktion auch personenbezogene Daten verarbeiten können, stellen neue Herausforderungen an Datenschutz und Datensicherheit. Es ergeben sich eine Reihe von Fragen z. B. nach der Sparsamkeit bei der Erhebung von personenbezogenen Daten und ihrer Zweckbindung, der Durchsetzung der Rechte von Betroffenen auf Information, Korrektur und Löschung ihrer Daten, der technischen Maßnahmen zum Schutz der Privatsphäre, dem Einfluss des Nutzers bei der Anwendung der technischen Maßnahmen sowie der Akzeptanz solcher Systeme in der Gesellschaft. Die Klärung der mit der mobilen und allgegenwärtigen Datenverarbeitung verbundenen juristischen, technischen und sozialen Fragen erfordert auch im Bereich des Datenschutzes neue oder veränderte Konzepte, die im Rahmen aktueller Forschungen erarbeitet werden sollen.[8]

---

[7] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A III

[8] siehe z. B. http://www.datenschutzzentrum.de/taucis

Beim Einsatz von RFID-Systemen können besondere Gefahren auftreten, die zur Verletzung der Privatsphäre der Betroffenen oder zur Beeinträchtigung der Datensicherheit führen. Die Hersteller solcher Systeme sind deshalb aufgefordert, verstärkt in Forschung und Entwicklung zu investieren, um bereits beim Systementwurf und der Realisierung geeignete technische Gegenmaßnahmen vorzusehen und somit Datenschutz und Datensicherheit zu einem Qualitätsmerkmal ihrer Produkte werden zu lassen. Für Betreiber von RFID-Systemen ist die projektspezifische Umsetzung von systemtechnischen Sicherheitsmaßnahmen genauso unverzichtbar wie die Wahrung der Rechte der Betroffenen auf sparsame Datenerhebung, Zweckbindung und Transparenz der Datenverarbeitung über den gesamten Prozess hinweg.

1.3 Kosten- und Leistungsrechnung in der Landesverwaltung

In unserem letzten Tätigkeitsbericht[9] hatten wir über die geplante Einführung der Kosten- und Leistungsrechnung (KLR) in ausgewählten Einrichtungen der Landesverwaltung berichtet und wesentliche Anforderungen aus der Sicht des Datenschutzes formuliert. Mittlerweile liegen erste, grundsätzlich positive Erfahrungen der Umsetzung dieser Forderungen in Pilotprojekten vor.

Die Einführung der KLR ist Bestandteil einer Reihe von Maßnahmen der Landesregierung zur Modernisierung des Rechnungswesens und zur Nutzung betriebswirtschaftlicher Steuerungselemente in der Verwaltung. Sie werden seit April 2005 unter der Bezeichnung „Neues Finanzmanagement Land Brandenburg“ zusammengefasst. Übergreifende Ziele der Maßnahmen sind die Sicherung der Transparenz der Aufstellung und Abwicklung von Haushalten, die Effizienz- und Kostenkontrolle bei der Erbringung von Verwaltungsleistungen und bei der Bereitstellung von Ressourcen sowie die realistische Darstellung der Vermögens-, Finanz- und Ertragslage des Landes. Gleichzeitig wird angestrebt, das Kostenbewusstsein, die Eigenverantwortung und die Mitarbeitermotivation innerhalb der Landesverwaltung durch die klare Definition von Zuständigkeiten und größere Gestaltungsspielräume im jeweiligen Verantwortungsbereich zu steigern.

Mithilfe der KLR sollen Informationen über erbrachte Leistungen und dadurch verursachte Kosten in einer Verwaltungseinheit ermittelt werden. Von datenschutzrechtlicher Bedeutung ist hierbei die Tatsache, dass Mitarbeiter die von ihnen jeweils aufgewendeten Anteile der Arbeitszeit auf vorab definierte Arbeitsbereiche, die sog. Produkte, buchen. Die Verrechnung der Arbeitszeitanteile aller an einem Produkt beteiligten Mitarbeiter mit pauschalierten Perso-

9 vgl. Tätigkeitsbericht 2003, A 4.4.4

nalkosten und die zusätzliche Berücksichtigung weiterer Kosten (z. B. Sachkosten) beantwortet die Frage nach den Gesamtkosten eines Produktes als Resultat des Verwaltungshandelns.

Auf der Grundlage eines Beschlusses der Landesregierung aus dem Jahr 2002 begann im Berichtszeitraum die Pilotierung der KLR in zwei Projektwellen. Die erste Welle umfasste vier Bereiche der Landesverwaltung (Staatskanzlei, Landesbetrieb Straßenwesen, Landeslabor sowie den Polizeibereich mit den beiden Polizeipräsidien und dem Zentraldienst der Polizei) und wurde im Januar 2005 mit dem Übergang in den Produktivbetrieb abgeschlossen. In der aktuellen zweiten Welle werden vier neue Projektbereiche in die KLR integriert (Ministerium der Justiz, Landesamt für Arbeitsschutz, Landesschule und Technische Einrichtung für Brand- und Katastrophenschutz sowie Landesbetrieb für Bau und Liegenschaften). Der Übergang in den Produktivbetrieb ist für Januar 2006 geplant, konnte für einige Bereiche jedoch vorgezogen werden. Die Leitung und Koordinierung aller KLR-Pilotprojekte liegt beim Zentralprojekt „Leitstand Rechnungswesen/KLR“ im Ministerium der Finanzen. Die Datenverarbeitung erfolgt mithilfe von SAP R/3-Systemen, die beim Zentraldienst der Polizei – für den Polizeibereich – bzw. beim Landesbetrieb für Datenverarbeitung und Statistik – für die anderen Projektbereiche – betrieben werden.

Unsere Behörde ist seit Beginn der ersten Projektwelle beratend in die Einführung der KLR einbezogen worden. Auf diese Weise war es möglich, wesentliche Anforderungen aus Sicht des Datenschutzes und der Datensicherheit bereits zu einem frühen Zeitpunkt in die Projekte einzubringen. Insgesamt ist festzustellen, dass unsere Hinweise und Empfehlungen bei der Durchführung der Pilotprojekte berücksichtigt wurden. Im Zentrum unserer Beteiligung standen die folgenden inhaltlichen Schwerpunkte:

1.3.1 Abschluss von Dienstvereinbarungen

Die Einführung eines Datenverarbeitungssystems zur Erfassung und Auswertung von Arbeitszeitdaten der Mitarbeiter wie im vorliegenden Fall der KLR berührt neben dem Datenschutz auch Fragen der Personalvertretung und ist nach § 65 Personalvertretungsgesetz des Landes Brandenburg mitbestimmungspflichtig. Zwischen der jeweiligen Behördenleitung und dem örtlichen Personalrat ist eine Dienstvereinbarung abzuschließen. Für die Einführung der KLR im Land Brandenburg wurde in dem Zentralprojekt unter Berücksichtigung unserer Hinweise eine Musterdienstvereinbarung erarbeitet, die jetzt als Grundlage für die konkreten, auf die Gegebenheiten der Piloteinrichtung angepassten Dienstvereinbarungen dienen kann.

Die Musterdienstvereinbarung beschreibt Ziele der KLR und den Ablauf des Verfahrens der Erfassung und Auswertung von produktbezogenen Arbeitszeitdaten der Mitarbeiter. Es werden die Grundsätze der Datensparsamkeit bzgl. der Stamm- und Zeiterfassungsdaten der Mitarbeiter und der Zweckbindung dieser Daten für die KLR sowie der Ausschluss von Leistungs- und Verhaltenskontrollen der Mitarbeiter festgeschrieben. Soweit es möglich ist, sind die produktbezogenen Arbeitszeitanteile durch den einzelnen Mitarbeiter selbst zu erheben und auf Produkte zu buchen. Korrekturen sind maximal drei Monate möglich, anschließend erfolgt automatisch die Datenlöschung. Zugriffe auf die Daten sind durch das Berechtigungskonzept reglementiert, die Vertraulichkeit von über Netzwerke übertragenen Daten wird durch eine Verschlüsselung der Daten gewährleistet. Der Personenbezug der produktbezogenen Zeiterfassungsdaten wird vor ihrer Auswertung durch Anonymisierung und Zusammenfassung (Aggregation) von Datensätzen aufgehoben. Er darf auch durch spezielle Formen der Auswertung nicht wiederhergestellt werden.

1.3.2 Erarbeitung eines Sicherheitskonzepts

Nach § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) sind automatisierte Verfahren, mit denen personenbezogene Daten verarbeitet werden, im Vorfeld auf mögliche Risiken, die sich für die Betroffenen ergeben können, zu untersuchen und ggf. entsprechende Sicherheitsmaßnahmen zur Beherrschung der Risiken festzulegen und umzusetzen. Diese Forderung gilt natürlich auch für die Datenverarbeitung in der KLR. Bei der Erstellung der erforderlichen Konzepte hat unsere Behörde beratend mitgewirkt.

Eine wesentliche Besonderheit ergibt sich aus der in den Pilotprojekten verwendeten rechentechnischen Infrastruktur: Das zur Buchung von Arbeitszeitanteilen auf Produkte sowie zur Verrechnung und Auswertung dieser Daten eingesetzte SAP-System wird für alle Pilotbereiche zentral von einem Dienstleister (Landesbetrieb für Datenverarbeitung und Statistik bzw. Zentraldienst der Polizei) auf einem Großrechner bzw. mehreren Servern betrieben. Für die Dateneingabe und das Berichtswesen werden die Arbeitsplatz-PCs der Mitarbeiter genutzt; Piloteinrichtungen und Dienstleister sind über ein Netzwerk verbunden. Da das Sicherheitskonzept das gesamte DV-System umfassen muss, andererseits jedoch die Anforderungen und lokalen Gegebenheiten in den Pilotbereichen vergleichbar sind, wurde eine zweiteilige Lösung erarbeitet. In einer so genannten Sicherheitsbetrachtung „Zentrale IT-Sicherheit“ werden die Sicherheitsmaßnahmen des Dienstleisters für den Großrechner- bzw. Serverbetrieb zusammengefasst. Daneben gibt es einen Sicherheitsleitfaden für die Piloteinrichtungen, der die jeweils in den Behörden lokal umzusetzenden Maßnahmen enthält und ggf. weiter ausgestaltet oder angepasst werden kann.

Die Sicherheitsmaßnahmen in beiden Konzepten, der zentralen Sicherheitsbetrachtung und dem Sicherheitsleitfaden, orientieren sich an den Vorschlägen des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik. Hintergrund ist, dass die im Projekt verarbeiteten personenbezogenen Daten einen mittleren Schutzbedarf haben und weiter gehende Maßnahmen, wie sie z. B. bei Daten mit Personalaktenqualität erforderlich wären, dem Prinzip der Angemessenheit nicht entsprechen würden.

Für die Umsetzung der Sicherheitsmaßnahmen ist stets die Daten verarbeitende Stelle im Sinne von § 3 Abs. 4 BbgDSG verantwortlich – hier also diejenige Einrichtung, die das Pilotprojekt durchführt. Durch die konkrete Gestaltung des Sicherheitsleitfadens und die tabellarische, checklistenartige Aufstellung der erforderlichen Maßnahmen werden die Erarbeitung eines Realisierungsplans und die Umsetzung der Maßnahmen wesentlich vereinfacht. Auch das Zentralprojekt im Ministerium für Finanzen sowie der jeweilige Dienstleister bieten Unterstützung hierfür an. Diese sollte im Bedarfsfall genutzt werden.

1.3.3 Verschlüsselung personenbezogener Daten

Zu den Forderungen, die wir seit vielen Jahren regelmäßig stellen, gehört die Verschlüsselung personenbezogener Daten bei ihrer Übertragung über offene Netzwerke. Daraus folgt für die Pilotprojekte der KLR, dass die von den Mitarbeitern produktbezogen erfassten Arbeitszeitanteile nur verschlüsselt zum SAP-System beim Dienstleister übertragen werden dürfen. Während das KLR-Teilprojekt im Polizeibereich ein separates, abgeschlossenes Netzwerk für den Datenaustausch verwendet, in dem alle Daten standardmäßig verschlüsselt werden, galt es, eine Lösung für die an das Landesverwaltungsnetz angeschlossenen KLR-Piloteinrichtungen zu finden.

Grundsätzlich bestehen für die Realisierung der Verschlüsselung in einem konkreten Projekt verschiedene Varianten, die wir mit den Projektverantwortlichen erörtert haben. Neben einer Ende-zu-Ende-Verschlüsselung bis auf die Ebene der KLR-Anwendung (d. h. der SAP-Applikation) wurde auch die Leitungsverschlüsselung zwischen den beteiligten Rechnern im Netzwerk oder zumindest für den Bereich des Landesverwaltungsnetzes – also zwischen dem Übergang aus dem lokalen Netz der Pilotbehörde in das Landesverwaltungsnetz und dem Übergang aus dem Landesverwaltungsnetz in das lokale Netz des Dienstleisters (hier: des Landesbetriebes für Datenverarbeitung und Statistik) – diskutiert.

Unter Berücksichtigung des mittleren Schutzbedarfs der in den KLR-Projekten verarbeiteten personenbezogenen Daten und der innerhalb der Pilot-

behörden realisierten Sicherheitsmaßnahmen nach dem IT-Grundschutzhandbuch fiel eine Entscheidung für die letztgenannte Variante der Leitungsverschlüsselung im Bereich des Landesverwaltungsnetzes. Die Lösung ist angemessen, sachgerecht und berücksichtigt auch den erheblichen finanziellen Aufwand, der für weiter gehende Verschlüsselungsmaßnahmen erforderlich gewesen wäre.

1.3.4 Berechtigungskonzepte und Vertretungsregelungen

Für den datenschutzgerechten Betrieb des KLR-Verfahrens, insbesondere zur Sicherung der Vertraulichkeit wurden Berechtigungskonzepte erarbeitet, die den Zugriff auf personenbezogene Daten der Mitarbeiter (Stammdaten und produktbezogene Arbeitszeitdaten) sowie auf Auswertungen und Berichte regeln. Die Konzepte liegen für jedes KLR-Teilprojekt vor und wurden von uns stichprobenartig geprüft. Dabei wurde festgestellt, dass Zugriffsrechte restriktiv und nur im Rahmen der Erforderlichkeit für die jeweilige Aufgabenerfüllung vergeben sind.

Weiterhin existieren in einem übergreifenden Berechtigungsrahmenkonzept organisatorische Regelungen für die temporäre oder dauerhafte Zuteilung von Rechten. Im Wesentlichen wird hierbei ein mehrstufiges Verfahren vorgeschrieben, das auf schriftlichen und zu genehmigenden Anträgen für die Zuweisung oder Änderung von Berechtigungen sowie auf einer strikten Rollentrennung auch bei der Berechtigungsadministration basiert. Die eigentliche technische Vergabe von Rechten erfolgt durch die Fachadministration im KLR-Zentralprojekt.

Ein Mitarbeiter einer KLR-Piloteinrichtung informierte uns über eine besondere Verfahrensweise in seinem Verantwortungsbereich: Dort sind die durch Mitarbeiter gebuchten Arbeitszeitdaten von einem Kostenstellenverantwortlichen explizit freizugeben. Zur Synchronisierung der KLR-Auswertungen muss die Freigabe regelmäßig und bis zu einem bestimmten Termin erfolgen. Für den Vertretungsfall galt in dieser Einrichtung die Regelung, dass der zu vertretende Kostenstellenverantwortliche sein persönliches Passwort an den Vertreter weitergibt. Der betroffene Mitarbeiter konnte sich mit diesem Zustand nicht einverstanden erklären und bat uns um Rat. Wir haben uns daraufhin mit dem KLR-Leitstand im Ministerium der Finanzen in Verbindung gesetzt. Uns wurde durch die verantwortliche Fachadministration die schnelle und unkomplizierte Zuteilung erforderlicher Rechte im Vertretungsfall zugesagt. Eine Weitergabe des Passworts ist in diesem Fall nicht mehr notwendig. Auf Anfrage teilte uns der KLR-Leitstand später mit, dass das Angebot der temporären Zuweisung von Vertreterrechten von der betroffenen KLR-Piloteinrichtung angenommen wurde.

Durch die frühzeitige Beteiligung unserer Behörde in den KLR-Projekten konnte der datenschutzgerechte Betrieb des DV-Systems bereits in der Pilotphase ermöglicht werden. Wir hoffen, dass die konstruktive Zusammenarbeit mit den Verantwortlichen im KLR-Projektleitstand und den Teilprojekten auch in Zukunft fortgesetzt bzw. auf andere, neue Projekte in der Landesverwaltung übertragen wird.

1.4 Der Schutz des Kernbereichs der persönlichen Lebensgestaltung

Das Bundesverfassungsgericht hat in drei Entscheidungen den Kernbereich der persönlichen Lebensgestaltung als den Ort, an dem der Einzelne Empfindungen, Gefühle, Überlegungen, Ansichten, Erlebnisse höchstpersönlicher Art zum Ausdruck bringt, unter absoluten Schutz gestellt. Hier darf der Staat auch mit den ansonsten zulässigen Überwachungsmaßnahmen nicht eindringen. Mit einer Entscheidung zu den Voraussetzungen der Beschlagnahme von Unterlagen bei Berufsgeheimnisträgern hat das Bundesverfassungsgericht dem Zugriff der Strafverfolgungsbehörden auf Datenbestände engere Grenzen gesetzt.

1.4.1 Der „Große Lauschangriff“

Das Grundrecht der Unverletzlichkeit der Wohnung steht unter bestimmten Voraussetzungen, insbesondere zur Bekämpfung der organisierten Kriminalität, der akustischen Überwachung von Wohnungen nicht entgegen. Dieser „Große Lauschangriff“ ist jedoch an das Vorliegen von Tatsachen geknüpft, die den Verdacht begründen, dass jemand, der eine durch Gesetz bestimmte besonders schwere Straftat begangen hat, sich vermutlich in der Wohnung aufhält und die Aufklärung der Straftat anders als durch das Abhören der Wohnung unverhältnismäßig erschwert oder aussichtslos wird. In seiner Entscheidung vom 3. März 2004 hat sich das Bundesverfassungsgericht mit der Verfassungsmäßigkeit der Vorschriften des „Großen Lauschangriffs“ in der Strafprozessordnung befasst.

Das Bundesverfassungsgericht hat mit seiner Entscheidung vom März 2004 die Regelungen der Strafprozessordnung zum „Großen Lauschangriff“ in wesentlichen Teilen für verfassungswidrig erklärt. Das Gericht begründete dies mit der grundgesetzlichen Garantie der Persönlichkeitsrechte in einem absolut geschützten Kernbereich privater Lebensgestaltung für jeden Menschen. In ihn darf der Staat selbst dann nicht eingreifen, wenn es im Interesse der Effektivität der Strafverfolgung und der Erforschung der Wahrheit liegt. Hier ist folglich auch keine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung und dem Strafverfolgungsinteresse zulässig. Selbst überwiegende Interessen der Allgemein-

heit können einen Eingriff in diese Freiheit zur Entfaltung in den höchstpersönlichen Angelegenheiten nicht rechtfertigen. Der Schutz des Kernbereichs der persönlichen Lebensgestaltung geht allerdings nicht soweit, dass er den Wohnraum generell umfasst. Auch in einer Wohnung geführte Gespräche über bereits begangene oder erst geplante Straftaten können daher überwacht werden, weil solche Gesprächsinhalte nicht zum geschützten Kernbereich gezählt werden. Andererseits können besonders vertrauliche und aus diesem Grunde zum Kernbereich der Persönlichkeit zu rechnende Unterredungen auch außerhalb des Wohnraums geführt werden. Unter bestimmten Voraussetzungen dürfen auch sie, unabhängig vom Ort, an dem sie stattfinden, nicht überwacht werden. Das Bundesverfassungsgericht hat damit die von den Datenschutzbeauftragten vorgetragenen verfassungsrechtlichen Bedenken gegen die Regelungen des „Großen Lauschangriffs“ aufgegriffen. Es hat die hohe Bedeutung des Grundrechts auf die Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung herausgestellt.

Das Bundesverfassungsgericht hat dem Gesetzgeber aufgegeben, den Kernbereich so zu sichern, dass dessen Verletzung auszuschließen ist. Die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung sind umso strenger, je größer das Risiko ist, mit ihr Gespräche höchstpersönlichen Inhalts zu erfassen. Sie ist von vornherein verboten, wenn Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt wird. In Fällen, in denen eine Überwachungsmaßnahme bereits begonnen hat, muss sie dann abgebrochen und die Aufzeichnung gelöscht werden, wenn deutlich wird, dass das überwachte Gespräch den absolut geschützten Kernbereich betrifft. Das Risiko, ihn zu berühren, besteht insbesondere beim Abhören von Gesprächen im engsten Familien- und Freundeskreis sowie bei Gesprächen mit besonderen Vertrauenspersonen wie z. B. Pfarrern, Ärzten und Strafverteidigern. Überwachungsmaßnahmen sind hier nur möglich, wenn bereits konkrete Anhaltspunkte vorliegen, dass die Gesprächsinhalte zwischen dem Beschuldigten und diesen Personen keinen absoluten Schutz erfordern, z. B. weil die Gesprächspartner im Verdacht stehen, Tatbeteiligte zu sein.

Die daraufhin erfolgte Änderung der Strafprozessordnung wird den Vorgaben des Bundesverfassungsgerichts nach Auffassung der Datenschutzbeauftragten sowie anderer Kritiker nur unzureichend gerecht. Sie enthält statt des verfassungsrechtlich eigentlich zwingenden Verbotes, Aufnahmen in bestimmten Situationen überhaupt vorzunehmen, lediglich ein Verwertungsverbot für einzelne Stellen tatsächlich erstellter Aufzeichnungen.

1.4.2 Präventive Telefonüberwachung

Des Weiteren prüfte das Bundesverfassungsgericht die Verfassungsmäßigkeit der neu in das niedersächsische Sicherheits- und Ordnungsgesetz aufgenommenen Befugnis zur präventiven Telefonüberwachung. Diese erlaubte der Polizei immer dann die Telefonüberwachung, wenn Tatsachen die Annahme rechtfertigen, dass bestimmte Straftaten begangen werden sollen und die vorbeugende Bekämpfung dieser Straftaten sonst aussichtslos oder wesentlich erschwert werden würde. Es handelte sich um eine Maßnahme der Polizei für Fälle, in denen noch nicht einmal der Anfangsverdacht einer Straftat vorlag. Schon in diesem frühen Stadium hätte die Polizei mit richterlicher Genehmigung Telefone abhören können. Für den Einzelnen war somit nicht absehbar, wann und ob er Ziel einer solchen Maßnahme hätte werden können.

Das Bundesverfassungsgericht hat in seiner Entscheidung im Juli 2005 die Regelung zur präventiven Überwachung im niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung mit Artikel 10 des Grundgesetzes (GG) für unvereinbar und nichtig erklärt. Es hat die Bedeutung des Rechts auf unbeobachtete Kommunikation und damit erneut den Schutz des Kernbereichs privater Lebensgestaltung betont. Das Gericht hat festgestellt, dass die mit der Verfassungsbeschwerde angegriffenen Vorschriften auch materiell mit der Verfassung unvereinbar sind, da es an der hinreichenden Bestimmtheit fehlt und die Vorschriften den Anforderungen des Grundsatzes der Verhältnismäßigkeit hinsichtlich ihrer Angemessenheit nicht genügen. Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung fehlen ganz. Damit hat das Bundesverfassungsgericht zum wiederholten Male deutliche Grenzen für den Schutz dieses Kernbereichs gesetzt. Es bleibt zu hoffen, dass die rechtsstaatlichen Maßstäbe in Gesetzgebungsverfahren wieder stärker Beachtung finden, denn die Entscheidung über die Grenzen der Freiheit des Bürgers darf nicht einseitig in das Ermessen der Verwaltung gestellt werden. Auch dies hat das Bundesverfassungsgericht bereits mehrfach klargestellt.

1.4.3 Verwertungsverbot von Selbstgesprächen

Bei der dritten Entscheidung schließlich hat das Bundesverfassungsgericht die Verwertung der während eines Krankenhausaufenthalts im Einzelzimmer geführten Selbstgespräche eines Patienten verboten.

Es handelte sich bei den aufgezeichneten Gesprächen eindeutig um Selbstgespräche, die der Angeklagte in einem nur mit ihm belegten Krankenhauszimmer führte. Das Einzelzimmer war damit dem nach Art. 13 GG geschützten Wohnraum gleichzusetzen und das Gespräch dem geschützten Kernbereich der privaten Lebensgestaltung zuzuordnen. Der Inhalt des Selbstge-

sprächs war zudem nicht so eindeutig, dass sich damit der Tatverdacht für eine bestimmte Straftat ohne weitere wertende Interpretation bestätigt hätte.

Auch wenn die Entscheidung in einem Einzelfall erging, hat sie doch wegen der Ausweitung des Art. 13 GG auf einen außerhalb der eigentlichen Wohnung liegenden Raum über den vorliegenden Fall hinaus Bedeutung.

1.4.4 Forderungen der Datenschutzbeauftragten zu Überwachungsmaßnahmen

Die Datenschutzbeauftragten haben die Entscheidungen des Bundesverfassungsgerichts zum Anlass genommen, auch bei den anderen in der Strafprozessordnung sowie in den Polizei- und Nachrichtendienstgesetzen geregelten Befugnisse zu eingriffsintensiven Überwachungsmaßnahmen zu prüfen, ob sie den Anforderungen der Entscheidungen zur Wahrung des absolut geschützten Kernbereichs der privaten Lebensgestaltung genügen.

Auch die rechtliche Ausgestaltung verdeckter Eingriffsbefugnisse von Polizei und Nachrichtendiensten des Bundes und der Länder muss sich an den Maßstäben der verfassungsgerichtlichen Entscheidungen ausrichten. Sie ist unter Beachtung der folgenden Aspekte zu prüfen und ggf. zu überarbeiten:

- Schutz der Kommunikationsinhalte, insbesondere bei Gesprächen mit Familienangehörigen, Vertrauten oder mit Berufsgeheimnisträgern,
- Überprüfung der Straftatenkataloge, insbesondere bei Eingriffsbefugnissen, bei denen der Gesetzgeber ein bestimmtes Gewicht der zu verhütenden Tat voraussetzt,
- Eingrenzung der Eingriffsermächtigung bei präventiver Überwachung,
- eindeutige Regelung der Löschung sowie Verpflichtung zur Löschung bei rechtswidriger Erhebung im Kernbereich privater Lebensgestaltung,
- Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten sowie eine Kennzeichnungspflicht zur Sicherstellung der Zweckbindung,
- Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen, von der allenfalls abgesehen werden kann, wenn die Identität der Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden könnte oder der Benachrichtigung überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen,
- gesetzliche Festlegung der Zeitabstände für die Benachrichtigung.

1.4.5 Voraussetzungen der Beschlagnahme von Datenträgern insbesondere bei Berufsgeheimnisträgern

Im Verlauf eines gegen einen Kompagnon einer gemeinsam betriebenen Rechtsanwaltskanzlei und Steuerberatungsgesellschaft anhängigen Ermittlungsverfahrens waren die Geschäftsräume durchsucht und die gesamten Datenbestände beschlagnahmt worden.

Das Bundesverfassungsgericht sah in der Durchsuchung und Sicherstellung der Daten einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Anwälte und Steuerberater sowie ihrer Mandanten. Zum Funktionieren des Rechtswesens muss die Kommunikation zwischen Mandanten und Rechtsanwalt besonders geschützt werden. Durch den Zugriff wurde dieses rechtlich besonders geschützte Vertrauensverhältnis in schwerwiegender Weise beeinträchtigt.

Die Sicherstellung und Beschlagnahme des gesamten Datenbestands war unverhältnismäßig, weil damit auch eine Vielzahl verfahrensunerheblicher Daten zahlreicher Personen, die in keiner Beziehung zu dem Tatvorwurf standen, betroffen waren. Die Beachtung des Verhältnismäßigkeitsgrundsatzes hätte aber geboten, dass der Zugriff auf solche für das Verfahren bedeutungslosen Informationen soweit wie möglich vermieden wird. Das Bundesverfassungsgericht verweist in seiner Entscheidung ausdrücklich auf die Verfahrensregelungen der Strafprozessordnung, die dazu dienen, Grundrechtseingriffen vorzubeugen oder diese zu minimieren. Dazu zählt auch die in § 110 StPO geregelte Durchsicht, die vor der eigentlichen Beschlagnahme erfolgen soll. Im vorliegenden Fall hätten die Daten vor Ort gesichtet und – soweit sie für das Verfahren nicht erheblich waren – von der Beschlagnahmung ausgenommen werden müssen.

Das Urteil des Bundesverfassungsgerichts hebt auch auf die Bedeutung der Beweismittel für das Strafverfahren ab. Danach kann im Einzelfall die Geringfügigkeit der Straftat und die geringe Beweisbedeutung der auf dem Datenträger vermuteten Informationen einer Sicherstellung des Datenbestands entgegenstehen. Dies ist insbesondere bei Beschlagnahmevorhaben bei Berufsgeheimnisträgern zu berücksichtigen. Um die datenschutzrechtlichen Positionen der Betroffenen angemessen zu schützen, hält das Bundesverfassungsgericht selbst ein Beweisverwertungsverbot von Datenträgern und den darauf vorhandenen Daten für geboten, wenn schwerwiegende, bewusste oder willkürliche Verfahrensverstöße festzustellen sind.

Mit seinen Entscheidungen hat das Bundesverfassungsgericht den Schutz des Kernbereichs privater Lebensgestaltung gestärkt, ohne allerdings bestimmte Formen oder Orte der Überwachung generell für verfassungswidrig zu erklären. Staatliche Überwachungsmaßnahmen dürfen auch dann nicht in diesen Bereich eindringen, wenn ohne sie die Effektivität der Strafverfolgung und Wahrheitsfindung beeinträchtigt werden. Die Neuregelung der einschlägigen Vorschriften zum „Großen Lauschangriff“ in der Strafprozessordnung setzen die Vorgaben der Gerichtsentscheidung nach Auffassung der Datenschutzbeauftragten nur unzulänglich um. Auch haben andere gesetzliche Überwachungsbefugnisse die Grundsätze zum Schutz des absoluten Kernbereichs zu berücksichtigen und sind daraufhin zu prüfen. Bei der Durchsuchung und Beschlagnahme von Datenträgern sind das Verhältnismäßigkeitsprinzip zu beachten und die strafprozessualen Verfahrensschritte zum Schutz des Rechts auf informationelle Selbstbestimmung stringend einzuhalten, sodass im Ergebnis auch nur solche Daten beschlagnahmt werden, die für das Ermittlungsverfahren tatsächlich relevant sind.

1.5 Sozialrecht

1.5.1 Hartz IV – Wie steht es mit dem Datenschutz?

Seit dem 1. Januar 2005 gilt Hartz IV. Das Gesetz regelt die Grundsicherung für Arbeitssuchende, die erwerbsfähig, aber hilfebedürftig sind und keinen Anspruch auf Arbeitslosengeld I haben. Kein anderes Thema beherrschte und beherrscht so die Diskussion in der Öffentlichkeit. Während die betroffenen Bürger verunsichert und von Existenzängsten bedroht sind, beklagen die Aufgabenträger der neuen Grundsicherung für Arbeitslose, die Bundesagentur für Arbeit und die Kommunen, die nicht ausreichenden Vorbereitungen für die Einführung. Massive datenschutzrechtliche Mängel waren und sind festzustellen.

Durch die Zusammenführung von Arbeitslosen- und Sozialhilfe waren die Arbeitsverwaltung und Kommunen gefordert, sich neu zu organisieren. Das Gesetz ermöglichte zwei Wege: zum einen die Gründung von Arbeitsgemeinschaften (ARGEn) zwischen Arbeitsagenturen und Kommunen, zum anderen die ausschließliche kommunale Vermittlung in den so genannten Optionskommunen.

Im Land Brandenburg betreuen die Landkreise Oberhavel, Oder-Spree, Ostprignitz-Ruppin, Spree-Neiße und Uckermark Langzeitarbeitslose als alleinige Träger. Die Trägerschaft für die Leistungen nach dem Sozialgesetzbuch Zweites Buch wird als Selbstverwaltungsaufgabe wahrgenommen und unterliegt der Rechtsaufsicht der Länder. Die anderen Landkreise und kreisfreien

Städte haben durch öffentlich-rechtlichen oder privatrechtlichen Vertrag Arbeitsgemeinschaften gegründet, die fast überall „Job-Center“ heißen.

Das Gesetz sieht also eine geteilte Leistungsträgerschaft innerhalb der Arbeitsgemeinschaften vor. Danach ist im Grundsatz die Bundesagentur für Arbeit zuständig. Die kommunalen Träger sind zuständig für

- die Leistungen für Unterkunft und Heizung,
- die Kinderbetreuungsleistungen,
- die Schuldner- und Suchtberatung,
- die psychosoziale Betreuung und
- die Übernahme von Leistungen für die Erstausstattung für Bekleidung und Wohnung sowie
- Leistungen für mehrtägige Klassenfahrten.

Die Arbeitsagentur und die Kommune sind in ihrem jeweiligen Aufgabenbereich als Träger verantwortlich. Nach außen müssen die Träger jedoch als eine Behörde auftreten. So erlässt die Arbeitsgemeinschaft einheitliche Verwaltungsakte und Widerspruchsbescheide.

Die Zusammenarbeit einer Bundesbehörde mit kommunalen Selbstverwaltungsbehörden in Form dieser Arbeitsgemeinschaften führte mangels eindeutiger gesetzlicher Regelungen im Sozialgesetzbuch Zweites Buch zu Unklarheiten bei den Zuständigkeiten - auch bezüglich der Fach- und Rechtsaufsichten. Diese bis heute ungelösten Probleme betreffen gleichfalls die Datenschutzbeauftragten des Bundes und der Länder hinsichtlich ihrer Datenschutzaufsicht. Die Tätigkeit der Arbeitsagenturen fällt nicht mehr wie bisher ausschließlich in den Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz, sondern hinsichtlich der Tätigkeit der Arbeitsgemeinschaften als Landesbehörden nunmehr auch in den des jeweiligen Landesbeauftragten für den Datenschutz. Die Überarbeitung der Zuständigkeitsregelungen im Sozialgesetzbuch Zweites Buch ist dringend geboten.

Hier ein Beispiel, um die Problematik zu verdeutlichen. Die Arbeitsgemeinschaften als eigenverantwortlich Daten verarbeitende Stellen des Landes arbeiten mit der Leistungs- und Berechnungssoftware A2LL. Nach dem Gesetz ist die Bundesagentur für Arbeit für die Entwicklung und Bereitstellung dieses Informationssystems zuständig. In ihrer Verantwortung liegt somit die datenschutzkonforme Ausgestaltung des Programms. Folglich muss der Bundesbeauftragte für den Datenschutz festgestellte datenschutzrechtliche Mängel beanstanden, obwohl die Arbeitsgemeinschaften der Kontrollzuständigkeit des jeweiligen Landesbeauftragten unterliegen.

Hinsichtlich der Software A2LL bestehen noch immer wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Auf diese gravierenden datenschutzrechtlichen Mängel machten die Datenschutzbeauftragten des Bundes und der Länder unter anderem durch Entschließungen der 68. und 70. Konferenz der Datenschutzbeauftragten[10] aufmerksam und forderten die Bundesagentur für Arbeit zur Nachbesserung auf. Insbesondere muss das Verfahren über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben. Entgegen der Zusagen des Bundesministeriums für Wirtschaft und Arbeit und der Bundesagentur für Arbeit gibt es jedoch noch immer keine erkennbaren Fortschritte bei der Beseitigung dieser Mängel. Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensitive Daten, wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so von Sachbearbeitern deutschlandweit eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne Arbeitsgemeinschaften reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet.

Seit Einführung des Arbeitslosengeldes II gab es immer wieder datenschutzrechtliche Fragen. So verschickten die Bundesagentur für Arbeit sowie einige Sozialämter im Sommer 2004 die Vordrucke für den Antrag auf Leistungen zur Sicherung des Lebensunterhaltes nach dem Sozialgesetzbuch Zweites Buch. Der umfangreiche Fragebogen verunsicherte viele Betroffene. Welche Angaben sind für die Prüfung der Leistungsgewährung notwendig und welche persönlichen Daten müssen nicht preisgegeben werden? In jedem Fall ist die Angabe der Telefonnummer und E-Mail Adresse freiwillig. Angaben zur Bankverbindung des Vermieters sind gleichfalls freiwillig, denn nur in bestimmten gesetzlich vorgeschriebenen Fällen darf ohne Zustimmung des Leistungsberechtigten die Miete an den Vermieter gezahlt werden. Große Unklarheit herrschte bezüglich der verwendeten Begriffe Bedarfs- und Haushaltsgemeinschaft. Ferner wurde auf ein und dem selben Bogen nach den Einkünften von Angehörigen gefragt, während auf der Rückseite der Arbeitgeber den Verdienst bescheinigen sollte. Dies sind nur einige Beispiele. Ins-

[10] siehe Dokumente zu Datenschutz und Informationsfreiheit 2004, A I 3 sowie 2005, A I 3

gesamt ergab die Prüfung der Antragsvordrucke, dass diese gegen datenschutzrechtliche Vorschriften verstießen und dringend überarbeitet werden mussten.

Nach nunmehr einem Jahr ist die Überarbeitung der Vordrucke durch die Bundesagentur für Arbeit unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder fast abgeschlossen. Es wurden Ausfüllhinweise erarbeitet, die zusammen mit den ebenfalls neuen Antragsvordrucken als „Paket“ an die Betroffenen ausgehändigt werden sollen. Nur so wird ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Dies bedeutet gleichzeitig, dass Überschussinformationen, aus den ursprünglichen Anträgen resultierend, gelöscht werden müssten.

Nachdem die ersten Bescheide erteilt waren, stellten die Arbeitsgemeinschaften fest, dass die Datenbestände in vielen Fällen fehlerhaft waren. Aus diesem Grund bot die Bundesagentur für Arbeit den Arbeitsgemeinschaften an, an einer Call-Center-Aktion durch ein von der Bundesagentur beauftragtes Call-Center kostenlos teilzunehmen. Mitarbeiter der Call-Center sollten telefonisch Daten bei den Betroffenen abfragen und mit dem vorhandenen Datenbestand abgleichen.

Wir haben deshalb im Sommer 2005 zwei von sechs Brandenburger Arbeitsgemeinschaften aufgesucht, die das Angebot der Bundesagentur für Arbeit zur Teilnahme an einer Call-Center-Aktion angenommen hatten. Dabei haben wir festgestellt, dass die Arbeitsgemeinschaften ihre Teilnahme lediglich auf Grundlage einer E-Mail von der Bundesagentur für Arbeit und in Unkenntnis des zwischen der Bundesagentur für Arbeit und T-Systems International GmbH diesbezüglich abgeschlossenen Vertrages erklärt haben. Eine schriftliche Auftragserteilung durch die Arbeitsgemeinschaften selbst erfolgte nicht. Genaue Kenntnisse zum Ablauf des Verfahrens und dem aktuellen Stand der Telefonaktion lagen nur teilweise vor. In beiden Gesprächen wurde uns als Grund für die Teilnahme an dieser Telefonaktion die erforderliche Bereinigung der bestehenden Datenbestände genannt. Die qualitative Verbesserung der Vermittlungsarbeit bzw. die individuelle Förderung der Kunden sei damit nicht zu erreichen und somit nicht Ziel und Zweck der Befragung. Die Betroffenen wurden nicht vorab von den Arbeitsgemeinschaften über die geplante Telefonaktion informiert und in den Gesprächen offenbar häufig auch nicht auf die Freiwilligkeit der Angaben hingewiesen.

Die Vorgehensweise der Arbeitsgemeinschaften stellt einen Verstoß gegen die Vorschriften zur Datenverarbeitung durch private Dritte im öffentlichen Auftrag dar. In einer Entschließung[11] zur 70. Konferenz der Datenschutzbe-

[11] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 3

auftragten des Bundes und der Länder wiesen die Datenschutzbeauftragten darauf hin, dass die Teilnahme an einer solchen Befragung freiwillig ist. Aus diesem Grund hatten die Betroffenen das Recht, die Beantwortung von Fragen am Telefon zu verweigern. Ferner rechtfertigt die Ablehnung der Teilnahme an einer solchen Befragung nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden. Künftig sollten die Betroffenen vorab über solche geplanten Aktionen informiert werden.

Bei unseren Informationsbesuchen haben wir auch festgestellt, dass die Arbeitsgemeinschaften oftmals keinen behördlichen Datenschutzbeauftragten hatten. § 7a Brandenburgisches Datenschutzgesetz (BbgDSG) bestimmt, dass Daten verarbeitende Stellen einen behördlichen Datenschutzbeauftragten zu bestellen haben. Insofern vertreten wir die Auffassung, dass entweder der bereits bestellte Datenschutzbeauftragte der Stadtverwaltung bzw. des Landkreises für die Arbeitsgemeinschaften zuständig ist oder die Arbeitsgemeinschaften bestellen einen eigenen behördlichen Datenschutzbeauftragten.

An dieser Stelle sei nochmals darauf hingewiesen, dass nach dem Brandenburgischen Datenschutzgesetz der behördliche Datenschutzbeauftragte keinem Interessenkonflikt mit seinen sonstigen dienstlichen Aufgaben unterliegen darf, die datenschutzrechtlichen Kontrollfunktionen könnten sonst nicht unabhängig wahrgenommen werden. Aus § 7a BbgDSG folgt, dass der behördliche Datenschutzbeauftragte sich unmittelbar an die Leitung der Daten verarbeitenden Stelle wendet bzw. ihr unmittelbar zu unterstellen ist. Dies ist nur denkbar, wenn der behördliche Datenschutzbeauftragte nicht selbst der Leitung der Stelle angehört.

Zu den Aufgaben der Arbeitsgemeinschaften und der optierenden Landkreise gehört es auch, mit den Betroffenen Eingliederungsvereinbarungen abzuschließen. Nach dem Fachkonzept der Bundesagentur für Arbeit „Beschäftigungsorientiertes Fallmanagement“ soll jeder Eingliederungsvereinbarung eine Chancen- und Risikoeinschätzung der Betroffenen vorausgehen. Diese Einschätzung wird in der Praxis als Profiling bezeichnet. Um eine Einschätzung von Vermittlungschancen bzw. bestehenden Vermittlungshemmnissen vornehmen zu können, wurden sowohl von den Arbeitsgemeinschaften, hier meist von der Bundesagentur für Arbeit vorgegeben, als auch von den optierenden Landkreisen Fragebögen entwickelt. Aus uns vorliegenden Eingaben ist zu sehen, dass diese Bögen häufig Daten abfragen, die für eine erfolgreiche Vermittlung nicht erforderlich sind. Beispielsweise wird nach der Nachbarschaft oder den Werten und Idealen des Betroffenen gefragt. Insgesamt werden die Betroffenen nicht darüber informiert auf welcher Rechtsgrundlage

die Datenerhebung erfolgt, dass sie teilweise freiwillig ist und wofür diese Angaben benötigt werden.

Grundsätzlich dürfen Sozialleistungsträger Sozialdaten dann erheben, wenn ihre Kenntnis für die Erfüllung einer ihnen im Sozialgesetzbuch zugewiesenen Aufgabe erforderlich ist, § 67a SGB X. Voraussetzung einer Erhebung ist also, dass der Leistungsträger diese Informationen unbedingt benötigt, um beispielsweise den Leistungsempfänger in Arbeit vermitteln zu können. Eine Datenerhebung, die faktisch auf eine Familienanamnese hinausläuft, ist als ein Verstoß gegen das Recht auf informationelle Selbstbestimmung zu werten.

Nach Einführung des Arbeitslosengeldes II sind viele Bürger an uns herangetreten, um sich bei Datenschutzproblemen bei der Umsetzung des neuen Verfahrens beraten zu lassen. Wir stellen hier die am meisten gestellten Fragen vor.

1.5.2 Einzelne Aspekte der Umsetzung sozialgesetzlicher Regelungen

1.5.2.1 Empfangsbereiche von Sozialbehörden

Im Berichtszeitraum erreichten uns zahlreiche Beschwerden über die Gestaltung von Empfangs- und Wartebereichen in Behörden und zur Durchführung von Beratungsgesprächen in den Arbeitsgemeinschaften. Bereits am Eingangstresen mussten vom Kunden personenbezogene Daten offen gelegt werden. Vorkehrungen, die eine Kenntnisnahme der Daten durch Dritte verhindern, waren oftmals unzureichend. Beratungen erfolgten teilweise sogar im Beisein anderer Antragsteller.

Zum Schutz des Sozialgeheimnisses muss vermieden werden, dass Unbefugte Sozialdaten zur Kenntnis nehmen oder Beratungen mithören können. Hierzu zählen neben anderen Antragstellern auch die unzuständigen mit dem Fall nicht befassten Kollegen.

Gespräche mit Betroffenen – auch im Empfangsbereich – müssen vertraulich bleiben. Das ist in vielen Arbeitsgemeinschaften oder „Job-Centern“ wegen der räumlichen Gegebenheiten nicht immer ohne weiteres möglich. Jedoch müssen die Behörden auf Wunsch der Betroffenen das Gespräch in einem gesonderten Raum vertraulich fortsetzen oder einen anderen Termin vereinbaren. Auf diese Möglichkeit kann beispielsweise mittels eines Hinweisschildes aufmerksam gemacht werden. Dabei darf der Wunsch nach Einzelberatung nicht zu einer Benachteiligung, etwa durch längere Wartezeiten führen.

Im Empfangsbereich muss auch auf die Einhaltung eines Diskretionsabstandes geachtet werden. Dies erschwert das Mithören für Wartende. Aus dem gleichen Grund sollten auch keine Regale mit Informationsmaterialien für die Bürger, sondern Sicht- bzw. Schallschutzwände genau neben den Beratungsplätzen aufgestellt werden. Die gesamte Eingangs- und Wartezone ist entsprechend zu gestalten.

In allen an uns herangetragenen Fällen konnte eine Verbesserung der datenschutzrechtlichen Situation erreicht werden. Die Mitarbeiter wurden noch einmal auf die Einhaltung datenschutzrechtlicher Vorschriften hingewiesen und die Behörden trafen die notwendigen organisatorischen Vorkehrungen zum Schutz des Sozialgeheimnisses.

Auch bei der Gestaltung der räumlichen Situation ist den Anforderungen des Datenschutzes Rechnung zu tragen. Mindestvoraussetzungen sind dabei die Möglichkeit zu vertraulichen Beratungen sowie die Einhaltung des Diskretionsabstandes.

1.5.2.2 Vorlage von Kontoauszügen in „Job-Centern“ und Sozialämtern

Für das Verlangen der „Job-Center“ und Sozialämter, bei der Beantragung von Sozialleistungen Kontoauszüge vorzulegen, gibt es keine eindeutigen Regelungen. Es ist unklar, wer wann, über welchen Zeitraum Kontoauszüge vorlegen muss oder ob die vorzulegenden Auszüge vom Antragsteller teilweise geschwärzt werden dürfen.

Alle, die Sozialleistungen beantragen, sind zur Mitwirkung verpflichtet. Dies bedeutet jedoch nicht, dass sie undifferenziert alle Bewegungen auf ihren Konten offen legen müssen. Die Behörden sind jedoch berechtigt, Kontoauszüge anzufordern:

- wenn erstmalig laufende Leistungen oder einmalige Beihilfen beantragt werden,
- während des laufenden Hilfebezuges frühestens nach Ablauf von zwölf Monaten,
- zum Zwecke der Klärung einer konkreten Frage zu der Einkommens- und Vermögenssituation der Antragsteller, wenn diese nicht durch die Vorlage anderer Unterlagen herbeigeführt werden kann bzw. wenn konkrete Zweifel an der Vollständigkeit oder Richtigkeit der Angaben der Hilfe Suchenden bestehen. Dies kann insbesondere dann der Fall sein, wenn konkrete Anhaltspunkte den Verdacht auf Vorliegen eines Missbrauchs von Sozialleistungen begründen. Denkbar ist dies auch im Rahmen des automatisierten Datenabgleichs. Der Sozialleistungsträger hat in diesen Fällen zu begrün-

den, warum andere Unterlagen nicht als Nachweis akzeptiert werden können.

Die Antragsteller müssen bereits bei der Anforderung der Kontoauszüge auf ihr Recht, einzelne Buchungen zu schwärzen, hingewiesen werden, insbesondere bei Soll-Buchungen über geringere Beträge (regelmäßig bis 50 Euro) können die zu den Einzelbuchungen aufgeführten Texte in der Regel geschwärzt werden. Über die Angabe der Beträge bzw. durch den Vergleich der Kontostände lässt sich die Einkommens- bzw. Vermögenssituation trotzdem weiterhin lückenlos feststellen. Allerdings kann bei Besonderheiten des Einzelfalles anderes gelten. Beispielsweise können regelmäßige Zahlungen von Beiträgen für kapitalbildende Lebensversicherungen, Ausbildungsversicherungen oder Bausparverträge leistungsrelevant sein. Insoweit wäre eine Schwärzung auch bei geringeren Beträgen hier nicht zulässig, was jedoch im konkreten Einzelfall zu erläutern ist. Denkbar ist zudem eine Teilschwärzung der Buchungstexte. Dies wäre bei regelmäßigen Überweisungen an eine Partei bzw. eine Gewerkschaft oder bei Zahlungen an eine Religionsgemeinschaft möglich, deren Mitgliedschaft nicht offen gelegt werden muss. Hier reicht es aus, dass vom Text „Mitgliedsbeitrag“ oder „Spende“ lesbar bleibt, ohne dass die Bezeichnung des Zahlungsempfängers erkennbar ist.

Das Schwärzen des Eingangs von Zahlungen kann dagegen zu einer Verletzung der Mitwirkungspflicht führen, da grundsätzlich das gesamte Einkommen bei der Hilfegewährung zu berücksichtigen ist.

Die Pflicht zur Vorlage von Kontoauszügen bedeutet nicht, dass von ihnen beliebig Kopien erstellt und aufbewahrt werden dürfen. Ebenso wie das Erheben der Daten (die Vorlage des Kontoauszuges) unterliegt auch deren Speichern (hier das Aufbewahren der Kopie des Kontoauszuges) dem Verhältnismäßigkeitsgrundsatz. Da die Auszüge über einen Zeitraum von drei bis sechs Monaten regelmäßig eine Vielzahl von Kontobewegungen enthalten, die für die Feststellung des Bedarfs des Hilfebedürftigen nicht relevant sind, ist eine generelle Speicherung dieser Daten unzulässig. Im Regelfall genügt ein Vermerk in der Akte, dass die Belege vorgelegen haben und keine gegen den Leistungsanspruch sprechenden Daten ermittelt wurden. Um möglichen Beweisproblemen zu begegnen, sind die Antragsteller darauf hinzuweisen, dass sie verpflichtet sind, diese aufzubewahren, um sie gegebenenfalls für spätere Nachweiszwecke erneut vorlegen zu können. Die Leistungsträger sollten sich schriftlich bestätigen lassen, dass sie auf diese Verpflichtung hingewiesen haben.

Die „Job-Center“ und Sozialbehören dürfen Kontoauszüge von den Betroffenen nicht routinemäßig und auf Vorrat über einen lange zurückliegenden Zeitraum verlangen. In jedem Einzelfall ist die Erforderlichkeit der Vorlage zu prüfen. Im Rahmen ihrer Mitwirkungspflicht müssen Leistungsempfänger ihre Kontobelege aufbewahren, um sie im weiteren Verfahren erforderlichenfalls erneut vorlegen zu können.

1.5.2.3 Sozialdatenschutz gegenüber dem Arbeitgeber

An uns wendete sich ein Bürger, der Leistungen nach dem Sozialgesetzbuch Zweites Buch beantragt hatte. Zum Nachweis für seine Nebenbeschäftigung reichte er Lohnbescheinigungen ein. Eine Mitarbeiterin der Leistungsabteilung verlangte daraufhin die Telefonnummer des Arbeitgebers, um mit diesem die Unterlagen besprechen zu können. Gründe für diese Rücksprache wurden dem Antragsteller nicht benannt. Bei solch einer Verfahrensweise befürchtete der Antragsteller erhebliche Nachteile bei seinem Arbeitgeber.

Grundsätzlich dürfen Leistungsträger Sozialdaten dann erheben, wenn ihre Kenntnis für die Erfüllung einer ihnen im Sozialgesetzbuch zugewiesenen Aufgabe erforderlich ist. Voraussetzung jeder Erhebung ist also, dass der Leistungsträger ohne diese Informationen den Anspruch auf die Leistung bzw. deren Höhe nicht feststellen kann.

Darüber hinaus sind Sozialdaten grundsätzlich beim Betroffenen zu erheben. Unter bestimmten Voraussetzungen dürfen die Leistungsträger Sozialdaten anstatt beim Betroffenen bei anderen Personen oder Stellen erheben. Eine solche Erhebung ist zulässig, wenn der Betroffene ausdrücklich darin eingewilligt hat. Ohne Einwilligung ist eine Datenerhebung bei Dritten – hier beim Arbeitgeber – nur zulässig, wenn eine Rechtsvorschrift dies erlaubt.

Auf Sozialleistungen angewiesen zu sein, kann im gesellschaftlichen und beruflichen Umfeld stigmatisierend wirken und daher von den Betroffenen als diskriminierend empfunden werden. Unabhängig davon unterliegt diese Information dem Sozialgeheimnis und darf auch dem Arbeitgeber des in einer Nebenbeschäftigung tätigen Arbeitslosengeld-II-Empfängers nur in eng begrenzten Ausnahmefällen offenbart werden.

Im vorliegenden Fall hatte der Betroffene einer Datenerhebung bei seinem Arbeitgeber ausdrücklich widersprochen. Eine Einwilligung lag somit nicht vor. Eine Rechtsvorschrift, die hier eine Datenerhebung bzw. -übermittlung zugelassen hätte, gab es auch nicht. Der Betroffene hatte bereits alle erforderlichen Angaben, die zudem vom Leistungsträger nicht bezweifelt wurden, mitgeteilt.

Der Fall konnte sehr schnell abgeschlossen werden. Auf Grund unserer Intervention beim Leistungsträger unterblieb die Kontaktaufnahme mit dem Arbeitgeber des Betroffenen. Die Mitarbeiter wurden nochmals auf die Einhaltung datenschutzrechtlicher Vorschriften hingewiesen.

Der Schutz des Sozialgeheimnisses verlangt, dass Dritte von der Tatsache des Leistungsbezuges eines Bürgers ohne dessen Zustimmung oder ohne rechtliche Grundlage keine Kenntnis erhalten. Grundsätzlich sind die erforderlichen Daten beim Betroffenen selbst zu erheben.

2 Technisch-organisatorische Entwicklungen

2.1 Überregionale Initiativen zur Verbesserung der IT-Sicherheit

Es ist heute unbestritten, dass Wirtschaft und Gesellschaft auf das zuverlässige Funktionieren der Informationstechnik angewiesen sind. Vor dem Hintergrund vielfältiger Bedrohungen und zahlreicher Angriffe auf informationstechnische Systeme begrüßen wir deshalb auch aus der Sicht des Datenschutzes alle Initiativen, die eine Erhöhung des Niveaus der IT-Sicherheit zum Ziel haben.

Im Berichtszeitraum waren mehrere solche Aktivitäten auf überregionaler Ebene zu verzeichnen. Neben der Initiative „Deutschland sicher im Netz“ sind insbesondere der Bericht zur Lage der IT-Sicherheit in Deutschland und der Nationale Plan zum Schutz der Informationsinfrastrukturen zu nennen.

Die Initiative „Deutschland sicher im Netz“[12] wurde im Januar 2005 von 13 Partnern aus Gesellschaft, Politik und Wirtschaft gegründet. Sie richtet sich an Privatleute, Behörden und Institutionen sowie an kleine und mittlere Unternehmen, um diese Nutzer für die potenziellen Gefahren bei der Nutzung des Internets zu sensibilisieren und über geeignete Maßnahmen zur Verbesserung des eigenen Online-Schutzes zu informieren. Die Initiative hat sieben Handlungsversprechen abgegeben, von denen mittlerweile sechs erfüllt sind. Hierzu gehören z. B. eine kostenlose Sicherheitsüberprüfung für Privat-PCs, die Bereitstellung einer Lerneinheit für sicheren Online-Handel, Aktivitäten zum Erwerb von Medienkompetenz für Kinder und Jugendliche, ein Sicherheitspaket für den Mittelstand sowie Veranstaltungen an Universitäten zur Entwicklung sicherer Software.

[12] siehe https://www.sicher-im-netz.de

Der Bericht zur Lage der IT-Sicherheit in Deutschland[13] wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im August 2005 vorgelegt. Es ist der erste seiner Art. Die Autoren schätzen im Rahmen einer Bestandsaufnahme den gegenwärtigen Stand der IT-Sicherheit ein, erläutern Bedrohungen und Gefahren. Hervorzuheben sind insbesondere die große Anzahl von Sicherheitslücken in existierender Software, die immer kürzere Zeit bis zur Ausnutzung erkannter Lücken und die stark gestiegene Zahl von Schadprogrammen (Viren, Würmer, Trojaner). Besonders neue Technologien wie die drahtlose und mobile Kommunikation sind Angriffen ausgesetzt. Dem Bericht zufolge sind die Ursachen für erfolgreiche Angriffe häufig auch Nachlässigkeit in der Administration von IT-Systemen, organisatorische Schwächen sowie ein zu gering ausgeprägtes Sicherheitsbewusstsein der Anwender. Für die Zukunft prognostizieren die Autoren eine Zunahme sowohl der Quantität als auch der Qualität der Angriffe. Immer stärker werden zentrale, kritische Komponenten von IT-Infrastrukturen im Mittelpunkt von Angriffen stehen (z. B. Router, Firewalls, Server für Namensdienste). Es ist mit einer Professionalisierung und Kommerzialisierung der Internetkriminalität zu rechnen. Angriffe werden zielgerichtet und organisiert erfolgen und meist mit finanziellen Interessen verbunden sein (z. B. im Bereich der Wirtschaftsspionage).

Zu den aus der Bestandsaufnahme und den erwarteten Entwicklungen abgeleiteten erforderlichen Maßnahmen und Aktivitäten gehört insbesondere die intensivere Aufklärung über Gefahren und die Herausbildung eines Sicherheitsbewusstseins und einer Sicherheitskompetenz. Alle Mitarbeiter in Wirtschaft und Verwaltung wie auch Privatanwender sind für das Thema der IT-Sicherheit zu sensibilisieren und sollten zumindest Grundkenntnisse über Sicherheitsmaßnahmen erwerben. Verantwortliche haben die Risiken zu analysieren, denen ihre IT-Systeme ausgesetzt sind, den Schutzbedarf zu bestimmen und erforderliche Maßnahmen zu ergreifen. Insbesondere in der Verwaltung ist ein angemessen hohes Sicherheitsniveau zu realisieren. Geeignete IT-Sicherheitsmanagementsysteme sind zu installieren. Behörden haben IT-Sicherheitsbeauftragte zu benennen, die im Auftrag der Behördenleitung die Erstellung und Umsetzung von Sicherheitskonzepten koordinieren.

Ebenfalls im August 2005 wurde vom Bundesinnenministerium der „Nationale Plan zum Schutz der Informationsinfrastrukturen“[14] vorgelegt. Dieser entspricht der IT-Sicherheitsstrategie der Bundesregierung und benennt strategische Ziele in den drei Bereichen Prävention, Reaktion und Nachhaltigkeit. Auf dem Gebiet der Prävention geht es um den angemessenen Schutz von Informationsinfrastrukturen, die Schärfung des Bewusstseins über Risiken bei der IT-Nutzung, den Einsatz sicherer IT-Produkte und -Systeme und die Gewährleistung umfassender Schutzvorkehrungen auf der Basis vorgegebener

[13] siehe http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf

[14] im Internet verfügbar unter http://www.bmi.bund.de

Richtlinien und abgestimmter Sicherheitsstrategien. Im Bereich der Reaktion formuliert der Plan als Ziele das Erkennen, Erfassen und Bewerten von IT-Sicherheitsvorfällen, das Informieren und Warnen sowie das wirkungsvolle, koordinierte Handeln bei aufgetretenen Vorfällen. Unter dem Aspekt der Nachhaltigkeit werden die Förderung von vertrauenswürdigen und verlässlichen IT-Produkten aus Deutschland, von Forschung und Entwicklung sowie von Aktivitäten in Schule und Ausbildung genannt. Weitere Ziele sind der Ausbau internationaler Kooperationen und das Setzen von Standards auf dem Gebiet der IT-Sicherheit. Für die Realisierung des Nationalen Plans zum Schutz von Informationsinfrastrukturen werden verschiedene Umsetzungspläne erarbeitet. Außerdem soll der Plan selbst regelmäßig überprüft und ggf. aktuellen Entwicklungen angepasst werden.

2.2 Sicherheit in Funknetzen

Während sich die Anzahl von Funknetzen im Land immer weiter erhöht, werden die Gefahren und Risiken ihres Einsatzes nicht immer im vollen Umfang erkannt.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat unter unserer Leitung eine Orientierungshilfe „Datenschutz in drahtlosen Netzen“ erarbeitet, die auf unserer Website verfügbar ist. Sie bietet in komprimierter Form eine Übersicht über mögliche Gefährdungen und geeignete Schutzmaßnahmen beim Einsatz von drahtlosen Technologien und richtet sich an behördliche Datenschutzbeauftragte, IT-Verantwortliche und Administratoren, die sich mit der Planung, dem Aufbau und dem Betrieb von drahtlosen Netzen beschäftigen. Es werden folgende Themen behandelt:

- Wireless Local Area Networks (WLANs),
- Bluetooth-Netze,
- Infrarotschnittstellen,
- mobile Endgeräte (z. B. Tastaturen, Mäuse und Personal Digital Assistants),
- allgemeingültige Sicherheitsmaßnahmen (u. a. Firewall, Verschlüsselung, Virenschutz) und
- datenschutzrechtliche Aspekte beim Einsatz drahtloser Netze.

Werden personenbezogene Daten in drahtlosen Netzen übertragen, sind zusätzliche technische und organisatorische Maßnahmen zu realisieren, die den Schutz dieser Daten gewährleisten. Die standardmäßig in den Produkten implementierten Sicherheitsmechanismen reichen in den meisten Fällen nicht aus.

2.3 Voice over IP – Telefonieren über das Internet

Telefonieren über das Internet (Voice over IP – VoIP) erfreut sich nicht nur bei Privatkunden zunehmender Beliebtheit. Auch Behörden oder Unternehmen versprechen sich davon Kostenvorteile. Die Vertraulichkeit der Telefongespräche ist jedoch nicht immer gewährleistet. Gespräche können bereits mit geringem Aufwand abgehört werden.

Auf der Basis des Internet-Protokolls (IP) werden bei VoIP die Sprachdaten zunächst in einzelne Pakete unterteilt und per Internet an den Gesprächsteilnehmer übermittelt. Dieser hält eine Technik vor, mithilfe derer die Pakete wieder in der richtigen Reihenfolge zusammengesetzt und als Sprache ausgegeben werden. Für diesen gesamten Vorgang stehen – unabhängig von der geografischen Entfernung der beiden Teilnehmer – nur Sekundenbruchteile zur Verfügung.

Ohne Hilfe eines Computers können Privatkunden entweder spezielle VoIP-Telefone verwenden oder ihr bisheriges Telefon mittels eines Adapters an die neue Technologie anpassen. Mithilfe einer VoIP-Software (Softphone), eines Lautsprechers und eines Mikrofons kann auch der PC ohne weitere Zusatzgeräte für die Kommunikation genutzt werden. In Behörden- und Firmennetzen wird in der Regel die vorhandene ISDN-Telefonanlage entweder entsprechend ergänzt oder durch eine rechnergestützte Software für Telefonanlagen ersetzt.

Im Vergleich zur herkömmlichen Telefonverbindung birgt das Telefonieren über das Internet ein größeres Gefährdungspotenzial für die Vertraulichkeit der Gespräche sowie für die Verlässlichkeit der Kommunikation. Dazu gehören insbesondere[15]:

- Lahmlegung von Netzwerken (Denial of Service) durch automatisierte Versendung von Klingelrundrufen,
- gezielte Blockierung einzelner Anschlüsse durch Datenüberflutung,
- mangelnde Einbindung von VoIP in bestehende Router und Firewalls,
- Ausspähung und Manipulation unverschlüsselt übertragener Daten,
- Missbrauch von Authentifizierungsdaten (Identitätsdiebstahl),
- Versand von SPAM (SPIT).

Hinzu kommt, dass Anbieter von VoIP-Diensten, die ihren Sitz außerhalb der Europäischen Union haben, geringeren Datenschutzanforderungen unterliegen, als sie innerhalb der Union vorgeschrieben sind. Da Festnetzteilnehmer

[15] siehe auch die Studie „VoIPSec“ des Bundesamtes für Sicherheit in der Informationstechnik: http://www.bsi.bund.de/literat/studien/VoIP/index.htm

in der Regel nicht erkennen können, dass ihr Gesprächspartner für den Anruf das Internet nutzt, können sie das Sicherheitsrisiko kaum einschätzen.

Noch wird bei dem Einsatz von VoIP eine vollständige Verschlüsselung der Kommunikation nicht angeboten, obwohl das Telefonieren über das Internet genauso dem Fernmeldegeheimnis unterliegt wie herkömmliche Telefonate. Unternehmen und Behörden sowie Anbieter von VoIP und Gerätehersteller sind daher gefordert, durch technische Vorkehrungen ein ausreichendes Sicherheitsniveau zu gewährleisten.

Auf der Basis der Arbeit einer Arbeitsgruppe des Arbeitskreises „Technik" wurde im Oktober 2005 bei der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung „Telefonieren mit Internettechnologie (Voice over IP – VoIP) verabschiedet, in der auf die Gefahren der Internet-Telefonie aufmerksam gemacht wird.[16]

Um Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität bei der Sprachübertragung über das Internet (VoIP) gewährleisten zu können, sind im Datennetz, auf den beteiligten Servern und an den installierten Endgeräten angemessene Sicherheitsmaßnahmen umzusetzen. Der Schutz des Fernmeldegeheimnisses kann nur über eine Verschlüsselung der zu übertragenen Daten garantiert werden.

2.4 Anonym im Internet

Jeder Internetnutzer hinterlässt beim Surfen Spuren und wird dadurch im Internet identifizierbar. Durch Verwendung von Anonymisierungsdiensten kann der Nutzer sein Recht auf Anonymität im Internet durchsetzen.

Sobald ein Nutzer eine Verbindung mit dem Internet hergestellt hat, wird sein Rechner durch eine Nummer, die so genannte IP-Adresse (z. B. 144.3.45.7), identifizierbar. Sei es beim bloßen Surfen, Online-Banking oder bei der Bestellung in einem Online-Shop. Beim Zugriff auf eine Webseite wird u. a. diese IP-Adresse an den Betreiber der Webseite übertragen. Die Speicherung dieser IP-Adresse darf nach deutschem Recht grundsätzlich nur für Abrechnungszwecke genutzt werden. Dennoch kann nicht ausgeschlossen werden, dass durch unzulässige Speicherung der IP-Adressen Nutzerprofile erstellt werden. Nach § 4 Abs. 6 Teledienstedatenschutzgesetz sind die Diensteanbieter verpflichtet, den Nutzern die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter einem Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Diese datenschutzfreundliche Form

[16] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 3

der Internetnutzung wird derzeit jedoch von den Diensteanbietern noch nicht zur Verfügung gestellt.

Die Lösung des Problems liegt für den Nutzer in der Nutzung von Anonymisierungsdiensten. Dabei durchlaufen die Datenpakete, in denen die IP-Adresse der Nutzer enthalten ist, bevor sie den eigentlichen Zielserver im Internet erreichen, eine Reihe von Proxy-Servern als Zwischen-Stationen. Im Ergebnis entsteht ein anonymisiertes Datenpaket, von dem aus nicht mehr auf den Internetnutzer rückgeschlossen werden kann.

Ein schon in der Praxis etablierter Anonymisierungsdienst ist AN.ON (Anonymität Online)[17]. Dabei handelt es sich um ein vom Bundesministerium für Wirtschaft und Arbeit gefördertes Projekt, der Dienst wird von den Universitäten Dresden, Regensburg und Berlin in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betrieben. Bevor man den Anonymisierungsdienst AN.ON nutzen kann, muss auf dem Rechner eine zusätzliche Software installiert werden, die auf der Webseite des AN.ON-Dienstes kostenlos zur Verfügung gestellt wird.

Auch beim Surfen im Internet sollten die Nutzer einen hohen Grad an Anonymität erreichen können. Durch Nutzung von Anonymisierungsdiensten lässt sich verhindern, dass über den Umweg von IP-Adressen unzulässig Profile erstellt werden.

2.5 Identitätsmanagement bei der Internetnutzung

Die Möglichkeiten des Internets sind vielfältig: das Kommunizieren per E-Mail und Chat, das Einkaufen bei Versandhäusern oder das Ersteigern von Gebrauchtwaren sind nur einige Beispiele. Zur Wahrung seiner Privatsphäre sollte jeder Nutzer darauf achten, hierbei nicht unnötig viele persönliche Daten zu offenbaren.

Häufig verwenden Web-Surfer verschiedene Pseudonyme und Passwörter, um einzelne Dienste im Internet in Anspruch zu nehmen. Sie legen sich diverse Online-Identitäten zu und können damit in unterschiedlichen Rollen agieren. Zum Teil verlangen Diensteanbieter bei der Registrierung unter einem Pseudonym auch die Angabe bestimmter persönlicher Daten (z. B. für die Abwicklung von Zahlungsvorgängen). Mit steigender Anzahl der verschiedenen Identitäten fällt es einem Anwender immer schwerer, den Überblick zu behalten, welche Pseudonyme er angelegt und welche Daten er welchem Anbieter zu welchem Zweck zur Verfügung gestellt hat.

[17] siehe http://anon.inf.tu-dresden.de

Identitätsmanagementsysteme haben das Ziel, den Internetnutzer hierbei technisch zu unterstützen. Sie dienen der Verwaltung und Verarbeitung der verschiedenen Identitäten und erlauben die Auswahl und die Kontrolle über den Umfang der in einem bestimmten Kontext offenbarten personenbezogenen Daten. Der Nutzer hat damit die Möglichkeit, die Preisgabe seiner persönlichen Daten zu steuern oder zumindest nachvollziehen zu können und somit sein Recht auf informationelle Selbstbestimmung besser wahrzunehmen.

Die Palette der technischen Lösungen, die sich selbst – nicht immer zu Recht – als Identitätsmanagementsysteme bezeichnen, ist vielfältig. Auf der einen Seite gibt es Ansätze, bei denen ein oder mehrere Diensteanbieter das Identitätsmanagement für viele Nutzer übernehmen. Beispiel für eine zentrale Lösung ist das heftig kritisierte und praktisch nicht mehr relevante Microsoft Passport: Der Nutzer registriert sich nur einmal mit allen personenbezogenen Daten bei diesem Dienst. Anschließend kann er verschiedenste Partnerwebseiten nutzen – für die jeweilige Anmeldung werden die personenbezogenen Daten im Hintergrund vom Passport-Server übertragen. Im Unterschied dazu verfolgt die Liberty Alliance, ein Zusammenschluss mehrerer Unternehmen, einen dezentralen Ansatz: Personenbezogene Daten liegen auf den Servern der kooperierenden Diensteanbieter verteilt und werden nur im erforderlichen Umfang und über standardisierte Protokolle zwischen diesen ausgetauscht. Sowohl der zentrale als auch der dezentrale Ansatz gestatten dem Nutzer nicht die Kontrolle über den Austausch seiner personenbezogenen Daten.

Datenschutzfreundlichere Lösungen für das Identitätsmanagement gehen demgegenüber davon aus, dass die Software zur Verwaltung von Pseudonymen und zugeordneten personenbezogenen Daten auf dem Rechner des Nutzers arbeitet. Auch hier gibt es Angebote mit unterschiedlichem Funktionsumfang. Er reicht von der sicheren Verwaltung von Passwörtern für unterschiedliche Internetangebote, über das datensparsame Ausfüllen von Formularen mit personenbezogenen Daten entsprechend dem jeweiligen Kontext bis zur Führung von Protokollen über die Empfänger und den Zeitpunkt von Datenübermittlungen. Einfachere Lösungen zur Passwortverwaltung finden sich mittlerweile in vielen Web-Browsern; komplexe Lösungen mit umfassenderen Funktionen sind meist Ergebnisse von Forschungsprojekten und tragen noch experimentellen Charakter. Auch Microsoft hat aus der Kritik an Passport gelernt und für die kommende Version des Windows-Betriebssystems eine Software mit dem Namen InfoCard angekündigt. Diese soll es dem Anwender dann gestatten, seine Pseudonyme und die relevanten personenbezogenen Daten selbst auf dem eigenen Rechner zu verwalten.

Identitätsmanagementsysteme gewinnen bei der Nutzung des Internets zunehmend an Bedeutung. Zur Umsetzung des Selbstdatenschutzes und zur Gewährleistung von Transparenz sollten derartige Systeme stets auf dem Rechner des Anwenders betrieben werden.

2.6 Computerkriminalität

Internet-Kriminalität hat in den letzten Jahren insbesondere durch den Missbrauch von Dialern, betrügerische Angebote bei Online-Auktionen, den Diebstahl personenbezogener Daten sowie durch die Verbreitung von Viren kontinuierlich zugenommen.

Dialer sind Einwahlprogramme in das Internet, deren Aufgabe im Betrieb kostenpflichtiger Internetangebote besteht. Unseriöse Anbieter nutzen diese, um hohe Kosten für zumeist geringe oder gar keine Leistung zunächst unbemerkt abzurechnen und die Nutzer dadurch finanziell zu schädigen. In der Vergangenheit wurden hierfür Telefonnummern mit der Vorwahl 0190 eingesetzt, die jedoch zum Schutz der Verbraucher zum Ende des Jahres 2005 deaktiviert wurden. Anbieter kostenpflichtiger Internetdienste müssen nunmehr 0900-Nummern verwenden und sich bei der Bundesnetzagentur registrieren lassen. Ihre Identifizierung wird dadurch vereinfacht; unseriöse Anbieter können leichter verfolgt werden.

Auktionsplattformen im Internet werden von Betrügern genutzt, indem der Versand bereits im Voraus bezahlter Ware verweigert oder Produkte unter Verwendung einer falschen Identität angeboten bzw. ersteigert werden.

Das so genannte Phishing – der Diebstahl und anschließende Missbrauch personenbezogener Daten – beginnt zumeist mit einer E-Mail, die den Empfänger verleiten soll, vertrauliche Informationen wie z. B. Passwörter oder Zugangsdaten für das Online-Banking auf einer in der E-Mail verlinkten Website preiszugeben. Durch die Ähnlichkeit dieser Seiten mit einer tatsächlich existierenden Homepage (z. B. eines Kreditinstituts) spiegeln die Betrüger eine nicht vorhandene Vertrauenswürdigkeit vor. Sie verwenden die gestohlenen Zugangsdaten schließlich, um die Identität der Opfer zu übernehmen und in dessen Namen Geschäfte zu tätigen. Zum Schutz gegen das Phishing sollte man sicherheitsrelevante Internetseiten nie über Links aus einer E-Mail aufrufen, sondern stets selbst in die Adresszeile des Browsers eingeben oder per Lesezeichen ansteuern. Grundsätzlich gilt: Banken und Versicherungen bitten nicht telefonisch, per E-Mail oder SMS um die Übermittlung von Zugangsdaten.

Auch Viren breiten sich bevorzugt über die Postfächer von E-Mail-Empfängern aus und verschicken sich ihrerseits selbst per E-Mail, um

dadurch weitere Rechner zu infizieren. Ziel des Versands von Viren ist es nicht mehr nur, Schäden auf den Rechnern zu verursachen. Vielmehr werden verstärkt betrügerische Absichten verfolgt, indem z. B. E-Mail-Adressen, die auf einem infizierten PC gespeichert sind, gesammelt und an Spammer verkauft oder infizierte Rechner (-netze) für weitere Angriffe vermietet werden. Der Einsatz einer Anti-Viren-Software sowie die Einhaltung einschlägiger Verhaltensregeln bei der Nutzung des Internet bieten hier einen ausreichenden Schutz.[18]

Das Risiko, Opfer von Computerkriminalität zu werden, kann durch das Wissen über Kriminalitätsformen und die Funktion von Schadsoftware, durch technische Sicherheitsmaßnahmen und ein gesundes Misstrauen auf ein Minimum reduziert werden.

2.7 Methoden der Risikoanalyse

Vor der Erstellung eines Sicherheitskonzepts muss zunächst ermittelt werden, gegen welche Gefährdungen überhaupt Maßnahmen ergriffen werden sollen. Wie ist bei einer solchen Risikoanalyse vorzugehen?

Eine Risikoanalyse dient dazu, im Vorfeld der Anwendung des Verfahrens bestehende oder gegebene Sicherheitslücken zu identifizieren und ihr Risikopotenzial zu bewerten, um daraus geeignete Maßnahmen zum Schutz der elektronischen Datenverarbeitung abzuleiten. Nach Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik sind drei Varianten denkbar: Der Grundschutzansatz, die detaillierte Risikoanalyse und eine Kombination aus beiden.

Der Grundschutzansatz geht von einer pauschalierten Gefährdungslage aus, die sich an den Grundbedrohungen Vertraulichkeit, Integrität und Verfügbarkeit orientiert. Er ist geeignet für IT-Systeme, in denen Daten niedrigen bis mittleren Schutzbedarfs verarbeitet werden. Die Risikoanalyse nach dem Grundschutzansatz beinhaltet im Wesentlichen die Schutzbedarfsfeststellung. Eine weitergehende Analyse ist nicht erforderlich.

Eine Risikoanalyse für IT-Systeme, mit denen personenbezogene Daten hohen bis sehr hohen Schutzbedarfs verarbeitet werden, fällt aufwändiger aus. Sie beginnt mit einer Bestandsaufnahme aller Anwendungen und verarbeiteten Informationen. Darauf basierend werden der jeweilige Schutzbedarf ermittelt sowie mögliche Schwachstellen und Bedrohungen identifiziert und analysiert. Aus der Wahrscheinlichkeit, dass ein Schaden eintritt sowie aus der möglichen Schadenshöhe bestimmt sich das potenzielle Risiko. Das Ergebnis

[18] siehe das Faltblatt „Keine Chance den Computer-Viren!“ auf unserer Website

einer Bewertung desselben führt zu einer Einstufung in tragbare und nicht tragbare Risiken. Gegen die nicht tragbaren Risiken müssen nun Maßnahmen bestimmt werden. Die Vorgehensweise für diese detaillierte Risikoanalyse ist dem IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik zu entnehmen.[19]

Eine Kombination von Grundschutz und detaillierter Risikoanalyse eignet sich vor allem für IT-Systeme, die nur punktuell einen erhöhten Schutzbedarf aufweisen. Hier werden zunächst die standardisierten Maßnahmen des Grundschutzes umgesetzt, um für alle Anwendungen den mittleren Schutzbedarf abzudecken. Eine detaillierte Risikoanalyse wird dann nicht umfassend, sondern nur an den Stellen durchgeführt, für die der erhöhte Schutzbedarf festgestellt wurde. Der Aufwand kann dadurch erheblich reduziert werden. Neben dem IT-Sicherheitshandbuch steht hierfür auch das Modell „Risikoanalyse auf der Basis von IT-Grundschutz“ als Orientierungshilfe zur Verfügung.[20]

Eine Risikoanalyse ist die Grundlage für jedes IT-Sicherheitskonzept. Der Aufwand für ihre Durchführung hängt vom Schutzbedarf der jeweiligen Datenverarbeitung ab.

2.8 IT-Sicherheitskonzepte im öffentlichen Bereich

Jede Daten verarbeitende Stelle muss ein IT-Sicherheitskonzept erstellen, sofern erstmalig ein automatisiertes Verfahren eingeführt wird, mit dem personenbezogene Daten verarbeitet werden. Dieser Forderung wird in der öffentlichen Verwaltung zum großen Teil noch nicht ausreichend entsprochen.

Mit dem IT-Sicherheitskonzept soll sichergestellt werden, dass die von einem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen beherrscht werden. Nur wenige Daten verarbeitende Stellen verfügen über fachlich korrekte Analysen und Konzepte. Auf Grund fehlender finanzieller Mittel und unzureichender personeller Ressourcen wird auf sicherheitsrelevante Untersuchungen verzichtet. Historisch gewachsene Strukturen sowie das bisherige Ausbleiben größerer sicherheitsrelevanter Vorfälle belegen nicht, dass ganzheitlich und sicherheitstechnisch ausreichend vorgesorgt wurde. Beispielsweise verfügt selbst das Landeskriminalamt trotz eigener Ankündigung noch immer nicht über ein tragbares IT-Sicherheitskonzept.

Der technische Fortschritt und die Modernisierung der IT-Infrastruktur machen es notwendig, dass die sicherheitstechnischen Maßnahmen ebenfalls

[19] siehe http://www.bsi.bund.de/literat/kriterie.htm

[20] siehe http://www.bsi.bund.de/gshb/risikoanalyse/index.htm

weiterentwickelt und an die neuen Gegebenheiten angepasst werden. Wird dieser notwendige Anpassungsprozess nicht rechtzeitig erkannt, so können unkalkulierbare und untragbare Risiken für die IT-Sicherheit der betroffenen Institution entstehen.

Bei der Erstellung von IT-Sicherheitskonzepten empfehlen wir, nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik vorzugehen. Dieses enthält Standard-Sicherheitsmaßnahmen, die auf den mittleren Schutzbedarf abgestimmt sind. Die Umsetzung dieser Maßnahmen entspricht den Mindestanforderungen an die IT-Sicherheit. Werden Komponenten mit höherem Schutzbedarf ermittelt, so ist eine detailliertere Untersuchung erforderlich. Automatisierte Verfahren können den Anwender bei der Erstellung eines IT-Sicherheitskonzepts unterstützen. Es muss nur darauf geachtet werden, dass in selbst entwickelten Anwendungen komplexe Zusammenhänge und logische Ablauffolgen korrekt implementiert werden.

Sicherheitskonzepte müssen nicht zwingend nach dem IT-Grundschutzhandbuch erstellt werden, auch andere anerkannte Standards können als Basis dienen, sofern mindestens dem Sicherheitsstandard des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik entsprochen wird.

In der brandenburgischen Verwaltung existieren noch immer erhebliche Defizite bei der Umsetzung von IT-Sicherheitskonzepten nach dem Brandenburgischen Datenschutzgesetz. In den Daten verarbeitenden Stellen hat sich das notwendige Bewusstsein für die IT-Sicherheit noch nicht ausreichend entwickelt.

2.9 IT-Sicherheitsleitlinie für die Landesverwaltung

In unserem letzten Tätigkeitsbericht[21] hatten wir die zeitnahe Erarbeitung einer zentralen IT-Sicherheitsleitlinie für die Landesverwaltung Brandenburg als Untersetzung der IT-Strategie 2004 – 2008 angemahnt. Nun zeichnen sich positive Entwicklungen ab.

Die von der Landesregierung verabschiedete IT-Strategie 2004 – 2008 legt die wesentlichen Ziele, Inhalte und Schritte zum weiteren Ausbau der Informations- und Kommunikationstechnik in der Landesverwaltung Brandenburg fest. Sie sieht u. a. den Aufbau einer einheitlichen IT-Sicherheitsarchitektur vor, zu der auch ein zentrales IT-Sicherheitsmanagement und allgemeine Richtlinien zur Gewährleistung der IT-Sicherheit in der Landesverwaltung gehören sollen.

[21] vgl. Tätigkeitsbericht 2003, A 2.9

Im Berichtszeitraum setzte der Interministerielle Ausschuss für Informationstechnik eine Arbeitsgruppe ein, die unter Leitung der IT-Leitstelle im Ministerium des Innern stand und deren Auftrag die Erarbeitung des Entwurfs für eine IT-Sicherheitsleitlinie war. Unsere Dienststelle war an den Arbeiten beteiligt.

Der vorliegende Entwurf der IT-Sicherheitsleitlinie[22] beschreibt den Aufbau und die Verwaltung eines zentral gesteuerten, ressortübergreifenden IT-Sicherheitsmanagementsystems. Ziel dieses Systems ist es, durch „eine ressortübergreifende IT-Sicherheitsorganisation und ressortübergreifende Regelwerke die Erfüllung der IT-Sicherheitsziele in der Landesverwaltung Brandenburg zu gewährleisten". Es soll sichergestellt werden, dass „dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um die Informationswerte und personenbezogene Daten angemessen zu schützen und um die Verfügbarkeit von informationstechnischen bzw. kommunikationstechnischen Verfahren zu gewährleisten."

Insbesondere legt der Entwurf der Sicherheitsleitlinie Mindeststandards für die Realisierung der IT-Sicherheit fest. So ist vor dem Einsatz informationstechnischer Verfahren zu prüfen, ob Risiken für die Aufrechterhaltung von Vertraulichkeit, Integrität und/oder Verfügbarkeit bestehen oder sich ergeben können. Gegebenenfalls sind in einem Sicherheitskonzept geeignete Sicherheitsmaßnahmen zur Beherrschung der Risiken festzulegen und für das Verfahren umzusetzen. Das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik bietet hierfür sowohl eine geeignete Methodik als auch einen Katalog grundlegender Maßnahmen. Sicherheitskonzepte, die hinter das Niveau des Grundschutzhandbuchs zurückfallen, sind nach dem Entwurf der Leitlinie nicht zulässig.

Zu den organisatorischen Festlegungen des Leitlinienentwurfs gehört die Einrichtung eines Sicherheitsmanagement-Teams des Landes Brandenburg, das aus dem von der IT-Leitstelle benannten IT-Sicherheitsmanager des Landes und den IT-Sicherheitsbeauftragten der einzelnen Ressorts besteht. Das Team ist u. a. für die Festlegung zentraler Ziele und Strategien der IT-Sicherheit sowie für die Fortschreibung der Sicherheitsleitlinie zuständig. Den IT-Sicherheitsbeauftragten der Ressorts obliegt die Präzisierung und Ausgestaltung der zentralen Leitlinie in ihrem Verantwortungsbereich.

Parallel soll ein CERT Brandenburg (Computer Emergency Response Team) eingerichtet werden, das ein Lagezentrum zur IT-Sicherheit betreibt, Warn-

[22] Stand vom 16. Dezember 2005

meldungen herausgibt, Hilfestellungen für Anwender anbietet sowie Sicherheitsvorfälle in der Landesverwaltung registriert und analysiert.

Der vorliegende Entwurf der IT-Sicherheitsleitlinie bietet eine gute Grundlage für die Etablierung eines landesweiten, übergreifenden Sicherheitsmanagementsystems. Nach der Verabschiedung der Leitlinie gilt es, sie in der täglichen Arbeit mit Leben zu erfüllen, die vorgesehenen Maßnahmen zu realisieren und die Einhaltung zu kontrollieren. Auch die Daten verarbeitenden Stellen in den Kommunen sollten sich an den in der Leitlinie festgelegten technischen Mindeststandards zur Realisierung der IT-Sicherheit orientieren.

2.10 Verschlüsselung und digitale Signatur

Verschlüsselung und digitale Signatur setzen sich im Land Brandenburg nur sehr schleppend durch, obwohl wir bereits mehrfach auf die Notwendigkeit des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten bei Transport und Speicherung hingewiesen haben.

Mit der Einführung des Landesverwaltungsnetzes Version 3 im Jahr 2004 wurde die Möglichkeit geschaffen, die Daten zwischen den öffentlichen Stellen grundsätzlich verschlüsselt zu übertragen. Dabei handelt es sich um eine Verbindungsverschlüsselung (IPSec) zwischen den Routern. Die Verbindungsverschlüsselung ist geeignet, personenbezogene Daten bis zur Stufe B (mittlerer Schutzbedarf) unseres Schutzstufenkonzeptes sicher zu übertragen. Handelt es sich jedoch um Daten mit einem höheren Schutzbedarf (Daten der Schutzstufe C bzw. besondere Kategorien personenbezogener Daten gem. § 4a BbgDSG), sind diese auf Anwendungsebene (Ende-zu-Ende-Verschlüsselung) zu verschlüsseln. Das bedeutet u. a., dass die personenbezogenen Daten nicht nur im Landesverwaltungsnetz, sondern auch im lokalen Netz der öffentlichen Stelle verschlüsselt übertragen werden.

Nicht nur bei dezentralen, sondern auch bei zentralen Verfahren ist die Verschlüsselung unabdingbar. Ein Beispiel für ein zentrales Verfahren ist das Haushalts-, Kassen- und Rechnungswesen, bei dem noch immer Teile der Datenübertragung unverschlüsselt erfolgen.

Derzeit bleibt es den öffentlichen Stellen überlassen, ob die technisch mögliche Verbindungsverschlüsselung genutzt wird oder nicht. In anderen Bundesländern wurden andere Wege gegangen. Man ging dort davon aus, dass in fast allen an das jeweilige Landesverwaltungsnetz angeschlossenen öffentlichen Stellen personenbezogene Daten übertragen werden und führte eine Grundverschlüsselung aller Verbindungen ein. Auch Brandenburg sollte diesem Beispiel folgen.

Auch die landesweite Einführung der digitalen Signatur zur Gewährleistung der Integrität, Zurechenbarkeit und Verbindlichkeit von übertragenen und gespeicherten personenbezogenen Daten sollte ernsthafter als bisher betrieben werden. Auf Grund der Komplexität der Prozesse sollte sie nur von zentraler Stelle aus geplant und umgesetzt werden. Schon vor einigen Jahren hat sich eine Arbeitsgruppe des Interministeriellen Ausschusses für Informationstechnik u. a. mit der Implementierung der Verschlüsselung und der digitalen Signatur im Bereich der E-Mail-Kommunikation beschäftigt. Auf Grund der unterschiedlichen Kommunikationssysteme in der Landesverwaltung (GroupWise und Exchange) entstanden Kompatibilitätsprobleme, die eine flächendeckende Einführung verhinderten.

Verschlüsselung und digitale Signaturen sind besonders geeignet, um die Vertraulichkeit, Verbindlichkeit und Integrität bei der Verarbeitung personenbezogener Daten zu gewährleisten. Die Landesregierung wird aufgefordert, Maßnahmen zu ergreifen, die eine zentrale flächendeckende Einführung kryptographischer Verfahren sicherstellen.

2.11 Sicheres Löschen von Festplatten – eine unendliche Geschichte?

Neue Studien und Umfragen, verschiedene Anfragen aus der Landesverwaltung und von interessierten Bürgern sowie konkrete, aktuelle Fälle haben uns dazu veranlasst, die Frage des sicheren (d. h. vollständigen und nicht umkehrbaren) Löschens von Festplatten erneut aufzugreifen und vertiefend zu behandeln.

Für eine Studie zum Datenschutz bei gebrauchten Festplatten ersteigerte eine Firma zu Beginn des Jahres 2005 im Internet 200 Festplatten. Die Untersuchung dieser Festplatten mit einfach zu beschaffender Datenrettungssoftware ergab, dass 71,5 % der noch intakten Festplatten persönliche und geschäftliche Daten ihrer Vorbesitzer enthielten, die erfolgreich rekonstruiert werden konnten. Unter anderem wurden interne Berichte und Protokolle einer Bundesbehörde, Geschäftsunterlagen einer deutschen Großbank sowie der Schriftverkehr eines Unternehmens gefunden.

Dass auch brisantes Material der brandenburgischen Polizei auf im Internet ersteigerten Festplatten zu finden sein kann, zeigt ein konkreter Fall aus dem Berichtszeitraum, der auch die Presse beschäftigt hat. Ein Angestellter des Zentraldienstes der Polizei hatte mehrere Festplatten, die zur Vernichtung durch eine private Firma vorgesehen waren und deshalb in seiner Einrichtung zwischengelagert wurden, entwendet und bei einem Internetauktionshaus zum Kauf angeboten. Ein Student ersteigerte eine dieser Festplatten, konnte

darauf enthaltene Daten rekonstruieren und wandte sich an die Presse. Die internen Ermittlungen führten erfreulicherweise zur schnellen Aufklärung des Falles sowie zur Überarbeitung der organisatorischen Richtlinien für die Registrierung und Aussonderung von Festplatten bei der brandenburgischen Polizei.

Die genannten Beispiele machen deutlich, dass die Sensibilisierung der verantwortlichen Entscheidungsträger, der Administratoren sowie jedes einzelnen Nutzers für das Problem des sicheren Löschens von Festplatten vor deren Verkauf, Aussonderung, Vermietung, Rückgabe, Reparatur oder neuen Nutzung unabdingbar ist. Technische und organisatorische Maßnahmen zum sicheren Löschen von Festplatten sind in die Sicherheits- und Datenschutzkonzepte der Daten verarbeitenden Stellen aufzunehmen und mit konkreten Handlungsanweisungen zu untersetzen. Eine geeignete Auswahl der Maßnahmen erlaubt auch die Begrenzung des Restrisikos für die Datensicherheit, welches sich aus menschlichem Fehlverhalten ergeben kann.

Vor diesem Hintergrund veröffentlichte der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum eine Orientierungshilfe, die von unserer Behörde erarbeitet wurde. Diese Orientierungshilfe enthält neben einer Darstellung der Grundlagen des Löschens konkrete Empfehlungen für die praktische Arbeit sowie Hinweise zu (kostenlosen) Softwarewerkzeugen für das sichere Löschen magnetischer Datenträger. Sie wird ergänzt durch ein Faltblatt der Landesbeauftragten. Beide Veröffentlichungen sind in unserem Internetangebot abrufbar.

Zu den wesentlichen Empfehlungen gehören folgende Punkte:

- Technisch-organisatorische Maßnahmen und Handlungsanweisungen zum sicheren Löschen von Festplatten müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
- Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu können verschlüsselte Dateisysteme verwendet werden. Zu beachten ist, dass auch temporäre und Auslagerungsdateien sowie Sicherungskopien schutzwürdige Daten enthalten können.
- Sollen noch intakte Datenträger verkauft, ausgesondert, vermietet, zurückgegeben oder einer neuen Nutzung zugeführt werden, so sind sie zuvor durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen.
- Das selektive Löschen einzelner Dateien durch Überschreiben eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der schutzwürdigen

Daten in diesen Dateien an anderen Orten abgelegt wurden oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können.
- Das einmalige, komplette Überschreiben mit Zufallszahlen sollte für Daten jeder Art praktiziert werden. Beim Löschen von personenbezogenen oder vertraulichen Daten niedriger bis mittlerer Schutzstufe sollten 3 bis 7 Überschreibzyklen ausgeführt werden. Für Daten hoher Schutzstufe oder Datenträger, die spezielle Aufzeichnungsverfahren nutzen, kann noch häufigeres Überschreiben sinnvoll sein.
- Defekte Datenträger lassen sich nur physikalisch zerstören: mechanisch durch hinreichend feine Zerkleinerung, thermisch durch Erhitzung auf sehr hohe Temperaturen oder magnetisch durch Durchflutung mit starken äußeren Magnetfeldern.
- Für Datenträger mit personenbezogenen oder vertraulichen Daten hoher Schutzstufe kann die physikalische Zerstörung von Vorteil sein, da sie gegenüber dem mehrfachen, kompletten Überschreiben mit Zufallszahlen einen geringeren zeitlichen Aufwand verursacht.

Technische und organisatorische Maßnahmen zum sicheren Löschen von Festplatten dürfen in keinem Sicherheitskonzept öffentlicher Daten verarbeitender Stellen fehlen. Das ein- oder mehrmalige, komplette Überschreiben der Daten sowie die physikalische Zerstörung des Datenträgers sind geeignet, Datenspuren zu vernichten. Um den Missbrauch von schutzwürdigen Daten auch nach dem Diebstahl von Festplatten oder ganzen Computern zu erschweren, sollten diese Daten bereits verschlüsselt gespeichert werden.

2.12 Datenschutzgerechter Einsatz von Laptop und PDA

Laptop und PDA (Personal Digital Assistant) gehören in der öffentlichen Verwaltung mittlerweile zur Standardausrüstung. Auf Grund ihrer Mobilität ergeben sich erhöhte Anforderungen an die Sicherheit und den Schutz der auf ihnen verarbeiteten personenbezogenen Daten.

Moderne Laptops unterscheiden sich in technischer Hinsicht von herkömmlichen PCs nur durch ihre Mobilität. PDAs dagegen waren ursprünglich kompakter und dienten vorrangig als Terminkalender, Nachschlagewerk und zur Erfassung relativ geringer Datenmengen. Mittlerweile sind auch PDAs mit einer dem PC sehr ähnlichen Ausstattung sowie Geräte mit integriertem Mobiltelefon – so genannte Smartphones – erhältlich. Durch die technologische Entwicklung wird eine klare Abgrenzung zwischen den einzelnen Typen tragbarer Rechner immer schwieriger.

Durch den mobilen Einsatz der kleinen Rechner entstehen zusätzliche Risiken für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten. Hierzu zählen in erster Linie der Diebstahl und der Verlust sowie die unberechtigte –

auch private – Nutzung. Personenbezogene Daten müssen auf Laptop und PDA mittels kryptographischer Verfahren verschlüsselt werden. Dies gilt auch für die Übertragung solcher Daten über ein Funknetz (WLAN). Eine Orientierungshilfe „Datenschutz in drahtlosen Netzen“ steht auf unserer Website für weitere Informationen zur Verfügung.[23]

Laptops müssen in der öffentlichen Verwaltung zum Einsatz formal freigegeben werden. Dem Freigabeverfahren ist eine spezielle Prüfung auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes zu Grunde zu legen. Darüber hinaus sollte eine Dienstanweisung die Art und den Umfang des Einsatzes mobiler Rechner regeln.

Mobile Rechner dürfen nur eingesetzt werden, wenn bei der Speicherung personenbezogener Daten auch die weiteren Anforderungen des behördlichen Sicherheitskonzeptes umgesetzt werden.

2.13 Sicherung der USB-Schnittstelle

Die USB-Schnittstelle eines jeden Rechners gleicht einem offenen Scheunentor, wenn sie nicht ausreichend gegen unbefugten Zugriff geschützt wird.

Externe Laufwerke und Speichermedien wie z. B. CD-ROM-Laufwerke, USB-Sticks, aber auch DVD-Brenner können über die USB-Schnittstelle (Universal Serial Bus) problemlos selbst im laufenden Betrieb an einem PC angeschlossen werden. Moderne Betriebssysteme erkennen diese Geräte sofort und ermöglichen eine Datenübertragung. Dadurch steigt das Risiko einer unkontrollierten Datenverarbeitung ebenso an wie das einer Manipulation oder Beschädigung der auf dem Rechner vorhandenen Daten oder Programme durch schadhafte Software.

Um die IT-Sicherheit sowie den Schutz personenbezogener Daten zu gewährleisten, ist es daher erforderlich, die USB-Schnittstelle zu sichern. Hierzu kann man die USB-Schnittstelle im BIOS (Basic Input Output System) vollständig deaktivieren oder durch die Änderung der Bootreihenfolge ein Starten des Rechners vom USB-Speicher aus verhindern. Falls der entsprechende Arbeitsplatz jedoch auf die Verwendung eines externen USB-Gerätes angewiesen ist (z. B. Tastatur), können alternativ hierzu die zur Verwaltung unerwünschter Geräte erforderlichen Treiber aus dem System entfernt werden. Bei der Verwendung von Windows kann die Überwachung des Registrierungsschlüssels für USB-Geräte einen wirksamen Schutz darstellen. Darüber

[23] siehe A 2.2

hinaus werden Programme angeboten, mit denen der Datentransfer über die USB-Schnittstelle kontrolliert und protokolliert werden kann.

Allerdings kann der Einsatz externer USB-Speicher auch sinnvoll sein. Insbesondere lassen sich dort sensitive Daten ausschließlich auf einem externen USB-Speicher sichern. Sie können verschlüsselt und der Speicher schließlich beispielsweise in einem Datentresor verschlossen werden.

Sowohl durch Mittel des Betriebssystems als auch mithilfe spezieller Programme kann die USB-Schnittstelle gegen einen unbefugten Zugriff geschützt werden.

2.14 Praxisprobleme bei der Systemadministration

Auf Grund der ständig steigenden Komplexität der IT-Systeme spielen die Systemadministratoren bei der dauerhaften Gewährleistung einer ganzheitlichen IT-Sicherheit eine immer größere Rolle. Einige Beispiele sollen die gestiegenen Anforderungen an diese Aufgabe verdeutlichen.

Auf Grund neuer Technologien und zunehmender Vernetzung ist die Komplexität von IT-Systemen um ein Vielfaches gestiegen. Moderne Betriebssysteme und Anwendungen enthalten immer mehr Funktionalitäten und werden damit nicht weniger fehleranfällig. Selbst unterbrechungsfreie Stromversorgungen beinhalten zur Administration einen integrierten Web-Server und holen sich die aktuelle Systemzeit von einem Zeit-Server im Netz. Der Stand der Technik hat sich in den letzten Jahren rasant weiterentwickelt. So sind z. B. Verschlüsselungsverfahren und Verfahren zur digitalen Signatur zu Standardmaßnahmen zum Schutz personenbezogener Daten geworden. Auch stellen E-Government-Projekte hohe Ansprüche an die zu realisierenden Sicherheitsmaßnahmen. Aus diesen Entwicklungen resultieren natürlich auch höhere Anforderungen an die Systemadministration.

Ein Problem bei der Administration von Servern und Arbeitsplatzcomputern, ist das zeitnahe Einspielen von Service Packs und Sicherheitsupdates. Beispielsweise stehen für Windows XP Service Pack 2 je nach Konfiguration derzeit ca. 48 Updates zur Verfügung. Eine manuelle Installation dieser Updates durch den Systemadministrator ist aus Zeitgründen nahezu unmöglich. Microsoft hat diese Situation erkannt und bietet mit dem Windows Server Update Service[24] (WSUS) eine Patch- und Updateverwaltung für Microsoft-Software an, mit der eine Verteilung der Softwareupdates auf Server und Arbeitsplatzcomputer automatisiert werden kann. Der WSUS-Server lädt dabei die erforderlichen Updates manuell oder zeitgesteuert aus dem Internet und

[24] siehe http://www.microsoft.com/germany/windowsserver2003/technologien/updateservices

speichert diese in einer Datenbank ab. Mit dem WSUS-Server erhält der Systemadministrator die Möglichkeit, die heruntergeladenen Updates erst zu prüfen, bevor ausgewählte Updates für alle Server und Arbeitsplatzcomputer im Netz freigegeben werden. Der Landesbetrieb für Datenverarbeitung und Statistik stellt seit einiger Zeit einen WSUS-Server für alle am Landesverwaltungsnetz angeschlossenen Einrichtungen zur Verfügung. Die öffentlichen Stellen sind aufgefordert, zur Entlastung ihrer Systemadministratoren diese effiziente Variante des Patchmanagements für Microsoft-Software zu nutzen.

Der Einsatz von Virenscannern auf zentralen und dezentralen Systemen hat sich in den letzten Jahren positiv entwickelt. Es haben sich Virenscanner durchgesetzt, die eine zentrale und automatisierte Verwaltung der Systembestandteile ermöglichen und damit die Systemadministratoren entlasten. Moderne Virensuchprogramme können die Updates automatisch auf den Systemen installieren. Man unterscheidet zwischen Programmupdates und Updates der Virensignaturen, die möglichst stündlich automatisiert aktualisiert werden sollten. Schon bei der Auswahl eines geeigneten Virensuchprogramms sollte man prüfen, ob diese Forderungen erfüllt werden.

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Durch eine restriktive Vergabe von Rechten kann für herkömmliche Benutzer der Zugriff auf personenbezogene Daten auf ein erforderliches Maß beschränkt werden. Anders sieht das bei den Systemadministratoren aus. Diese haben standardmäßig Zugriff auf fast alle Daten im System. Einerseits muss ausgeschlossen werden, dass die Administratoren personenbezogene Daten missbräuchlich verwenden können, andererseits sollte aber auch der Schutz des Administrators vor ungerechtfertigten Vorwürfen berücksichtigt werden. Er hat in den wenigsten Fällen die Möglichkeit, einen „Nicht-Zugriff“ auf personenbezogene Daten nachzuweisen. Dies kann jedoch durch eine revisionssichere Protokollierung seiner Aktivitäten gewährleistet werden. Administratoren müssen erkennen, dass es auch in ihrem eigenen Interesse ist, einen Zugriff auf personenbezogene Daten zu beschränken. Der Verschlüsselung personenbezogener Daten kommt deshalb auch hier eine große Bedeutung zu.

Die Behördenleitungen sollten den Administratoren genügend Zeit zur Verfügung stellen, um sich in neue sicherheitsrelevante Technologien einarbeiten zu können. Die Schulung der Administratoren muss bei der Etablierung eines Sicherheitsmanagements eine zentrale Rolle spielen.

2.15 Fernzugriff und Wartung von PCs mit der Software VNC

Ein Personalrat fragte uns, ob die Wartung von Arbeitsplatz-PCs durch Administratoren mithilfe der Software VNC datenschutzgerecht sei.

Die Software VNC (Virtual Network Computing) erlaubt den Fernzugriff auf PCs und deren Fernsteuerung. Hierzu werden Bildschirminhalte sowie Tastatureingaben und Mausbewegungen über das Netzwerk übertragen. Die wesentliche Arbeitserleichterung für Administratoren besteht darin, dass sie ihren Arbeitsplatz während der Wartung nicht mehr verlassen müssen. VNC existiert in verschiedenen Ausprägungen von unterschiedlichen Herstellern, welche die ursprüngliche Version der Firma ATT weiterentwickeln. Auch kostenfreie Angebote sind verfügbar.

§ 11a Brandenburgisches Datenschutzgesetz (BbgDSG) sowie dessen Anlage 1 enthalten Anforderungen, die bei einer datenschutzgerechten Gestaltung von Wartungsprozessen zu berücksichtigen sind. Dazu gehört insbesondere, dass nur autorisiertes Personal die Wartung vornimmt, jeder Wartungsvorgang nur mit Zustimmung der speichernden Stelle erfolgt, alle Wartungsvorgänge während und nach der Wartung kontrolliert werden können sowie keine Programme während der Wartung unbefugt gestartet oder verändert werden. Prinzipiell sollte bei Wartungsarbeiten gar nicht oder nur im unbedingt erforderlichen Umfang auf personenbezogene Daten zugegriffen werden. Eine unbefugte Entfernung oder Übertragung personenbezogener Daten ist auszuschließen.

Grundsätzlich ist VNC bei entsprechender Konfiguration geeignet, die datenschutzrechtlichen Anforderungen für die Wartung zu erfüllen. Voraussetzung ist die strikte Trennung der beiden Teile der Software: Der erste Teil, der VNC Server, sollte nur auf den zu wartenden Mitarbeiter-PCs installiert werden. Er nimmt bei Bedarf Verbindungswünsche des zweiten Teils, des VNC Viewers, entgegen. Dieser Teil ist auf den Administrator-PCs zu installieren. Ein aktiver VNC Server ist unter dem Betriebssystem MS Windows als Symbol in der sog. Task Leiste eingetragen. Besteht eine Verbindung zu einem VNC Viewer und somit die Möglichkeit des Fernzugriffs auf den zu wartenden PC, ändert sich die Farbe dieses Symbols.

Wir empfehlen für die VNC Server auf den Mitarbeiter-PCs die folgenden Einstellungen bei der Konfiguration:

- Administratoren müssen sich bei der Verbindungsaufnahme durch Eingabe eines Passworts authentifizieren,
- die Adressen der PCs, von denen Administratoren Verbindungen aufbauen können, werden fest konfiguriert,

- Mitarbeiter müssen Verbindungswünsche von Administratoren explizit in einem Dialogfenster bestätigen – erfolgt keine Bestätigung, ist kein Fernzugriff möglich,
- Einstellungen des VNC Servers können nur von Administratoren geändert werden.

Während einer Wartung mittels der Software VNC werden alle Bildschirminhalte und Eingaben des Mitarbeiters unverschlüsselt über das Netz an den Administrator übertragen. Diese Weise der Wartung eignet sich daher ausschließlich für Rechner, auf denen nur personenbezogene Daten mit geringer Sensitivität verarbeitet werden. Bei PCs, auf denen beispielsweise Personal- oder Sozialdaten vorhanden sind, darf VNC nicht angewandt werden. Auch müssen alle beteiligten PCs über restriktiv konfigurierte Firewalls geschützt werden. Die Übertragung der Daten über offene Netze wie das Internet ist zu verhindern. Eine Fernwartung durch Dritte, die nicht innerhalb der Daten verarbeitenden Stelle beschäftigt sind, kommt nur in Betracht, wenn überhaupt keine personenbezogenen Daten auf den Rechnern verarbeitet werden.
Wartungsvorgänge sollten anhand eines Wartungsprotokolls nachvollziehbar sein. Nur wenige VNC-Versionen können überhaupt Protokolle erstellen. Eine Sicherung gegen nachträgliche Manipulation der Protokolle bietet keines der uns bekannten Produkte. Deshalb kommt der Kontrolle der Wartungsarbeiten während ihrer Durchführung eine besondere Bedeutung zu. Hier ist der Nutzer gefordert, auf dessen PC zugegriffen wird. Er muss den Verbindungswunsch eines Administrators explizit bestätigen und kann am Bildschirm die Aktivitäten verfolgen sowie notfalls die Verbindung manuell beenden.

Der Einsatz einer Software wie VNC, die den Fernzugriff auf Mitarbeiter-PCs gestattet, ist nach § 65 Personalvertretungsgesetz des Landes Brandenburg mitbestimmungspflichtig. Wir empfehlen deshalb den Abschluss einer entsprechenden Dienstvereinbarung, die neben den oben genannten Punkten zu den technischen Maßnahmen auch eine Regelung enthält, welche die Nutzung von durch Fernzugriff gewonnenen Daten für Zwecke der Leistungs- und Verhaltenskontrolle der Beschäftigten ausschließt.

Gegen die Nutzung der Software VNC für Zwecke der Wartung von PCs und der Nutzerbetreuung bestehen keine Einwände, wenn eine datenschutzgerechte Konfiguration verwendet wird und sich die Aktivitäten auf PCs in lokalen, nach außen abgesicherten Netzen beschränken. Der Abschluss einer Dienstvereinbarung wird empfohlen.

2.16 Digitalfunk BOS

Das Bundesministerium des Innern plant gemeinsam mit den Innenministerien der Länder den Aufbau eines bundesweit einheitlichen digitalen Funknetzes für Polizei, Feuerwehr, Rettungsdienst, Katastrophenkräfte und ähnliche Einrichtungen.

Das neue Digitalfunknetz der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) soll das veraltete analoge Funknetz ablösen. Dieses arbeitet teilweise unzuverlässig und kann durch Unbefugte problemlos abgehört werden. Aus der Vergangenheit sind Fälle bekannt, in denen beispielsweise Reporter und andere Interessierte noch vor der Polizei beim Tatort eintrafen. Eine grundlegende Forderung ist daher der Einsatz von Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit der Kommunikation.

Die technischen und organisatorischen Anforderungen an das neue BOS-Digitalfunknetz werden von Vertretern des Bundes und der Länder gemeinsam erarbeitet. In Projektgruppen sind eine Reihe von Fragen zu klären. Das hiesige Ministerium des Innern bezog uns schon frühzeitig in die Planungen des Funknetzes ein und ermöglichte die Teilnahme an einer Projektgruppensitzung, auf der insbesondere technische Fragen zur Sicherheit des Systems diskutiert wurden.

Die Ausbaudichte der erforderlichen Basisstationen kann von den einzelnen Bundesländern in Abhängigkeit von den Anforderungen der BOS und den zur Verfügung stehenden finanziellen Mitteln selbst bestimmt und in unterschiedlichen Ausbaustufen gestaltet werden. Derzeit werden verschiedene Ansätze diskutiert. Die komfortabelste und teuerste Variante sieht vor, dass man ein zusätzliches Mobilfunknetz ähnlich der bereits vorhandenen öffentlichen Mobilfunknetze errichtet. Damit könnte man eine separate Versorgung der BOS mit Mobiltelefon bis in alle Gebäudeteile hinein erreichen und auch die Funkalarmierung der erforderlichen Einsatzkräfte realisieren.

Bei einer kostengünstigeren Variante wird die Anzahl der Basisstationen gering gehalten. Diese Variante hat den Nachteil, dass in den Einsatzfahrzeugen der BOS leistungsstarke Funkgeräte eingesetzt werden müssten, um die Erreichbarkeit zu gewährleisten. Ein allgemein üblicher Betrieb von Mobiltelefonen wäre dann nur mit speziellen Geräten in einem Umkreis von etwa einigen hundert Metern zum Einsatzfahrzeug möglich. Dabei wird über das Funkgerät im Einsatzfahrzeug die Verbindung zur entfernten Basisstation aufgebaut. Vorerst soll diese Variante des Digitalfunknetzes im Land Brandenburg implementiert werden. Die Alarmierung der Einsatzkräfte erfolgt weiterhin über das bestehende passive System (sog. „Pieper“).

Während das Netz auf Bundesebene einheitlich ausgeschrieben wird, bleibt die Auswahl der Endgeräte den BOS in den einzelnen Ländern überlassen. Man kann davon ausgehen, dass ein breites Spektrum von Geräten zum Einsatz kommen wird.

Es wurde bereits festgelegt, dass die Möglichkeit einer Ende-zu-Ende-Verschlüsselung nach einem vom Bundesamt für Sicherheit und Informationstechnik erstellten Verschlüsselungskonzept gegeben sein muss. Dies ist natürlich nur möglich, wenn bei der Beschaffung darauf geachtet wird, dass die Geräte über die entsprechenden Leistungsmerkmale verfügen. Die verschlüsselte Übertragung von Gesprächsdaten sollte hierbei die Standardeinstellung der Endgeräte sein.

Nach Auffassung der BOS soll unter bestimmten Umständen auch eine unverschlüsselte Kommunikation möglich sein. Beispielsweise könne dies in besonderen taktischen Lagen erforderlich sein, da der Aufbau einer verschlüsselten Verbindung mehrere Sekunden benötigt. Auch ist nach Aussagen der Projektbeteiligten die Kommunikation mit Teilnehmern außerhalb des BOS-Funknetzes nur unverschlüsselt möglich. Das würde für das Land Brandenburg bedeuten, dass man BOS-relevante Dienststellen im Nachbarstaat Polen nur unverschlüsselt erreichen würde. Nach unserer Auffassung sollte dieser Mangel z. B. durch eine Ausrüstung ausgewählter polnischer Leitstellen mit einem BOS-Anschluss behoben werden.

Die bereits jetzt bestehenden Möglichkeiten zur Aufzeichnung von Gesprächsinhalten bei der Polizei und den Rettungsdiensten sollen im BOS-Funknetz nicht erweitert werden.

Durch Einführung eines bundeseinheitlichen digitalen Funknetzes für Behörden und Organisationen mit Sicherheitsaufgaben kann insbesondere die Vertraulichkeit der Kommunikation besser als bisher sichergestellt werden. Wir fordern das Ministerium des Innern auf, sich auch weiterhin für eine Verschlüsselung aller Verbindungen einzusetzen.

2.17 Das JobCard-Verfahren

Im Jahr 2002 hat die Bundesregierung die Einführung des JobCard-Verfahrens beschlossen. Danach erhalten alle Arbeitnehmer eine Signaturkarte, mit deren Hilfe die Arbeitsverwaltungen auf zentral gespeicherte Daten der Arbeitnehmer zugreifen können. Die Datenschutzbeauftragten des Bundes und der Länder haben unter unserer Beteiligung das Projekt datenschutzrechtlich begleitet.

Die Bundesregierung beabsichtigt, mit dem JobCard-Verfahren die Arbeitgeber zu entlasten, die Verwaltungen effizienter zu gestalten und gleichzeitig den Einsatz der Signaturkarte zu fördern. Derzeit stellen die Arbeitgeber jährlich ca. 60 Millionen Bescheinigungen in Papierform aus. Diese Nachweise sollen zukünftig elektronisch an eine zentrale Speicherstelle übertragen und dort gespeichert werden. Bei den elektronischen Bescheinigungen handelt es sich u. a. um Beschäftigungszeiten, Höhe von Entgeltzahlungen sowie Angaben zur Auflösung von Beschäftigungsverhältnissen der Arbeitnehmer.

Das Verfahren soll folgendermaßen ausgestaltet werden: Jeder Arbeitnehmer erhält eine Signaturkarte mit einem qualifizierten Zertifikat nach den Vorschriften des Signaturgesetzes, mit der er sich bei einer Registrierungsstelle zur Teilnahme am JobCard-Verfahren anmelden muss. In einem zentralen Verzeichnisdienst werden die zur Teilnahme am JobCard-Verfahren angemeldeten Signaturkarten registriert.

Wird beispielsweise einem Arbeitnehmer gekündigt und er sucht daraufhin eine Arbeitsagentur auf, um einen Antrag auf Arbeitslosengeld zu stellen, so werden die zur Berechnung benötigten Bescheinigungen von der zentralen Speicherstelle abgerufen. Ein Zugriff auf die in der zentralen Speicherstelle gespeicherten Daten ist nur mit je einer gültigen Signaturkarte des Arbeitnehmers und des Mitarbeiters der Arbeitsagentur möglich. Erst durch Eingabe der persönlichen Identifikationsnummer (PIN) des Arbeitnehmers wird die elektronische Abfrage der Daten initiiert. Liegen die Bescheinigungen des Arbeitgebers noch nicht in der zentralen Speicherstelle vor, so erstellt der Antragsteller mithilfe seiner Signaturkarte eine elektronische Vollmacht, sodass die Daten auch zu einem späteren Zeitpunkt noch vom Mitarbeiter der Arbeitsagentur zur Bearbeitung seines Antrages abgerufen werden können. Das wiederholte Vorsprechen des Antragstellers bei der Arbeitsagentur ist in diesem Fall nicht erforderlich.

Personenbezogene Daten dürfen nur gespeichert werden, wenn der Zweck der Verwendung hinreichend bestimmt ist. Da schon jetzt erkennbar ist, dass nicht alle in der zentralen Speicherstelle abgelegten Bescheinigungen jemals verwendet werden, stellt sich die Frage, ob es sich hierbei um eine unzulässige Vorratsdatenspeicherung handelt.

Aus technisch-organisatorischer Sicht sind in der zentralen Speicherstelle besonders hohe Anforderungen an den Schutz der gespeicherten personenbezogenen Daten zu stellen. Die Bescheinigungen werden von den Arbeitgebern verschlüsselt an die zentrale Speicherstelle übertragen, dann entschlüsselt, mit einem Master-Key wieder verschlüsselt und dann in der zentralen Datenbank abgelegt. In diesem ursprünglichen Konzept hätte die zentrale Speicherstelle Zugriff auf den Schlüssel und die Daten. Ein Missbrauch der

Daten innerhalb der zentralen Speicherstelle könnte so nicht ausgeschlossen werden. Die Datenschutzbeauftragten des Bundes und der Länder schlugen daraufhin eine Lösungsvariante vor, bei der die Daten durchgängig mithilfe der Ende-zu-Ende-Verschlüsselung vor dem Zugriff Dritter geschützt werden. Die Daten werden dabei schon beim Arbeitgeber mit dem öffentlichen Schlüssel des Arbeitnehmers verschlüsselt und erst bei der abrufenden Stelle unter Zuhilfenahme des geheimen Schlüssels des Arbeitnehmers wieder entschlüsselt, wobei sich beide Schlüssel auf der Signaturkarte des Arbeitnehmers befinden und der geheime Schlüssel nur durch Eingabe der PIN freigeschaltet werden kann. Die so verschlüsselten Bescheinigungen wären in der zentralen Speicherstelle nach dem heutigen Stand der Technik vor einem unberechtigten Zugriff sicher. Die vorgeschlagene Lösungsvariante wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als technisch möglich aber als zu aufwändig bewertet. Daraufhin wurde dieser Lösungsvorschlag wieder fallen gelassen. Derzeit ist in der Diskussion, die Module zur Ver- und Entschlüsselung der Bescheinigungsdaten einer unabhängigen Instanz zu unterstellen. Damit wäre ein Missbrauch bzw. eine Zweckentfremdung der Bescheinigungsdaten innerhalb der zentralen Speicherstelle nicht mehr möglich.

Die in der zentralen Speicherstelle abgelegten Bescheinigungsdaten der Arbeitnehmer sind durch technisch-organisatorische Maßnahmen so zu sichern, dass eine unbefugte Nutzung dieser Daten ausgeschlossen ist.

2.18 Einführung der elektronischen Gesundheitskarte

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung wurde die Einführung einer elektronischen Gesundheitskarte festgeschrieben. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind u. a. rechtliche und technisch-organisatorische Voraussetzungen zu schaffen, die das Patientengeheimnis wahren.

Die Einführung der elektronischen Gesundheitskarte ist ab 1. Januar 2006 vorgesehen. Aufbauend auf den Erfahrungen mit der bisherigen Krankenversichertenkarte soll durch den Einsatz moderner Informationstechnologien im Gesundheitswesen die Qualität der medizinischen Versorgung und gleichzeitig die Wirtschaftlichkeit verbessert werden. Auf Grund der Komplexität des gesamten Verfahrens wird eine flächendeckende Einführung jedoch zu einem späteren Zeitpunkt erfolgen. Derzeit wurde damit begonnen, in ausgewählten Regionen die elektronische Gesundheitskarte zu testen.

Die elektronische Gesundheitskarte wird die bisherige Krankenversichertenkarte ersetzen. Sie wird sowohl administrative Funktionen enthalten als auch medizinische Daten verfügbar machen. Der administrative Teil der Gesund-

heitskarte wird auch als Pflichtteil bezeichnet und enthält Angaben über den Versicherten, ermöglicht die Ausstellung eines elektronischen Rezepts und berechtigt zu einer Behandlung im europäischen Ausland.

Neben dem Pflichtteil wird die elektronische Gesundheitskarte auch einen Zugriff auf medizinische Daten ermöglichen. Die Nutzung des medizinischen Teils der elektronischen Gesundheitskarte ist für die Versicherten freiwillig. Nach dem derzeitigen Stand soll der medizinische Teil folgende Daten bzw. Anwendungen enthalten:

- Arzneimitteldokumentation,
- Notfallinformationen (z. B. Blutgruppe, Allergien, Impfungen und Röntgenuntersuchungen),
- elektronische Patientenakte (EPA),
- elektronischer Arztbrief,
- Informationen über die vom Arzt erbrachten Leistungen und deren Kosten und
- von den Patienten selbst gespeicherte Informationen (z. B. Verlaufsprotokolle und Patientenverfügungen).

Ob die medizinischen Daten direkt auf der Gesundheitskarte oder auf einem zentralen Serversystem gespeichert werden, ist noch nicht endgültig entschieden worden. Im Falle einer zentralen Speicherung der medizinischen Daten enthielte die Gesundheitskarte nur die entsprechenden Verweise.

Ein Zugriff auf den Großteil der auf der elektronischen Gesundheitskarte gespeicherten Daten und Anwendungen ist nur in Verbindung mit einem elektronischen Heilberufsausweis möglich, den z. B. Ärzte und Apotheker erhalten. Ein Arzt kann z. B. ein elektronisches Rezept auf der Gesundheitskarte hinterlegen und ein Apotheker dieses wieder auslesen. Der Patient erhält die Möglichkeit, an Terminals, die z. B. in den Apotheken untergebracht werden könnten, bestimmte Rezepte, die auf der Gesundheitskarte abgelegt wurden, zu sperren oder frei zugeben. Damit kann er entscheiden, welcher Apotheker welches Rezept lesen kann.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich schon frühzeitig mit den aus der Einführung einer elektronischen Gesundheitskarte resultierenden datenschutzrechtlichen und technischen Fragestellungen beschäftigt. So wurden zum Thema „Chipkarten im Gesundheitswesen“ auf der 47.[25] und 50.[26] Konferenz und zum Thema „Elektronische Gesundheitskarte“ auf der 69.[27] Konferenz der Datenschutzbeauftragten grundsätzliche daten-

[25] http://www.lda.brandenburg.de/sixcms/detail.php?gsid=5lbm1.c.77049.de&template=lda_entschl
[26] http://www.lda.brandenburg.de/sixcms/detail.php?gsid=5lbm1.c.79078.de&template=lda_entschl
[27] http://www.lda.brandenburg.de/sixcms/detail.php?gsid=lbm1.c.219114.de&template=lda_entschl

schutzrechtliche Forderungen formuliert. Weiterhin begleitet eine Unterarbeitsgruppe „Elektronische Gesundheitskarte“ der Arbeitskreise „Technik“ und „Arbeit und Soziales“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die aktuellen Entwicklungen und nimmt Einfluss auf die datenschutzgerechte Ausgestaltung der elektronischen Gesundheitskarte.

Bei der Einführung der elektronischen Gesundheitskarte müssen die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten gewahrt bleiben. Durch umfangreiche technisch-organisatorische Maßnahmen ist der Schutz der besonders sensitiven Patientendaten zu garantieren.

3 Medien und Telekommunikation

3.1 Rundfunk

3.1.1 Datenschutzrechtliche Prüfung bei der Gebühreneinzugszentrale (GEZ)

Angesichts einer steigenden Zahl von Bürgerbeschwerden haben die Landesdatenschutzbeauftragten von Hessen, Bremen, Berlin und Brandenburg eine datenschutzrechtliche Prüfung bei der Gebühreneinzugszentrale (GEZ) durchgeführt.

Die GEZ hat in erster Linie die Funktion eines Rechenzentrums, das die Rundfunkanstalten bei der gesamten Abwicklung des Einzugs der Rundfunkgebühren unterstützt. Sie verarbeitet dabei die Daten von bundesweit rund 40 Millionen Rundfunkteilnehmern. Die GEZ ist aber keine selbstständige Behörde, sie wird vielmehr für die Landesrundfunkanstalten tätig, in deren Auftrag sie auch die personenbezogenen Daten verarbeitet. In Berlin und Brandenburg handelt sie im Auftrag des Rundfunks Berlin-Brandenburg (RBB).

Grundsätzlich konnte festgestellt werden, dass die GEZ dem Datenschutz und der Datensicherheit eine hohe Bedeutung beimisst. Die Zugriffsberechtigungen für einzelne Mitarbeiter und Verfahren bei der Verarbeitung personenbezogener Daten sind aus unserer Sicht aber noch nicht optimal ausgestaltet. So ist die Sachbearbeitung bei der GEZ in der Weise organisiert, dass grundsätzlich keine Differenzierung nach örtlichen oder sachlichen Kriterien vorgenommen wird. Dies hat zur Folge, dass die Sachbearbeiter technisch einen bundesweiten Zugriff auf alle Teilnehmerkonten haben. Eine Beschränkung der Zugriffsrechte würde eine komplette Neuordnung der Organisationsstruktur der GEZ voraussetzen. Hier gilt es, gemeinsam mit den Rund-

funkanstalten und der GEZ an Lösungen zu arbeiten, die künftig ein differenzierteres Zugriffskonzept ermöglichen, ohne dabei die Effizienzvorteile eines gemeinsamen Rechenzentrums aufzuheben.

Datenschutzrechtlich problematisch ist der Umfang, in dem die als Außendienstmitarbeiter tätigen Rundfunkgebührenbeauftragten auf den Datenbestand der GEZ zugreifen können. Auch diese haben einen bundesweiten Online-Zugriff auf alle Teilnehmerkonten, obwohl sich ihre Zuständigkeit nur auf bestimmte Gebiete innerhalb des Sendegebiets einer einzigen Rundfunkanstalt beschränkt. Eine Erforderlichkeit des bundesweiten Zugriffs ist nicht gegeben.

Die GEZ hat für die Löschung personenbezogener Daten ein datenschutzgerechtes Löschungskonzept entwickelt. Bei der Prüfung sind allerdings an dessen praktischer Umsetzung in einigen Punkten Zweifel aufgetreten. Personenbezogene Daten, die zur Aufgabenerfüllung nicht mehr erforderlich sind, müssen gelöscht werden. Ungeachtet dessen hatten einzelne Sachbearbeiter Zugriff auf frühere Wohnanschriften und Kontoverbindungen oder auf vor langer Zeit gewährte Befreiungen von der Gebührenpflicht einschließlich des Befreiungsgrundes.

Geprüft wurde erneut die Verarbeitung personenbezogener Daten im Zusammenhang mit den sog. Mailing-Aktionen der GEZ. Zu diesem Zweck mietet sie gezielt Adressbestände von kommerziellen Adresshändlern an. Es handelt sich dabei um Adressen solcher Personen, bei denen ein besonders hoher Anteil an Schwarzsehern und -hörern vermutet wird, wie z. B. Abonnenten von Fernsehzeitschriften oder des PayTV, Teilnehmern an Gewinnspielen von Rundfunksendern oder Kunden bestimmter E-Mail-Anbieter. Diese Personen werden angeschrieben und aufgefordert, ihre Geräte anzumelden. Die beschriebene Praxis ist nach dem geltenden Recht nach wie vor unzulässig. RBB und GEZ sind hier allerdings anderer Ansicht und setzen die Mailing-Aktion unverändert fort. Der Arbeitskreis Medien der Datenschutzbeauftragten in Bund und Ländern hat – unterstützt durch einige Datenschutzbeauftragte der Rundfunkanstalten – den Rundfunkreferenten der Länder Vorschläge zur Änderung des Rundfunkgebührenstaatsvertrages unterbreitet, die für mehr Rechtsklarheit sorgen sollen.

Datenschutzrechtlich nicht zu beanstanden ist hingegen, dass die GEZ bei Umzügen oder beim Tod eines Einwohners von den Meldebehörden automatisch bestimmte Daten übermittelt bekommt. In Brandenburg erhält sie z. B. Namen und Vornamen, die neue und alte Anschrift und das Geburtsdatum frühestens zwei Monate nach dem Umzug.

Angesichts häufiger Beschwerden über den Inhalt der von der GEZ versandten Formschreiben, haben wir sämtliche Muster dieser Schreiben aus datenschutzrechtlicher Sicht geprüft. Wir haben dabei festgestellt, dass in zahlreichen dieser Schreiben den Empfängern unter Androhung von Maßnahmen des Verwaltungszwangs eine Pflicht zur Beantwortung der Schreiben auch dann suggeriert wird, wenn eine solche Pflicht nicht besteht. Hier haben wir dem RBB entsprechende Änderungen empfohlen.

Die vergleichsweise hohe Zahl von Beschwerden, aber auch der außergewöhnliche Umfang der bundesweiten Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einzug der Rundfunkgebühren, erfordern eine regelmäßige Prüfung der Einhaltung des Datenschutzes in diesem Bereich. Bei den anstehenden Modernisierungen der Datenverarbeitungstechnik in der GEZ sehen wir zudem eine Chance zur Überarbeitung von Datenzugriffskonzepten und hoffen auch auf die weitere fruchtbare Zusammenarbeit mit den Datenschutzbeauftragten von RBB und GEZ.

3.1.2 Überflüssige Datensammlung bei der Rundfunkgebührenbefreiung

Mit der Erhöhung der Rundfunkgebühren am 1. April 2005 hat sich auch das Verfahren über die Befreiung von der Rundfunkgebühr geändert. Es ist seitdem nicht nur erheblich bürokratischer geworden, sondern hat sich auch aus datenschutzrechtlicher Sicht wesentlich verschlechtert.

Anders als bisher entscheiden über Anträge auf Befreiung von der Rundfunkgebühr nicht mehr die Sozialämter, sondern die Rundfunkanstalten selbst, hier der Rundfunk Berlin-Brandenburg (RBB). Diese haben weit gehend die Gebühreneinzugszentrale (GEZ) mit der Durchführung des Verfahrens beauftragt.

Von der Rundfunkgebührenpflicht werden in der Regel nur noch Empfänger bestimmter Sozialleistungen wie z. B. Sozialhilfe, Arbeitslosengeld II oder BAföG bzw. wie bisher Menschen mit bestimmten Behinderungen befreit. Die Bezieher von Sozialleistungen müssen ihrem Antrag den vollständigen Sozialleistungsbescheid einschließlich etwaiger Berechnungsbögen bzw. beglaubigte Kopien davon beifügen. Andere Antragsteller müssen mit der Vorlage des Schwerbehindertenausweises ihre Berechtigung nachweisen. Die GEZ erhält auf diese Weise Kenntnis von einer Vielzahl zum Teil sensitiver personenbezogener Daten. Sie benötigt aber weder Angaben über Bankverbindungen, die Krankenkassenzugehörigkeit, die Größe und Kosten des Wohnraums, noch Informationen über die soziale Situation der Angehörigen des Antragstellers.

Erforderliche Daten sind in der Regel lediglich die Angaben über die Behörde, die den Sozialleistungsbescheid ausgestellt hat, die Identität des Antragstellers, den Bewilligungszeitraum und die Art der bewilligten Leistung sowie in Abhängigkeit vom konkreten Befreiungsgrund wenige weitere Angaben. Der RBB hat bisher nicht überzeugend begründen können, zu welchen Zwecken die zahlreichen Informationen erforderlich sein sollen.

Hinzu kommt, dass die GEZ die Kopien der ihr zugegangenen Bescheide vollständig scannt und im jeweiligen Datensatz des Rundfunkteilnehmers speichert. Dies ist auch nach der neuen Rechtslage[28] unzulässig, da die Mehrzahl der Daten zum einen überhaupt nicht gebraucht wird und zum anderen der Rundfunkgebührenstaatsvertrag nur die Vorlage der Bescheide, nicht aber deren Speicherung verlangt. Die GEZ ist vielmehr verpflichtet, unmittelbar nach Prüfung der Voraussetzungen alle nicht erforderlichen Daten vor der Speicherung zu schwärzen oder nach Übernahme der erforderlichen Daten die Bescheide an die Antragsteller zurückzusenden bzw. Kopien zu vernichten.

Wir haben den Betroffenen deshalb empfohlen, die Rücksendung oder Vernichtung ihrer Kopie zu verlangen und die GEZ aufzufordern, nur die für die Befreiung unmittelbar erforderlichen Daten zu speichern. Rechtlich halten wir es auch für zulässig, dass die Antragsteller selbst die nicht erforderlichen Daten schwärzen, soweit sie der GEZ keine Originalbescheide oder beglaubigte Kopien zusenden. Dies wird von der GEZ allerdings nicht akzeptiert.

Als Ausweg haben wir dem RBB vorgeschlagen, auf dem Antragsformular zur Rundfunkgebührenbefreiung die Möglichkeit vorzusehen, die für die Befreiung erforderlichen Daten aus den Nachweisen einzutragen und durch die jeweilige Sozialbehörde (z. B. Sozialamt, Jobcenter, Amt für Ausbildungsförderung oder Versorgungsamt) durch Stempel und Unterschrift bestätigen zu lassen.

Die von uns vorgeschlagene Bestätigung durch die jeweilige Behörde hätte den gleichen Wert wie eine beglaubigte Kopie und würde die Zusendung der Kopien von Bescheiden, Ausweisen oder Berechnungsbögen überflüssig machen. Ein solches Verfahren wäre erheblich datenschutzfreundlicher und auch unbürokratischer, da Rundfunkanstalten und GEZ von vornherein nur die tatsächlich erforderlichen Daten erhalten würden und die GEZ mit erheblich weniger Papier umzugehen hätte. Die unzulässige Speicherung von nicht benötigten Daten infolge des Einscannens der vollständigen Bescheide entfiele.

[28] Achter Rundfunkänderungsstaatsvertrag vom 15. Oktober 2004, Gesetz vom 17. März 2005, GVBl. I 2005, S. 114 ff.

Unsere Vorschläge wurden von der Datenschutzbeauftragten des RBB zwar wohlwollend aufgenommen. Es besteht allerdings wenig Spielraum, das Verfahren zu ändern, da insbesondere die Sozialbehörden und kommunalen Spitzenverbände es aus Kostengründen ablehnen, Bescheinigungen anderer Stellen zu bearbeiten.

Die Datenschutzbeauftragten in den Ländern setzen sich daher gemeinsam gegenüber ihren Landesregierungen für eine entsprechende Änderung des Rundfunkgebührenstaatsvertrages ein.

Bei der Bearbeitung der Anträge auf Befreiung von den Rundfunkgebühren werden eine Vielzahl von Daten verarbeitet, die für die Beurteilung der Gebührenbefreiungstatbestände nicht erforderlich sind. Die Staatskanzlei des Landes Brandenburg wird gebeten, die gemeinsam von den Datenschutzbeauftragten des Bundes und der Länder mitgetragenen Vorschläge für ein datenschutzgerechtes Verfahren bei der Befreiung von der Rundfunkgebührenpflicht in den Staatsvertragsverhandlungen mit den anderen Ländern zu unterstützen.

3.2 Internet und Telekommunikation

3.2.1 Vorratsdatenspeicherung in der elektronischen Kommunikation

Nachdem der deutsche Gesetzgeber nicht zuletzt wegen datenschutzrechtlicher und verfassungsrechtlicher Bedenken bewusst davon Abstand genommen hatte, in das neue Telekommunikationsgesetz eine Pflicht zur Vorratsdatenspeicherung aufzunehmen, wird auf der Ebene der Europäischen Union eine solche Verpflichtung für alle Mitgliedsstaaten verbindlich vorgesehen.

Das Europäische Parlament hat Ende Dezember 2005 dem Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation zugestimmt. Danach sollen alle Anbieter elektronischer Kommunikation verpflichtet werden, eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang zwischen sechs Monaten (Internet) und einem Jahr (Telekommunikation) selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) nicht benötigen. Zweck dieser umfassenden Speicherung soll es sein, die Daten für mögliche Abrufe von Sicherheitsbehörden zur Verfügung zu stellen.

Diese Verpflichtung würde auch für alle öffentlichen Stellen des Landes Brandenburg gelten, soweit sie ihren Bediensteten die private Nutzung von Telekommunikation, E-Mail oder anderen Internetdiensten gestatten.

Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner, sondern auch Zeitpunkt und Dauer jeder Einwahl ins Internet, die dabei zugeteilte IP-Adresse, die Verkehrsdaten jeder einzelnen E-Mail und SMS sowie die Standorte der Handy-Nutzer. Damit ließen sich europaweite Bewegungs- und Nutzerprofile für einen Großteil der Bevölkerung erstellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben dieses Vorhaben in einer Entschließung als unverhältnismäßigen Eingriff in die durch das Grundgesetz und die Europäische Menschenrechtskonvention garantierten Grundrechte abgelehnt.[29] Es würde auch gegen die brandenburgische Landesverfassung verstoßen. Bisher hat niemand überzeugend begründen können, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig ist und zu einer effektiveren Strafverfolgung überhaupt beitragen würde.

Die Datenschutzbeauftragten kritisieren, dass alternative Regelungsansätze wie das anlassbezogene Vorhalten von Verkehrsdaten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) bisher nicht ernsthaft erwogen worden sind.

Wie die Erfahrungen der Vergangenheit zeigen, wecken vorhandene Datenbestände Begehrlichkeiten. Trotz aller gegenteiligen Beteuerungen droht eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten, wobei schon jetzt etwa bei der Internetnutzung nicht mehr eindeutig zwischen Verkehrs- und Inhaltsdaten zu trennen ist.

Die langfristige, anlassunabhängige Speicherung von Verkehrsdaten im Bereich der elektronischen Kommunikation bedeutet einen erheblichen Eingriff in die Grundrechte der Bürger, ohne dass daraus ein Gewinn an Sicherheit folgt.
Wir fordern die Landesregierung auf, sich gegenüber der Bundesregierung und im Bundesrat dafür einzusetzen, um die in Deutschland verfassungsrechtlich höchst bedenkliche Verpflichtung zur Vorratsdatenspeicherung in der elektronischen Kommunikation im Rahmen der vom europäischen Recht vorgesehenen Spielräume möglichst datenschutzfreundlich umzusetzen.

[29] siehe Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 3

3.2.2 Fortentwicklung des Medienrechts

Im Berichtszeitraum haben Bund und Länder die Arbeiten an der Fortentwicklung des nationalen Multimediarechts weitergeführt. Die bisherigen gesetzlichen Regelungen sollen vereinheitlicht werden, ohne dabei das bisherige hohe Datenschutzniveau aufzugeben.

Nach wie vor ist das für die elektronische Kommunikation geltende Datenschutzrecht durch eine starke Zersplitterung gekennzeichnet. So gelten für Telekommunikationsdienste, Teledienste und Mediendienste unterschiedliche Datenschutzbestimmungen und Aufsichtszuständigkeiten, obwohl eine Abgrenzung zwischen diesen einzelnen Diensten in der Praxis immer weniger möglich ist. Seit Jahren ist beispielsweise umstritten, ob Internet-Zugangsanbieter (Access Provider) oder E-Mail-Anbieter Teledienste oder Telekommunikationsdienste erbringen. Bei neueren Angeboten wie dem Telefonieren über das Internet (Voice over IP)[30] ist die Grenze zwischen beiden Diensten noch schwerer zu ziehen. Nahezu unmöglich ist eine sinnvolle Abgrenzung zwischen Telediensten, für die das Teledienstedatenschutzgesetz (TDDSG) gilt und Mediendiensten, bei denen sich der Datenschutz nach dem Mediendienste-Staatsvertrag (MDStV) richtet.

Bund und Länder sind daher übereingekommen, die Unterscheidung zwischen Mediendiensten und Telediensten aufzugeben. Die Vorschriften des Teledienste- und des Teledienstedatenschutzgesetzes sowie des Mediendienste-Staatsvertrages sollen durch ein einheitliches Telemediengesetz ersetzt werden, welches sich bereits im Entwurfsstadium befindet. Die in der Gesetzgebungskompetenz der Länder liegenden Bereiche sollen im Rundfunkstaatsvertrag ergänzt werden, der hinsichtlich der datenschutzrechtlichen Bestimmungen wiederum auf das Telemediengesetz verweisen soll. Letzteres wird in Zukunft sowohl für die Internetauftritte öffentlicher Stellen in Brandenburg als auch für die private Nutzung von Internetdiensten am Arbeitsplatz gelten. Damit bestehen für sie die gleichen hohen Datenschutzanforderungen wie für private Provider.

Die Schaffung eines einheitlichen Rechtsrahmens für alle elektronischen Informations- und Kommunikationsdienste ist ein erster Schritt. Ihm muss auf Dauer ein einheitliches Datenschutzrecht für den gesamten Bereich der elektronischen Kommunikation folgen, das insbesondere die unübersichtlichen Aufsichtszuständigkeiten klarer zu regeln hat.

Erfreulich ist, dass das hohe Datenschutzniveau im Multimediabereich beibehalten werden soll. So sollen auch künftig für die Verarbeitung von Bestands- und Nutzungsdaten das Erforderlichkeitsprinzip und eine strenge Zweckbin-

[30] siehe A 2.3

dung gelten. Personenbezogene Nutzungsdaten (insbesondere IP-Adressen) müssen nach den Entwürfen weiterhin mit Ende des Nutzungsvorganges gelöscht werden, wenn sie nicht zu Abrechnungszwecken erforderlich sind. Die Entwürfe enthalten zwar erweiterte Öffnungsklauseln zu Gunsten von Strafverfolgungsbehörden, Geheimdiensten oder Inhabern von Urheberrechten, diese führen aber nicht zu neuen Befugnissen. Nach wie vor sollen die berechtigten Stellen nur dann Bestands- oder Nutzungsdaten erhalten können, wenn die für sie jeweils maßgeblichen Bestimmungen (z. B. Strafprozessordnung, Verfassungsschutzgesetz oder Urheberrechtsgesetz) selbst eine Erhebung solcher Daten erlauben.

Die Vereinheitlichung und Zusammenfassung der die elektronischen Medien betreffenden rechtlichen Vorschriften ist geeignet, Unklarheiten darüber zu beseitigen, ob ein bestimmtes technisches Medium unter eine Vorschrift fällt oder welche Aufsichtsbehörde anzusprechen ist. Die Einhaltung eines hohen Datenschutzniveaus in der elektronischen Kommunikation ist dabei eine notwendige Voraussetzung für das Vertrauen der Bürger bei der Nutzung dieser Medien.

3.2.3 Neues Telekommunikationsrecht gilt auch für öffentliche Stellen

Im Juni 2004 ist das neue Telekommunikationsgesetz (TKG)[31] in Kraft getreten. Dessen Datenschutzbestimmungen gelten zum Teil auch für öffentliche Stellen in Brandenburg.

Das Telekommunikationsgesetz gilt für alle geschäftsmäßigen Anbieter von Telekommunikationsdiensten. Dazu gehören auch die öffentlichen Stellen in Brandenburg, soweit sie ihren Beschäftigten die private Nutzung der Telekommunikationseinrichtungen erlauben. Dies gilt nicht für die dienstliche Kommunikation.

Die Datenschutzvorschriften des Telekommunikationsgesetzes bestimmen, dass die öffentlichen Stellen das Fernmeldegeheimnis bei privater Nutzung beachten müssen, welches neben den eigentlichen Gesprächsinhalten auch die Verkehrsdaten schützt. Die Verkehrsdaten sind unverzüglich nach Verbindungsende zu löschen, es sei denn, sie werden zu Abrechnungszwecken oder zur Erstellung von Einzelverbindungsnachweisen benötigt. Dann dürfen sie bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Zwar ist die Speicherung vollständiger Zielrufnummern zulässig, wir empfehlen jedoch, die Zielrufnummern lediglich verkürzt um die letzten drei Ziffern zu speichern. Das reicht für Abrechnungszwecke aus und ist gleichzei-

[31] BGBl. I 2004, S. 1190 ff.

tig geeignet, die Interessen Dritter zu wahren, die nun nicht mehr anhand der vollständigen Nummern zu identifizieren sind. Generell ist anzuraten, die Verarbeitung von Verkehrsdaten sowohl bei der dienstlichen als auch bei der privaten Kommunikation in einer Dienstvereinbarung zu regeln.

Die Mehrzahl der Landesbehörden hat darüber hinaus die Dienstanschlussvorschrift des Ministeriums der Finanzen zu beachten, die teilweise ein strengeres Datenschutzniveau vorsieht, als das Telekommunikationsgesetz selbst. Die neue Dienstanschlussvorschrift (DAV) wurde vom Ministerium der Finanzen am 16. Februar 2005 erlassen.[32] Sie ist mit wenigen Ausnahmen verbindlich für die gesamte Landesverwaltung einschließlich der staatlichen Hochschulen. Sie regelt vor allem den Umgang mit Verbindungsdaten dienstlicher und privater Telefongespräche der Bediensteten. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wurde bei der Novellierung der Verwaltungsvorschrift frühzeitig eingebunden.

Im Gegensatz zu anderen Anbietern müssen die öffentlichen Stellen keine Schnittstellen für die Überwachung einrichten. Ebenso wenig sind sie verpflichtet, ihre Bestandsdaten zum automatisierten Abruf durch Sicherheitsbehörden vorzuhalten. Im Einzelfall müssen sie bestimmten Sicherheitsbehörden nach § 113 TKG jedoch Auskünfte erteilen.

Gestatten öffentliche Stellen ihren Bediensteten die private Nutzung der Telekommunikation, müssen sie das Fernmeldegeheimnis beachten und unterliegen den Datenschutzvorschriften des Telekommunikationsgesetzes. Landesbehörden haben außerdem vorrangig die Dienstanschlussvorschriften zu beachten.

4 Datenschutz und E-Government – eine ständige Herausforderung

Im August 2004 hat die Landesregierung einen „Masterplan eGovernment“ und einen „Aktionsplan eGovernment“ verabschiedet, um die entsprechenden Aktivitäten des Landes zu bündeln.

Der Masterplan definiert 35 so genannte Leitprojekte, denen die Landesregierung eine besondere Priorität einräumt. Zu den Leitprojekten gehören Infrastrukturmaßnahmen (z. B. das elektronische Grundbuch oder die automatisierte Liegenschaftskarte), Basiskomponenten (wie z. B. das Brandenburger

[32] Allgemeine Verwaltungsvorschrift über die Einrichtung und Nutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg (Dienstanschlussvorschrift – DAV) vom 16. Februar 2005, ABl. 2005, S. 434

Online Amt – BOA – als integriertes Verwaltungsportal von Land und Kommunen oder behördenübergreifende Dokumentenmanagementsysteme) und einzelne Fachanwendungen (z. B. das Projekt Meldedaten-Online). Letztere sollen dabei im Rahmen der einheitlichen Strategie gemeinsam Basiskomponenten nutzen. So soll das Online-Angebot der Meldebehörden beispielsweise in Zukunft in BOA zur Verfügung stehen.

Bei der datenschutzrechtlichen Einschätzung der einzelnen Projekte hat sich gezeigt, dass einzelne Bestimmungen des Brandenburgischen Datenschutzgesetzes (z. B. die sehr restriktiven Regeln zum automatisierten Abruf personenbezogener Daten) nicht mehr zeitgemäß sind und einer modernen Verwaltung eher im Wege stehen. Hier gilt es zukunftsfähige Lösungen zu entwickeln.

Im Allgemeinen ermöglichen die technikneutral formulierten datenschutzrechtlichen Bestimmungen jedoch eine rechtssichere Umsetzung von E-Government-Projekten. Besonderer Wert ist auf die Gewährleistung eines hohen Maßes an Datensicherheit durch entsprechende technische und organisatorische Maßnahmen zu legen. Der Einsatz von Verschlüsselungsverfahren zur Wahrung der Vertraulichkeit oder von Signaturverfahren zur Gewährleistung von Authentizität und Integrität der Daten sollte selbstverständlich sein. Die Realisierung neuer Anwendungen setzt in der Regel eine umfassende Risikoanalyse und ggf. die Erstellung eines Sicherheitskonzeptes voraus. Diese Einsicht hat sich noch nicht in allen Verwaltungen durchgesetzt.

Bei der datenschutzrechtlichen Beratung einzelner Projekte ist derzeit das Projekt Meldedaten-Online beispielhaft hervorzuheben, das vom Ministerium des Innern geleitet wird. Die Landesbeauftragte ist hier an der Projektgruppe zur Einführung des Online-Meldewesens beteiligt. Ab 1. Januar 2007 soll bei Umzügen die Abmeldung bei der bisherigen Meldebehörde durch eine automatisierte Rückmeldung von der Zuzugsmeldebehörde ersetzt werden.

Für den sicheren Austausch der Meldedaten wird das in Bremen entwickelte, standardisierte Übertragungsprotokoll OSCI-Transport[33] verwendet, die Datensatzstruktur folgt den bundesweit einheitlichen Festlegungen von OSCI XMeld. Da wegen der fehlenden Standardisierung der kommunalen IT-Landschaft eine direkte, sichere Kommunikation mit den über 5.000 Meldebehörden im übrigen Bundesgebiet nicht möglich ist, wird das Land Brandenburg (ähnlich wie andere Bundesländer auch) eine zentrale sog. „Clearingstelle“ einrichten, über die der Datenaustausch abgewickelt wird. Aus Sicht des Datenschutzes sollte dies jedoch nur eine Zwischenlösung sein und die direkte Unterstützung der OSCI-Standards sowie der entsprechenden Schnittstellen in allen ca. 200 Meldebehörden Brandenburgs angestrebt wer-

[33] OSCI = Online Services Computer Interface, siehe http://www.osci.de

den. Diese Forderung wurde von den Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung hervorgehoben.[34]

Zusätzlich ist im Projekt Meldedaten-Online geplant, bei einer zentralen Stelle einen gespiegelten Auskunfts- und Informationsdatenbestand aller Meldebehörden zu speichern, der – über das Portal des Brandenburger Online Amts – die Übermittlung von Meldedaten an andere Behörden und die einfache Melderegisterauskunft an Private erheblich erleichtern soll. Die zentrale Stelle soll hier im Rahmen einer Datenverarbeitung im Auftrag eingebunden werden. Hier ist aus datenschutzrechtlicher Sicht darauf zu achten, dass die einzelnen Meldebehörden entsprechend den Vorgaben des Brandenburgischen Meldegesetzes für ihre jeweiligen Melderegister allein verantwortlich bleiben und die Trennung der Melderegister durch entsprechende technische und organisatorische Maßnahmen aufrechterhalten wird, um der Gefahr eines unzulässigen zentralen landesweiten Melderegisters zu begegnen.

Neben der Beratung der öffentlichen Stellen im Land haben die Datenschutzbeauftragten in Bund und Ländern die Zusammenarbeit bei der datenschutzgerechten Einführung von E-Government intensiviert, um bundesweit möglichst einheitliche datenschutzrechtliche Anforderungen zu formulieren. Hierfür wurde unter Leitung des Landesbeauftragten für den Datenschutz Niedersachsen ein Arbeitskreis eingerichtet. Im Vordergrund stehen dabei einerseits die allgemeinen datenschutzrechtlichen Anforderungen an Infrastrukturen und Basiskomponenten und andererseits die konkreten datenschutzrechtlichen Anforderungen an länderübergreifende Fachanwendungen wie z. B. Meldedaten-Online.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird die datenschutzgerechte Einführung von E-Government in Brandenburg weiterhin aktiv begleiten und steht den öffentlichen Stellen des Landes beratend zur Verfügung.

5 Inneres

5.1 Polizei- und Ordnungsbehörden

5.1.1 Neuregelung der DNA-Analyse

Mit der Änderung der Strafprozessordnung ist für die Durchführung einer DNA-Analyse in vielen Fällen keine richterliche Anordnung mehr erforderlich. Teilweise entfällt der Richtervorbehalt bereits beim Beschaffen

[34] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2005, A I 4

der zu analysierenden Proben, wenn in ihre Entnahme eingewilligt wurde.

Die Strafprozessordnung (StPO) unterscheidet zwischen der Beschaffung einer DNA-Probe durch körperlichen Eingriff beim Betroffenen und ihrer Untersuchung. Die Probe wird im Regelfall durch die Entnahme einer Blut- oder Speichelprobe gewonnen. Gegen den Willen des Betroffenen ist das nach § 81a StPO wie bisher grundsätzlich nur mit richterlicher Genehmigung möglich.

Die Änderungen der Strafprozessordnung beziehen sich vor allem auf die weitere Verwendung und Auswertung der einmal gewonnenen Proben. Nunmehr kann nach § 81f StPO ihre molekulargenetische Untersuchung auch mit schriftlicher Einwilligung des Betroffenen erfolgen. Im Rahmen eines laufenden Ermittlungsverfahrens bei Gefahr im Verzug kann sie ohne die Einwilligung des Betroffenen sogar auf Grund einer Anordnung der Staatsanwaltschaft erfolgen, obwohl kein Richter damit befasst war.

Eine Einwilligung ist nur rechtswirksam, wenn sie freiwillig und ohne Druck erfolgt. Daher halten wir es gerade in Strafermittlungsverfahren für problematisch, wenn eine Einwilligung eine richterliche Entscheidung ersetzen soll. Es besteht die Gefahr, dass das Recht von Verdächtigen, sich nicht selbst zu belasten, ausgehöhlt wird. Nicht nachvollziehbar ist zudem die Erforderlichkeit der Einführung einer Eilkompetenz für die Staatsanwaltschaft. Ein auf wissenschaftliche Erhebungen gestützter Nachweis, dass die Notwendigkeit des Einholens einer richterlichen Anordnung dazu geführt hat, dass DNA-Analysen nicht rechtzeitig durchgeführt werden konnten und dadurch der Ermittlungserfolg ausblieb oder auch nur gefährdet wurde, erfolgte nicht. Damit ist ohne zwingenden Grund eine verfahrensrechtliche Sicherung von Grundrechten gemindert worden.

Gleiches gilt für die Regelung des § 81g StPO, die sich auf die bloße Feststellung der Identität einer Person richtet. Statt einer richterlichen Genehmigung reicht nunmehr auch hier die schriftliche Einwilligung des Beschuldigten in die Entnahme und Untersuchung von DNA-Material aus. Ebenfalls vorgesehen ist eine Eilkompetenz der Staatsanwaltschaft.

Schließlich ist mit § 81h StPO die gesetzliche Grundlage für das bislang nicht geregelte und auf freiwilliger Basis erfolgte DNA-Massenscreening geschaffen worden. Auch in seiner gesetzlichen Fassung bleibt die Teilnahme daran zunächst freiwillig. Vom Screening ist regelmäßig eine Vielzahl unverdächtiger Personen betroffen. Auf sie treffen Merkmale zu, die auch auf den mutmaßlichen noch unbekannten Täter, dessen DNA-Spuren beispielsweise am Tatort gefunden wurden, zutreffen könnten. Die Vorschrift regelt jedoch nicht

in ausreichender Klarheit, dass zunächst die Möglichkeiten anderer gesetzlich geregelter Ermittlungsmaßnahmen zur Tataufklärung ausgeschöpft sein müssen und dass ein Massenscreening erst als letztes Mittel in Betracht kommt.

Durch die neue Regelung der DNA-Analyse kann das Erfordernis der Einholung einer richterlichen Genehmigung durch die Einwilligung des Betroffenen ersetzt werden. Damit ist eine wichtige verfahrensrechtliche Schranke zur Sicherstellung von Rechten im Strafverfahren und insbesondere auch dem Recht auf informationelle Selbstbestimmung zu Gunsten der Verfahrensvereinfachung aufgegeben worden.

5.1.2 Datenverarbeitung zur Fußball-Weltmeisterschaft 2006

Der Veranstalter der Fußball-Weltmeisterschaft 2006 (WM 2006), der Deutsche Fußballbund, und die Bundesregierung wollen eine möglichst umfassende Sicherheit garantieren. Beim Deutschen Fußballbund werden Daten von ca. 3,8 Mio. Personen, vom Arzt über den Würstchenverkäufer bis zum Zuschauer, zwecks Sicherheitsprüfung erfasst.

Bereits das Ticketverkaufsverfahren soll sicherstellen, dass jede verkaufte Eintrittskarte ihrem Erwerber weltweit über den Spieltag hinaus zugeordnet werden kann. Diese Vorgabe wird durch den ausschließlich als Bestellverfahren organisierten Verkauf erreicht: Es müssen Name, Alter, Anschrift, Pass- oder Personalausweisnummer, Telefon- und Faxnummer, E-Mail-Adresse, Bankverbindung oder Kreditkartendaten angegeben werden. Die Daten werden beim Deutschen Fußballbund erfasst und ca. zwei Jahre lang aufbewahrt. Sie werden auch mit der bei der Zentralen Informationsstelle Sport geführten Stadionverbotsdatei und mit den polizeilichen Datenbeständen über Gewalttäter und Hooligans abgeglichen und zur Durchführung der Eintrittskontrollen an den Spieltagen genutzt.

Alle Eintrittskarten verfügen über einen Radio-Frequency-Identification (RFID) Chip. Auf diesem sind zwar keine personenbezogenen Daten gespeichert, jedoch ermöglicht er den Abgleich des Tickets mit den Daten des Zutrittskontrollsystems. In Zweifelsfällen muss ein Ausweis vorgezeigt werden.

Datenschutzrechtliche Bedenken bestehen gegen die mit dem Ticketverfahren verbundene umfangreiche Datenverarbeitung. Mit ihr ist der anonyme Besuch von Veranstaltungen nicht mehr möglich. Der WM 2006 könnte insoweit eine Vorreiterfunktion zukommen. Schon jetzt steht fest, dass die angeschafften Zutrittskontrollsysteme der Austragungsstadien nach der WM 2006 nicht wieder abgebaut werden sollen.

Ein Akkreditierungsverfahren regelt darüber hinaus den Zutritt derjenigen Personen, die in den Stadien ihrer beruflichen Tätigkeit nachgehen oder als freiwillige Helfer tätig sind. Die zu Akkreditierenden werden mit ihrer schriftlich erteilten Einwilligung durch eine Abfrage bei Polizei- und Verfassungsschutzbehörden auf ihre Zuverlässigkeit überprüft. Ungeachtet der Tätigkeit, für die jemand sich bewirbt, und des Arbeitsorts innerhalb des Stadions ist das Verfahren für alle Personengruppen gleich. Nach positivem Abschluss des Akkreditierungsverfahrens erhält der Betroffene einen Ausweis, der ihn zum Betreten des Stadions ohne weitere Zutrittskontrolle berechtigt. Personen mit negativem Ergebnis werden nicht zugelassen. Zu den insgesamt ca. 300.000 Personen, die sich akkreditieren lassen müssen, gehören

- Mitarbeiter der FIFA und des Organisationskomitees,
- Angehörige der Mannschaften und Begleitdelegationen,
- Mitarbeiter und Berechtigte der Sponsoren,
- Presseangehörige und Journalisten,
- Mitarbeiter der Sicherheitsunternehmen und der Polizei,
- freiwillige Helfer,
- Servicepersonal aller Sparten.

Das Akkreditierungsverfahren wird überwiegend über das Internet abgewickelt. Die Bewerber müssen zunächst ein Online-Antragsformular ausfüllen. Es beinhaltet die Einwilligungserklärung in die Zuverlässigkeitsüberprüfung und die dazu erforderliche Datenübermittlung zwischen Organisationskomitee und Polizei sowie Verfassungsschutz. Weiterhin enthält es eine Datenschutzinformation, mit der der Bewerber über die Tatsache der Überprüfung, ihren Umfang und die Folgen sowie über seine Rechte unterrichtet wird. Arbeitgeber, die Sammelakkreditierungen für ihre Beschäftigten beantragen, müssen deren Einwilligung einholen und für die Dauer der Weltmeisterschaft aufbewahren. Das Bundeskriminalamt gleicht in dem Verfahren zunächst als zentrale Stelle die Daten mit der Datei „Gewalttäter Sport“ ab. Anschließend werden die Datensätze nach Wohnsitz den Ländern, der Bundespolizei und dem Verfassungsschutz zugeordnet und übersandt. Diese Stellen gleichen ihrerseits die Daten ab und bewerten die Ergebnisse anhand eines bundesweit einheitlichen Kriterienkatalogs. Sie senden die Datensätze zusammen mit dem Votum „Bedenken“ bzw. „keine Bedenken“ an das Bundeskriminalamt zurück.

Eine ablehnende Empfehlung ist vorgesehen, wenn die überprüfte Person wegen einer Straftat von erheblicher Bedeutung rechtskräftig verurteilt wurde oder wenn sie in der Datei „Gewalttäter Sport“ erfasst ist. In Einzelfällen können aber auch wiederholte Verurteilungen wegen leichter Straftaten und vorliegende Erkenntnisse über Staatsschutz– oder Betäubungsmitteldelikte sowie organisierte Kriminalität zu einer negativen Beurteilung führen.

Grundlage der Sicherheitsprüfung ist die Einwilligung des Antragstellers sowie in Brandenburg auch § 30 Abs. 1 Nr. 1 Brandenburgisches Polizeigesetz für den Abgleich der personenbezogenen Daten mit den hiesigen kriminalpolizeilichen Sammlungen. Letzterer befugt die Polizei zum Abgleich personenbezogener Daten von Störern und Tatverdächtigen. Die Vorschrift schließt auch solche Personen ein, die bisher nicht polizeibekannt geworden sind, wenn dies zur Gefahrenabwehr sowie zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die Übermittlung der Daten vom Organisationskomitee an die Polizei sowie die Mitteilung des Abgleichsergebnisses in Form von „Bedenken“ bzw. „keine Bedenken“ stützt sich wiederum auf die Einwilligungserklärung des Betroffenen.

Die datenschutzrechtliche Kritik richtet sich gegen die große Zahl der überprüften Personen und der undifferenzierten Überprüfung nach dem Tätigkeits- und Einsatzbereich. Eine Verfahrensänderung ist mit der Begründung abgelehnt worden, dass es angesichts der aktuellen Gefährdungslage für die Weltmeisterschaft 2006 nicht darauf ankomme, zu welchen Bereichen die zu überprüfenden Personen Zutritt erhalten und welche Tätigkeiten sie dort ausüben. Akkreditierte Personen hätten kontrollfreien Zutritt zu vielen Bereichen, die normalen Besuchern verwehrt seien. Von einem Würstchenverkäufer im Stadiongelände könne somit die gleiche Gefahr ausgehen, wie von einem Servicebediensteten in der VIP-Lounge.

Für das Akkreditierungsverfahren ist in Brandenburg beim Landeskriminalamt eine Datenbank eingerichtet worden. Die Rechtsgrundlage für den Betrieb der Datei ist neben den einschlägigen Vorschriften des Brandenburgischen Polizeigesetzes der die Einwilligung in eine Datenverarbeitung regelnde § 4 Abs. 1 Buchstabe b Brandenburgisches Datenschutzgesetz. Die konkrete Datenschutzinformation, die der Einwilligung zu Grunde liegt, ist auf unser Drängen als ein Bestandteil in das Verfahrensverzeichnis zur Datei aufgenommen worden.

Die Datenverarbeitungsmaßnahmen im Rahmen des Ticket- und Akkreditierungsverfahrens sind mit Eingriffen in die Persönlichkeitsrechte der Betroffenen verbunden. Die Kriterien, die zur Ablehnung einer Akkreditierung führen, sind teilweise sehr weit gehend und unpräzise. Die Datenschützer konnten sich mit ihren Vorschlägen, sie restriktiver zu fassen, jedoch nicht durchsetzen.

5.1.3 Prüfung der Kriminalaktenhaltung in einem Schutzbereich

Ein Ziel der Polizeistrukturreform des Landes Brandenburg war die Verlagerung von Zuständigkeiten von den Polizeipräsidien auf kleinere Einheiten, die so genannten Schutzbereiche. Während früher die gesamte Kriminalaktenhaltung in den Präsidien selbst zentralisiert war, ist nun jeder Schutzbereich für die dort anfallenden Akten verantwortlich. Nach Abschluss der Verteilung der Aktenbestände von den Präsidien auf die Schutzbereiche haben wir eine erste datenschutzrechtliche Prüfung durchgeführt.

Der geprüfte Schutzbereich hat ca. 13.000 Kriminalakten von seinem Polizeipräsidium übernommen und ohne eine erneute Erforderlichkeitsprüfung in den Bestand eingegliedert und datenschutzgerecht in verschlossenen Räumen untergebracht.

Das in der Kriminalaktenhaltung tätige Personal hat Schreib- und Änderungsrechte für das brandenburgische Polizeiliche Auskunftssystem Straftaten (PASS) und den Kriminalaktennachweis (KAN) Land/Bund. Es legt eigenständig die Aussonderungsprüffristen fest, führt die nach Fristablauf vorgeschriebenen Erforderlichkeitsprüfungen durch und entscheidet über die Löschung bzw. Weiterspeicherung der Daten in den kriminalpolizeilichen Sammlungen (PASS, KAN und Kriminalakte).

Alle geprüften Akten enthielten Merkblätter mit Beschreibungen des Tathergangs zu den einzelnen Tatvorwürfen sowie das Abgabedatum an die Staatsanwaltschaft. Der Verfahrensausgang war jedoch in keiner der geprüften Akten registriert. Dazu erklärte der Schutzbereich, dass das auf das brandenburgische Staatsanwaltschaftliche Verfahrensregister MESTA (Mehrländer-Staatsanwaltschaft-Automation) gestützte Rückmeldeverfahren erst seit 2003 funktioniere und die Polizei daher auch erst seit 2003 ohne Nachfrage Kenntnis vom Verfahrensausgang erhalte. Es sei nicht möglich, bei alten Kriminalakten den Verfahrensstand der vor 2003 abgeschlossenen Ermittlungsverfahren durch Nachfrage bei der Staatsanwaltschaft festzustellen. Dies geschehe nur im Einzelfall bei Auskunfts- und Löschungsbegehren. Weiterhin wurde die Auffassung vertreten, dass eine Löschungsverpflichtung erst mit Ablauf der Aussonderungsprüffrist eintrete.

Ungeachtet der praktischen Umsetzungsprobleme beim Rückmeldeverfahren ist der Umgang mit den Akten datenschutzrechtlich zu bemängeln. Zur Durchführung der Erforderlichkeitsprüfung ist die Kenntnis des Verfahrensausgangs unverzichtbar. Nach § 47 Abs. 2 Nr. 3 Brandenburgisches Polizeigesetz (BbgPolG) muss zudem nicht nur nach Ablauf der Aussonderungsprüffrist festgestellt werden, ob die Kriminalakte oder ein automatisiert ge-

speichertes Datum zur Aufgabenerfüllung noch erforderlich ist, sondern auch aus Anlass einer Einzelfallbearbeitung. Als Einzelfallbearbeitung mit der Verpflichtung zu einer Erforderlichkeitsprüfung gilt dabei jeder Anlass, zu dem die Akte eingesehen werden muss. Unabhängig vom Aussonderungsprüfdatum sind die Daten immer dann zu löschen, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Die einmalige Aktenübernahme aus dem Präsidium begründet für sich noch keine Verpflichtung zur Erforderlichkeitsprüfung aller ca. 13.000 übernommenen Akten. Eine Einzelfallbearbeitung i. S. v. § 47 Abs. 2 Nr. R BbgPolG ist hier noch nicht anzunehmen. Anders verhält es sich jedoch bei Kriminalakten, die infolge eines Wohnortwechsels der Betroffenen an die Polizeidienststelle übersandt werden. Hier ist das Tatbestandsmerkmal „Einzelfallbearbeitung“ erfüllt. Der Schutzbereich hat sich unserer Auffassung angeschlossen und angewiesen, dass die Erforderlichkeitsprüfung nicht erst mit Ablauf der Aussonderungsprüffrist erfolgt, sondern auch, wenn die Mitteilung des Ausgangs des staatsanwaltschaftlichen Ermittlungsverfahrens eingeht. Ferner wird sie nun auch bei Anfragen auf Datenübermittlungen oder Eingang von zu den Kriminalakten zu nehmenden neuen Informationen sowie bei Neuzugang oder Abgabe einer Kriminalakte durchgeführt. Das Ergebnis der Erforderlichkeitsprüfung ist jeweils zu dokumentieren.

Den gesamten vom Polizeipräsidium übernommenen Kriminalaktenbestand rückwirkend zu sichten und ggf. um die Verfahrensausgänge zu ergänzen, ist nicht zu leisten. Alle neuen, die Akten betreffenden Arbeitsvorgänge müssen jedoch zum Anlass genommen werden, zu prüfen, ob deren weitere Speicherung im konkreten Einzelfall noch gerechtfertigt ist.

5.1.4 Keine Benachteiligung wegen Eingaben bei der Datenschutzbeauftragten

Auf Grund der Mitteilung eines Petenten, dass ein Polizeibeamter Daten unzulässigerweise an Dritte weitergegeben habe, hat das Polizeipräsidium gegen den betroffenen Polizeibeamten Strafanzeige gestellt. Als sich herausstellte, dass der Sachverhalt frei erfunden war, stellte dieser wiederum Strafanzeige gegen den Petenten. Fraglich ist, inwieweit das Verbot, Betroffene wegen ihrer Petition zu benachteiligen, hier berührt sein könnte.

Gemäß § 21 Brandenburgisches Datenschutzgesetz hat jedermann das Recht, sich an die Datenschutzbeauftragte des Landes Brandenburg zu wenden, wenn er der Ansicht ist, durch die Datenverarbeitung einer öffentlichen Stelle in seinen Persönlichkeitsrechten verletzt zu sein. Daraus darf ihm kein Nachteil erwachsen.

Die Vermutung des Petenten, in seinen Rechten durch einen Verstoß gegen das Datenschutzrecht verletzt worden zu sein, reicht aus, um vom Anrufungsrecht zulässigerweise Gebrauch machen zu dürfen. Auf das tatsächliche Vorliegen einer Verletzung seines Rechts auf informationelle Selbstbestimmung oder die Möglichkeit, sie beweisen zu können, kommt es nicht an.

Der Nachweis des Sachverhalts sowie dessen rechtliche Bewertung fallen in den Aufgabenbereich der Landesbeauftragten. Sie erforscht diesen bei den Daten verarbeitenden Stellen, die ihrerseits verpflichtet sind, sie bei dieser Arbeit zu unterstützen und ihr unbeschränkten Zutritt zu Räumlichkeiten und Einsicht in Unterlagen zu gewähren. Dies gilt auch, soweit bei der Bearbeitung einer Eingabe die persönliche Sphäre der Verwaltungsmitarbeiter berührt wird. Als Angehörige des öffentlichen Dienstes unterliegen sie hinsichtlich ihres Amtshandelns einer umfassenden rechtlichen Kontrolle. Ergeben sich aus der datenschutzrechtlichen Beurteilung dienst-, arbeits- oder gar strafrechtliche Konsequenzen, dürfen dem Petenten, der die Untersuchung veranlasste, keine negativen Folgen daraus erwachsen. Das gilt selbst dann, wenn sich bei einer späteren gerichtlichen Überprüfung herausstellt, dass die Vorwürfe gegen die Verwaltungsangehörigen keinen rechtlichen Bestand haben.

Aus dem Grundsatz, dass die Wahrnehmung von Grundrechten dort an ihre Grenzen stößt, wo sie in die Grundrechte anderer eingreift, folgt allerdings, dass der Schutz des Benachteiligungsverbots dort erlischt, wo ein Petent durch vorsätzlich falsche Tatsachenbehauptungen gerade beabsichtigt, einem Dritten mittels seiner Eingabe Schaden zuzufügen. In solchen Fällen kann auch die Einleitung rechtlicher Schritte gegen einen Petenten auf Grund seiner Eingabe zulässig sein. Die Rechtsordnung schützt hier vor der wissentlichen Behauptung unwahrer Tatsachen, die geeignet ist, jemanden herabzuwürdigen und stellt sie als Verleumdung unter Strafe.

Bei dieser Abwägung von Grundrechten ist zu berücksichtigen, dass ein Petent i. d. R. nicht über interne Kenntnisse der Verwaltung verfügt. Sein vorgetragener Sachverhalt ist verständig zu werten und nicht jede nicht beweisbare Darstellung oder Äußerung subjektiver Eindrücke darf negative rechtliche Folgen für ihn entfalten. Die datenschutzrechtliche Prüfung des Sachverhalts darf nicht Bestandteil des eigentlichen Verwaltungsvorgangs werden. Eine andere Handhabung kann sonst unabhängig vom Ergebnis zu einer Voreingenommenheit der Bearbeiter bei der nachfolgenden Befassung führen. Daher ist es sinnvoll, die Bearbeitung einer solchen Eingabe von einer nicht mit der ursprünglichen Verwaltungsaufgabe betrauten Abteilung der Daten verarbeitenden Stelle vornehmen zu lassen.

Das Verbot, einen Petenten auf Grund seiner Eingabe zu benachteiligen, erstreckt sich grundsätzlich über den gesamten Zeitraum der datenschutzrechtlichen Bearbeitung. Erst nach deren Abschluss können weitere rechtliche Schritte in Betracht gezogen werden. Nur in Ausnahmefällen, wenn sich herausstellt, dass mit der Eingabe bei der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht mit Wissen und Vorsatz einem Dritten geschadet werden soll, können auch gegen den Petenten strafrechtliche Maßnahmen eingeleitet werden.

5.1.5 Technische Kontrolle des Landeskriminalamtes

Die im Rahmen der Polizeistrukturreform vollzogene Zentralisierung der polizeilichen Datenverarbeitung beim Zentraldienst der Polizei führte zu zahlreichen datenschutzrechtlichen Mängeln, die durch bessere Vorbereitung und die rechtzeitige Erstellung eines IT-Sicherheitskonzeptes[35] vermeidbar gewesen wären. Nicht alle Mängel wurden bisher abgestellt.

Im November 2003 führten wir eine mehrtägige, von den einzelnen Fachverfahren weitest gehend unabhängige Kontrolle im Landeskriminalamt durch. Da zu diesem Zeitpunkt im Zuge der Polizeistrukturreform nahezu die gesamte Informationstechnik aus dem Landeskriminalamt ausgegliedert und beim Zentraldienst der Polizei konzentriert wurde, fand auf Wunsch des Landeskriminalamtes ein wesentlicher Teil der Kontrolle beim Zentraldienst der Polizei in Wünsdorf statt.

Bereits während der Prüfungsvorbereitung sah das Landeskriminalamt für Teile seiner Datenverarbeitung keine eigene Zuständigkeit mehr und es traten erhebliche Unklarheiten darüber auf, welche der von uns für die Prüfung angeforderten Unterlagen vom Landeskriminalamt und welche vom Zentraldienst der Polizei bereitzustellen waren. Der Zentraldienst der Polizei hatte seinerseits Bedenken, uns im Vorfeld vertrauliche Unterlagen zur Vorbereitung zu übergeben und wollte uns lediglich Einsicht während der Kontrolle gewähren. Im Ergebnis trafen die unvollständigen Unterlagen mit erheblicher Verspätung, zum Teil erst drei Tage vor dem vereinbarten Kontrolltermin ein und der überwiegende Teil wurde uns vor Ort übergeben. Nur dank der kooperativen Zusammenarbeit und der geleisteten Unterstützung durch die an der Kontrolle beteiligten Mitarbeiter des Landeskriminalamtes und des Zentraldienstes der Polizei konnten wir unseren gesetzlichen Kontrollauftrag trotz Probleme im Vorfeld noch erfüllen. Nach der Polizeistrukturreform herrschten noch erhebliche Unsicherheiten bezüglich der datenschutzrechtlichen Verantwortung zwischen dem Landeskriminalamt und dem Zentraldienst der Polizei. So erwies es sich im Verlauf der Kontrolle oft als schwierig,

[35] vgl. dazu schon oben A 2.8

aussagefähige Ansprechpartner zu finden, die in der Lage waren, einzelne Sachverhalte der technisch-organisatorischen Maßnahmen bzw. des Ablaufs der Datenverarbeitung darzustellen. Vielmehr wurde dazu jeweils auf den anderen Vertragspartner verwiesen.

5.1.5.1 Verantwortung für die Datenverarbeitung

Im Zuge der Polizeistrukturreform wurde die komplette Datenverarbeitung, einschließlich der gesamten Technik und des zuständigen IT-Personals, vom Landeskriminalamt an den Zentraldienst der Polizei ausgegliedert. Datenschutzrechtlich liegt eine Datenverarbeitung im Auftrag[36] gem. § 11 Brandenburgisches Datenschutzgesetz vor: Das Landeskriminalamt hat als Auftrag gebende Stelle die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes mit dem Zentraldienst der Polizei vertraglich zu vereinbaren. Zum Zeitpunkt der Kontrolle bestanden keine entsprechenden Vereinbarungen, obwohl die Auftragsdatenverarbeitung bereits seit längerer Zeit praktiziert wurde. Man verwies auf einen Globalvertrag, den das Ministerium des Innern vorbereite. Die fehlenden vertraglichen Regelungen führten dazu, dass wesentliche Verantwortlichkeiten nicht eindeutig zugeordnet waren. Teilweise hatten wir den Eindruck, dass sowohl das Landeskriminalamt als auch der Zentraldienst der Polizei dies nutzten, um die Verantwortung jeweils dem anderen Partner zuzuweisen. Das Landeskriminalamt kann unter diesen Voraussetzungen seiner Kontrollpflicht gegenüber dem Zentraldienst der Polizei nicht nachkommen.

Unterschiedliche Auffassungen bestanden zwischen dem Landeskriminalamt und dem Zentraldienst der Polizei bezüglich der rechtlichen Einordnung der Datenverarbeitung[37]. Während der Zentraldienst der Polizei strikt von einer Datenverarbeitung im Auftrag ausging, vertrat das Landeskriminalamt die Meinung, dass mit der Ausgestaltung der Aufgaben des Zentraldienstes der Polizei zumindest eine teilweise Funktionsübertragung[38] auf dem Gebiet der Datenverarbeitung vorgenommen wurde. Dafür hätte auch der beim Landeskriminalamt verbliebene sehr geringe Bestand an IT-Fachkräften sprechen können, da dieser die mit der Datenverarbeitung im Auftrag verbundenen datenschutzrechtlichen Aufgaben nicht hätte bewältigen können. Außerdem bestand keine Weisungsbefugnis des Landeskriminalamtes bezüglich der Datenverarbeitung gegenüber dem Zentraldienst der Polizei.

Wir haben den Innenminister in einem Schreiben auf diesen Mangel bei der Sicherstellung der datenschutzrechtlichen Verantwortung des Landeskriminalamts hingewiesen und gebeten, dafür Sorge zu tragen, dass im Landes-

[36] vgl. Tätigkeitsbericht 2003, A 1.2.1
[37] vgl. Tätigkeitsbericht 2003, A 1.2
[38] vgl. Tätigkeitsbericht 2003, A 1.2.2

kriminalamt qualifiziertes Personal z. B. im Rahmen von IT-Kopfstellen zur Verfügung gestellt wird, das gegenüber dem Zentraldienst der Polizei Weisungen erteilen kann. In seiner Antwort verwies das Ministerium des Innern auf die ständige Fortbildung des bestehenden Personals und einen bereits bestehenden Organisationsbereich mit Führungs- und Controllingverantwortung und teilte uns mit: „Die Einrichtung zusätzlicher IT-Kopfstellen wird daher derzeit nicht erwogen. Vielmehr sind die Polizeibehörden und -einrichtungen grundsätzlich bereits jetzt in der Lage, die ihnen obliegende datenschutzrechtliche Verantwortung wahrzunehmen.“ Der Zustand besteht daher unverändert fort.

5.1.5.2 Risikoanalyse und IT-Sicherheitskonzept

Das uns zur Kontrolle vorgelegte IT-Sicherheitskonzept des Landeskriminalamts war identisch mit einer bereits im Mai 2001 vorgelegten Fassung, die wir damals bemängelt hatten. Sie entsprach in keiner Weise den Forderungen des Bundesamtes für Sicherheit in der Informationstechnik.

Die Verantwortung für die Erstellung eines IT-Sicherheitskonzeptes auf der Basis einer projektspezifischen Risikoanalyse bleibt bei der hier vorliegenden Datenverarbeitung im Auftrag beim Landeskriminalamt als Auftraggeber. Es erscheint allerdings sinnvoll, dass sich beide Vertragsparteien auf gemeinsame Sicherheitsstandards einigen und für beide Seiten verbindliche technische und organisatorische Maßnahmen vertraglich festlegen. Die Verantwortung für die Kontrolle der Einhaltung der vereinbarten Maßnahmen und ihre laufende Anpassung an den aktuellen Stand der Technik verbleibt ebenfalls beim Landeskriminalamt. Vom Zentraldienst der Polizei sollten als fachlich kompetentem IT-Dienstleister entsprechende Vorschläge unterbreitet werden, die vom Landeskriminalamt zu überprüfen, ggf. zu erweitern und zu bestätigen sind.

Das Landeskriminalamt stellte in seiner Stellungnahme die Erstellung des IT-Sicherheitskonzeptes bis zum IV. Quartal 2004 in Aussicht und versprach, uns ein Exemplar unaufgefordert nachzureichen. Dies geschah bisher allerdings nicht.

Die Ausgliederung von Teilen der Datenverarbeitung (Outsourcing) oder ganzer IT-Bereiche an zentrale Dienstleister erfordert bereits im Vorfeld Maßnahmen, die sicherstellen, dass die datenschutzrechtliche Verantwortung stets eindeutig zugeordnet werden kann. Mithilfe von IT-Sicherheitskonzepten ist nachzuweisen, dass die damit verbundenen Risiken beherrschbar sind. Die erforderlichen technischen und organisatorischen Maßnahmen orientieren sich u. a. am jeweiligen Stand der Technik und müssen diesem fortlaufend angepasst werden.

5.1.6 Die Internetwache der Polizei in Brandenburg

Bereits seit Anfang des Jahres 2003 betreibt die Polizei in Brandenburg eine Internetwache, deren Möglichkeiten im Laufe der Jahre 2004 und 2005 noch einmal deutlich erweitert wurden. Durch die frühzeitige Beteiligung der Landesbeauftragten durch das Ministerium des Innern und die Polizei wurden die datenschutzrechtlichen Belange von Anfang an berücksichtigt.

Die Internetwache[39] erleichtert durch eine Reihe von Funktionen die Kontaktaufnahme zur Polizei. So kann man beispielsweise über das Internet eine Anzeige aufgeben, eine Versammlung anmelden, sich bei der Polizei bedanken, beschweren oder bewerben. Darüber hinaus bietet die Internetwache seit einiger Zeit den Service der Einrichtung eines persönlichen virtuellen Postfaches. Damit können Bürger die Bearbeitung ihrer Angelegenheit durch die Polizei jederzeit verfolgen.

Auch um die Akzeptanz des Angebotes zu erhöhen, wurde von Anfang an Wert auf ein hohes Datenschutz- und Datensicherheitsniveau gelegt, obwohl ein umfassendes Sicherheitskonzept seitens des Ministeriums des Innern noch aussteht.

Zur Gewährleistung der Vertraulichkeit der Kommunikation setzt die Polizei für die Übertragung verschiedene Verschlüsselungsverfahren ein. Für die Kommunikation zwischen Nutzer und Webserver wird über das Protokoll https eine gesicherte SSL-Verbindung (128 bit) aufgebaut. Für die interne Kommunikation zwischen Webserver und einem polizeiinternen Server wird das Verfahren PGP verwendet. Beim virtuellen Postfach wird die Vertraulichkeit der gespeicherten Daten über ein asymmetrisches Verschlüsselungsverfahren gesichert, wobei der private (geheime) Schlüssel allerdings auf dem Server selbst abgelegt wird. Dies gibt versierten Angreifern die Möglichkeit, den privaten Schlüssel auszulesen. Durch den Einsatz einer chipkartenbasierten Lösung ließe sich diese Schwachstelle beheben. Insgesamt ist die Nutzung der Internetwache freiwillig. Konsequenterweise sieht die Polizei keine Pflichtfelder vor. Damit ist grundsätzlich auch eine anonyme Kontaktaufnahme zur Polizei möglich. Die zahlreichen Webformulare beschränken sich jeweils auf die erforderlichen Daten. Auch werden bei der Internetwache auf dem Webserver keine IP-Adressen der auf das Angebot zugreifenden Rechner gespeichert. Damit wird die zentrale gesetzliche Verpflichtung des Multimediadatenschutzrechts erfüllt, Nutzungsdaten unverzüglich nach Ende der Nutzung zu löschen. Nutzungsprofile können von der Polizei so nicht gebildet werden.

[39] siehe http://www.polizei.brandenburg.de oder http://www.internetwache.de

Aus datenschutzrechtlicher Sicht sind bei der Umsetzung des Projekts „Internetwache“ bei der Polizei viele positive Ansatzpunkte zu bemerken. Dennoch müsste die Datensicherheit durch den Einsatz von Chipkarten zur Verschlüsselung noch verbessert und ein dem Brandenburgischen Datenschutzgesetz genügendes Sicherheitskonzept erstellt werden.

5.1.7 Bildung eines zentralen IT-Dienstleisters für das Land

Die von der Landesregierung beschlossene IT-Strategie für die Jahre 2004 bis 2008 sieht u. a. vor, die Abteilung Datenverarbeitung des Landesbetriebes für Datenverarbeitung und Statistik und den Bereich Informationstechnik des Zentraldienstes der Polizei zu einem zentralen IT-Dienstleister zusammenzuführen. Dieses Vorhaben wird später um die Aufgabe erweitert, eine Zentralstelle für das Beschaffungswesen für die Landesverwaltung zu schaffen. Es soll ein „Zentraldienst für Technik und Beschaffung des Landes Brandenburg“ geschaffen werden.

In unserem Tätigkeitsbericht 2003 haben wir bereits ausführliche Hinweise zu den mit dem Outsourcing[40] von Datenverarbeitungsleistungen verbundenen Problemen gegeben und Lösungsvorschläge unterbreitet.

Bei der Schaffung eines zentralen Großrechenzentrums, das alle zentralen IT-Verfahren für das Land bearbeitet und im Rahmen der bestehenden Möglichkeiten auch umfassende Datenverarbeitungsleistungen für die Landkreise und Gemeinden mit dem Ziel der Kosteneinsparung anbietet, besteht immer auch die Gefahr, dass durch eine erhebliche Konzentration personenbezogener Daten an einer zentralen Stelle ein „gläsernen Bürger“ geschaffen werden könnte.

Die bestehenden Datenschutzregelungen bieten jedoch ausreichende Möglichkeiten, dies zu verhindern. Technische und organisatorische Maßnahmen, die auf der Grundlage von IT-Sicherheitskonzepten festzulegen und fortlaufend dem aktuellen Stand der Technik anzupassen sind, spielen dabei eine wesentliche Rolle. Sie ermöglichen nicht nur eine konsequente Abschottung der einzelnen Datenbestände voneinander und eine restriktive Gestaltung der Zugriffsrechte, sondern sind auch für die Sicherheit und Verfügbarkeit der Daten von besonderer Bedeutung. Sie tragen dazu bei, Datenverfälschungen oder totale Datenverluste zu verhindern, die bei der heute gegebenen Abhängigkeit von der Informationstechnik in den meisten Fällen praktisch zum völligen Zusammenbruch der Arbeitsfähigkeit einer Einrichtung führen könnten. Sicherheitstechniken zur Verschlüsselung und zur digitalen Signatur[41],

[40] vgl. Tätigkeitsbericht 2003, A 1.2
[41] vgl. A 2.10

zur Protokollierung von Datenzugriffen, zur Kontrolle möglicher Täter aus den Reihen der Beschäftigten[42] und zur Behandlung von Ausfällen der Informationstechnik spielen dabei eine besondere Rolle.

Der bisherige IT-Dienstleister des Landes, der Landesbetrieb für Datenverarbeitung und Statistik, konnte bei der Einführung und Betreuung zentraler IT-Verfahren bereits gute Erfahrungen sammeln und eine führende Rolle im Land Brandenburg übernehmen. Die Vereinigung mit dem IT-Bereich beim Zentraldienst der Polizei sollte deshalb so gestaltet werden, dass diese Erfahrungen auch künftig nutzbar bleiben.

Obwohl bis zum gegenwärtigen Zeitpunkt noch keine endgültige Entscheidung über die Struktur und organisatorische Zuordnung der neu zu schaffenden Organisationseinheit gefallen ist, wurden wir bereits im Juni des Jahres 2005 im Interministeriellen Ausschuss für Informationstechnik (IMA-IT) darüber informiert, dass der gemeinsame IT-Dienstleister unter dem „Dach der Polizei“ angesiedelt werden soll. Dabei würden sich aus der Sicht des Datenschutzes zusätzliche Probleme ergeben, wenn wesentliche personenbezogene Daten der Bürger überwiegend von verbeamteten Polizisten, die in eine Polizeistruktur eingebunden sind, verarbeitet werden. Wir haben dem Ministerium des Innern unsere diesbezüglichen Bedenken mitgeteilt und auf einen möglichen Vertrauensverlust bei den Bürgern gegenüber der Verwaltung hingewiesen, wenn ihre gesamten Daten unter dem „Dach der Polizei“ des Landes verarbeitet werden.

Die jüngsten Pläne des Ministeriums des Innern den zentralen IT-Dienstleister in einem völlig neuen Organisationsgebilde, dem Zentraldienst für Technik und Beschaffung des Landes Brandenburg, einzugliedern, betrachten wir deshalb mit Sorge. Wird man der wachsenden Bedeutung, die eine zentrale Informationstechnik für die Landesverwaltung und den kommunalen Bereichen des Landes hat, dadurch gerecht, indem man sie als Teil einer gewaltigen Organisationsstruktur, die auch alle Beschaffungsaufgaben des Landes lösen soll, betrachtet? Werden die IT-Sicherheitsfragen und der Datenschutz eine angemessene Berücksichtigung finden oder aus Kostengründen zu Gunsten anderer notwendiger Beschaffungen benachteiligt? Unsere Sorge wird übrigens von führenden Polizeibeamten des Landes geteilt. Es wurde inzwischen eine Projektgruppe eingerichtet, die sich zunächst ergebnisoffen mit den möglichen Organisationsformen eines IT-Dienstleisters für das Land Brandenburg befassen soll.

[42] vgl. A 2.14

Die Schaffung eines zentralen Dienstleisters für die Verarbeitung von Bürgerdaten unter dem Dach der Polizei sehen wir kritisch. Wegen der damit verbundenen datenschutzrechtlichen Fragen haben wir unsere Mitarbeit in der zuständigen Projektgruppe angeboten.

5.2 Verfassungsschutz: Mit „Viper“ zum papierlosen Büro

Mit Änderung des Brandenburgischen Verfassungsschutzgesetzes vom 24. Mai 2004 ist die Einführung eines „papierlosen Büros“ möglich. Die Neuregelung schafft keine neuen Datenverarbeitungsbefugnisse, sondern erlaubt nur eine sich ausschließlich auf automatisierte Datenverarbeitung stützende Aufgabenerledigung.

Auf den ersten Blick würde ein papierloses Büro verwaltungstechnische Vereinfachungen mit sich bringen. Der Verzicht auf jedweden papierenen Aktenrückhalt kann aber auch problematisch sein. Bislang musste jede in einer automatisierten Datei gespeicherte personenbezogene „Primärinformation“ durch die im Aktenrückhalt abgelegten „Sekundärinformationen“ belegt und damit nachvollziehbar gemacht werden können. Der Wegfall des Aktenrückhalts wäre daher nur unter den folgenden Voraussetzungen hinnehmbar: Die Zugriffsrechte auf die automatisierte Datenverarbeitung müssen so festgelegt werden, dass sie organisatorisch exakt den bisherigen Zustand abbilden. Es dürfen nicht mehr Personen als bisher Zugriff zu den Informationen haben, nur weil das durch die elektronische Form der Aktenhaltung erleichtert wird. Zum anderen muss sichergestellt werden, dass die Daten nur nach sicherer Authentifikation der Mitarbeiter gespeichert und verändert werden können. Alle Änderungen in einem Vorgang müssen eindeutig nachvollziehbar bleiben. Das ist nur garantierbar, wenn eine qualifizierte elektronische Signatur eingesetzt wird.

Während die rechtlichen Voraussetzungen für das papierlose Büro bei der Verfassungsschutzbehörde vorhanden sind, haben sich die technischen Probleme bei der Realisierung der hierfür erforderlichen Datenbank als so gravierend herausgestellt, dass die Einführung abgebrochen wurde. Stattdessen ist nunmehr ein neues Content Management System „Viper“ (Verfassungsschutz-Informationsportal für Ermittlung und Recherche) eingeführt worden, mit dessen Hilfe umfangreiche Datensätze gespeichert, verknüpft und ausgewertet werden können.

Die Verfassungsschutzbehörde verarbeitet im Content Management System „Viper“ sensitive personenbezogene Daten mit hohem und sehr hohem Schutzbedarf. Das hat zur Folge, dass die in jedem Fall umzusetzenden Standardsicherheitsmaßnahmen des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik, die für den mittleren

Schutzbedarf einen angemessenen und ausreichenden Schutz bieten, im Ergebnis einer ergänzenden Sicherheitsanalyse erweitert werden müssen. Die derzeit vom Verfassungsschutz erstellte Dokumentation zur Realisierung technisch-organisatorischer Maßnahmen entspricht noch nicht diesen Forderungen.

Im System Viper ist auch eine umfassende Protokollierung der Abrufe vorgesehen. Die Protokollierung der lesenden Zugriffe erfolgt auf Grund der großen Datenmengen außerhalb des Datenbanksystems in Excel-Dateien, ändernde Zugriffe werden im Datenbanksystem selbst gespeichert. Nach Auffassung des Verfassungsschutzes sind die Protokolldatensätze zehn Jahre lang aufzubewahren. Zwar sind gemäß § 8 Abs. 4 Brandenburgisches Verfassungsschutzgesetz gespeicherte personenbezogene Daten über verfassungsfeindliche Bestrebungen nach spätestens zehn Jahren zu löschen. Das bedeutet nach unserer Auffassung jedoch nicht, dass auch die Protokolldateien erst nach zehn Jahren zu löschen sind. Hier reichen wesentlich kürzere Speicherfristen aus. In der Orientierungshilfe[43] des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Datenschutzrechtlicher Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)“ wird gefordert, Einträge in den Protokolldateien spätestens ein Jahr nach Entstehung zu löschen.

Die Verfassungsschutzbehörde hat uns zugesichert, die von uns geforderten technisch-organisatorischen Maßnahmen bei der Erstellung eines umfassenden IT-Sicherheitskonzeptes zu berücksichtigen. Ein erster Schritt wurde diesbezüglich schon getan. In einer gemeinsamen Beratung mit der Verfassungsschutzbehörde werden wir die notwendigen Schritte, die bei der Erstellung eines IT-Sicherheitskonzeptes nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik erforderlich sind, erörtern.

Anstelle der ursprünglich geplanten Einführung eines papierlosen Büros beim Verfassungsschutz wird dort künftig ein weniger weit reichendes Content Management System aufgebaut, das Ermittlung und Recherche unterstützen soll. Auf Grund der Verarbeitung besonders sensitiver personenbezogener Daten sind neben den Grundschutzmaßnahmen des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik erweiterte Sicherheitsbetrachtungen erforderlich. Die daraus resultierenden technisch-organisatorischen Maßnahmen sind in einem IT-Sicherheitskonzept zu dokumentieren und zeitnah umzusetzen.

[43] siehe http://www.lda.brandenburg.de/sixcms/detail.php?id=87042&template=allgemein_lda

5.3 Ausländer: Brandenburg richtet eine Härtefallkommission ein

Das bisherige Ausländergesetz ist durch das Artikelgesetz zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern abgelöst worden. Artikel 1 beinhaltet das Aufenthaltsgesetz, welches Bestimmungen zur Einrichtung einer Härtefallkommission enthält.[44]

Das Härtefallverfahren ist in § 23a Aufenthaltsgesetz (AufenthG) geregelt. Die oberste Landesbehörde darf in Fällen, in denen die Aufenthaltsbeendigung eine Härte gegenüber dem Betroffenen darstellen würde, anordnen, dass trotz Vorliegen eines Versagungsgrundes einem Ausländer eine Aufenthaltserlaubnis erteilt wird. Das setzt allerdings ein Ersuchen der Härtefallkommission voraus.

In der Härtefallkommissionsverordnung (HFKV) ist festgelegt, dass die Kommission aus acht Mitgliedern und ihren Vertretern besteht, die vom Innenministerium auf Vorschlag der evangelischen sowie der katholischen Kirche, der Flüchtlingsorganisation, des Städte- und Gemeindebundes, des Landkreistages und der Ministerien für Arbeit, Soziales, Gesundheit und Familie sowie des Innern berufen werden. Sie ist keine öffentliche Stelle, sondern ein nicht weisungsgebundenes Gremium, dessen Mitglieder teilweise aus Nicht-Regierungsorganisationen kommen und daher auch nicht dienstrechtlich zu verpflichten sind. Die Kommission ist keine Revisions-, sondern eine Gnadeninstanz, die von sich aus tätig wird. In der Praxis bedeutet dies, dass ein Mitglied der Kommission einen Fall als Härtefall aufgreifen und einen diesen betreffenden Antrag über die Geschäftsstelle in die Härtefallkommission einbringen muss. Die Geschäftsstelle erwirkt von der zuständigen Ausländerbehörde eine Stellungnahme zu dem Antrag. Folgt die Kommission dem Antrag, ersucht sie das Ministerium des Innern, den weiteren Aufenthalt anzuordnen. Bis zur Entscheidung ist die Abschiebung des Betroffenen ausgesetzt.

Die Härtefallkommission verarbeitet eine Vielzahl, häufig zum privaten Kernbereich des Betroffenen zählender Daten, um beurteilen zu können, ob ein Härtefall vorlag. Sie erhält sie teilweise vom Betroffenen selbst, zum Teil von den zu beteiligenden Ausländerbehörden.

Datenschutzrechtlich ist die Überlassung personenbezogener Unterlagen durch die Ausländerbehörden an die Kommissionsmitglieder eine Übermittlung personenbezogener Daten an eine nichtöffentliche Stelle. Sie stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar und bedarf der

[44] siehe BGBl. I 2004, S. 1950

ausdrücklichen Einwilligung des Betroffenen oder einer Rechtsgrundlage. Da es keine spezielle Rechtsvorschrift gibt, bleibt das Erfordernis der Einwilligung. Mit dieser stimmt der Betroffene der Datenverarbeitung durch die Geschäftsstelle der Härtefallkommission und ihrer Übermittlung an die Kommissionsmitglieder unter der Voraussetzung zu, dass dies zur Bearbeitung des Falls erforderlich ist.

Beratungsinhalte und im Verfahren bekannt gewordene Daten sowie das Abstimmungsverhalten unterliegen der Verschwiegenheitspflicht. Der Betroffene darf über den Ausgang seines Falls informiert werden sowie darüber, ob die Kommission eine Bleibeempfehlung ausgesprochen hat, ob sein Fall an Ausschlussgründen gescheitert ist oder ob er gar nicht beraten wurde. Im Übrigen ist das Beratungsgeheimnis zu wahren, Einzelheiten über das Abstimmungsverhalten der anderen Mitglieder oder die Diskussion innerhalb des Gremiums sind auch gegenüber den Betroffenen vertraulich zu behandeln.

Wir haben vorgeschlagen, in der Geschäftsordnung für die Arbeit der Kommission auch den Umgang mit personenbezogenen Daten zu regeln. Danach soll die Geschäftsstelle zur Vorbereitung der Sitzungen entsprechend der Anzahl der Kommissionsmitglieder eindeutig gekennzeichnete Sitzungsunterlagen fertigen, die den einzelnen Mitgliedern per Einschreiben oder persönlich zugestellt werden. Die Sitzungsunterlagen müssen nach Abschluss des Falls vollständig in der Geschäftsstelle, die den Versand und Verbleib der Unterlagen dokumentiert, abgegeben werden. Das Vervielfältigen von Sitzungsunterlagen außerhalb der Geschäftsstelle durch Mitglieder der Härtefallkommission oder durch andere Personen ist unzulässig. Dem Wunsch einzelner Mitglieder der Kommission, die Unterlagen dauerhaft behalten zu dürfen, um damit eine Fallsammlung zu schaffen und eine Gleichbehandlung bei zukünftigen Entscheidungen zu gewährleisten, kann nicht entsprochen werden. Die Einwilligung des Antragstellers in die Verarbeitung seiner Daten erlischt mit dem Ende der Bearbeitung seines Falls.

Der Entwurf der Einwilligungserklärung des Betroffenen sah zunächst vor, dass sowohl der Betroffene selbst als auch die Angehörigen generell ihre Religionszugehörigkeit angeben sollten. Das haben wir für unzulässig gehalten. Nur soweit diese Information für die Beratung der Härtefallkommission erforderlich ist, muss sie Bestandteil der von der Geschäftsstelle zusammengestellten Sitzungsunterlagen sein und nicht schon Bestandteil der Einwilligung. Die Kommission ist unserer Auffassung gefolgt und hat die pauschal verlangte Angabe der Religionszugehörigkeit aus dem Einwilligungsformular gestrichen.

Der Leiter der Geschäftsstelle nimmt zwar die Außenvertretung der Härtefallkommission wahr. Auf Grund der strikten Verschwiegenheitspflicht darf er

aber nicht die Öffentlichkeit über bestimmte Einzelfälle informieren. Allerdings bleibt es dem einzelnen Betroffenen unbenommen, dass er selbst mit seinem Fall an die Öffentlichkeit geht.

Wird ein Fall Gegenstand einer parlamentarischen Anfrage, sind zur Wahrung der Persönlichkeitsrechte der Betroffenen die Regeln der nicht öffentlichen Sitzung einzuhalten. In öffentlichen Drucksachen des Landtages dürfen keine personenbezogenen Angaben erscheinen.

Die Härtefallkommission kann nur dann ihrer Aufgabe erfolgreich nachgehen, wenn alle beteiligten Stellen und die Betroffenen Vertrauen in ihre Integrität haben. Ein wesentlicher Aspekt dabei ist die Einhaltung der Verschwiegenheitspflicht durch jedes einzelne Kommissionsmitglied sowie der korrekte und sorgfältige Umgang mit den personenbezogenen Daten der Betroffenen.

5.4 Meldewesen

5.4.1 Umsetzung des Melderechtsrahmengesetzes

Die Landesregierung hat mit dem Zweiten Gesetz zur Änderung des Brandenburgischen Meldegesetzes zahlreiche Änderungen des Melderechtsrahmengesetzes des Bundes in Landesrecht umgesetzt.[45]

Die Gesetzesnovelle sieht u. a. vor, künftig bei Wohnungsumzügen die Rückmeldung der Zuzugsmeldebehörde an die Wegzugsmeldebehörde auf elektronischem Wege durchzuführen. Sie eröffnet jetzt auch die Möglichkeit zur automatisierten Erteilung von einfachen Melderegisterauskünften. Für beide Zwecke wird beim Landesbetrieb für Datenverarbeitung und Statistik eine zentrale Vermittlungsstelle eingerichtet.

Mit der Umsetzung dieser rechtlichen Neuerungen ist seit längerem eine Projektgruppe im Ministerium des Inneren befasst, an der wir beratend teilnehmen. Wir setzen uns vor allem dafür ein, dass die Sicherheit der Daten auf den Übertragungswegen und die klare Trennung der unterschiedlichen Melderegister gewahrt werden.

Im Vorfeld der Gesetzesnovellierung hatten wir erneut angeregt, die derzeitige Zustimmungslösung bei der Weitergabe von Meldedaten an politische Parteien und Adressbuchverlage durch eine konkrete Einwilligung der betroffenen Bürger zu ersetzen. Bislang müssen sie einer solchen Weitergabe ausdrücklich widersprechen, damit sie unterbleibt.

[45] siehe GVBl. I 2005, S. 274

Da die Zustimmungsregelung nicht in das Gesetz aufgenommen worden ist, kommt der Information der Bürger über ihr Widerspruchsrecht vor Wahlen eine besondere Bedeutung zu.

Bei der Umsetzung der neuen Meldebestimmungen werden wir auf die Einhaltung der Datenschutzvorschriften hinwirken.

5.4.2 Weitergabe von Meldedaten an private Adressbuchverlage

Das Brandenburgische Meldegesetz lässt zu, dass Meldedaten an privatwirtschaftliche Adressbuchverlage herausgegeben werden können, solange kein entsprechender ausdrücklicher Widerspruch der betroffenen Bürger im Melderegister eingetragen ist.

Eine Vielzahl von Beschwerden richtet sich gegen die Veröffentlichung von Namen und Anschriften in einem von privaten Verlagen erstellten Adressbuch. Den Meldebehörden wurde in diesem Zusammenhang massiv der Vorwurf des Rechtsbruchs gemacht. Der Vorwurf bestätigt sich jedoch nicht: § 33 Abs. 5 Brandenburgisches Meldegesetz (BbgMeldG) erlaubt es, Angaben aus den Melderegistern an private Adressbuchverlage weiterzugeben. Die Datenweitergabe hat zu unterbleiben, wenn der betroffene Bürger von seinem ihm nach § 33 Abs. 6 BbgMeldG eingeräumten Widerspruchsrecht Gebrauch macht. Über dieses Widerspruchsrecht sind die Bürger einmal jährlich in amtlichen Bekanntmachungen zu informieren. Die große Anzahl der Beschwerden zeigt jedoch, dass die Information nur in unzureichendem Maße die Bürger erreicht.

Durch eine intensivere Informationspolitik müssen die Bürger über die bestehende Rechtslage, insbesondere über ihr Widerspruchsrecht zur Weitergabe von Meldedaten aufgeklärt werden.

5.4.3 Parteienwerbung zur Wahl

Mit anstehenden Wahlterminen werden Bürger regelmäßig durch persönliche Wahlwerbung der Parteien über deren politische Ziele und Vorhaben informiert. Genauso regelmäßig fragen Bürger: „Woher haben die politischen Parteien meine Anschrift?“

Während des Wahlkampfs senden die politischen Parteien ihre Werbung an die Bürger. Dies erfolgt oftmals auch persönlich adressiert und mit einer Anrede versehen, um den Werbeeffekt zu erhöhen. Immer wieder beschweren sich Bürger, weil ihnen nicht klar war, wie die Parteien in den Besitz von Namen und Anschrift gekommen sind. Nach § 33 Abs. 1 Brandenburgisches Meldegesetz (BbgMeldG) erhalten die politischen Parteien, politischen Verei-

nigungen, Wählergruppen und Listenvereinigungen auf ihren Antrag hin in einem Zeitraum von bis zu sechs Monaten vor einer anstehenden Wahl zu Wahlwerbezwecken von den Meldeämtern Namen und Anschrift von wahlberechtigten Bürgern. Die übermittelten Daten müssen von den jeweiligen Empfängern spätestens eine Woche nach der Wahl gelöscht werden.

Wer diese Form der Wahlwerbung nicht wünscht, hat gemäß § 33 Abs. 6 BbgMeldG die Möglichkeit, einer Weitergabe von Name und Anschrift an politische Parteien, politische Vereinigungen, Wählergruppen und Listenvereinigungen zu widersprechen und diesen Widerspruch im Melderegister vermerken zu lassen. Eine Weitergabe von Namen und Anschriften zu Wahlwerbezwecken darf dann nicht mehr erfolgen. Dieses Widerspruchsrecht wird einmal jährlich mittels amtlicher Bekanntmachung publiziert oder per Aushang in den Meldestellen veröffentlicht.

Wer keine an ihn adressierte Wahlwerbung politischer Parteien erhalten möchte, muss das im Melderegister seines Wohnortes eintragen lassen.

5.4.4 Namensverwechslung bei Melderegisterauskunft und ihre Folgen

Eine brandenburgische Meldebehörde übermittelte einer Anwaltskanzlei aus Baden-Württemberg die Anschrift eines Potsdamer Bürgers im Rahmen einer Schuldnerermittlung. Dieser trug zufällig den gleichen Namen wie der gesuchte Schuldner und erhielt infolgedessen Mahnschreiben über Forderungen, die nie gegen ihn bestanden.

Die Meldebehörde hätte in diesem Fall der Namensgleichheit nicht unkontrolliert eine Anschrift übermitteln dürfen, sondern hätte zusätzlich persönliche Angaben des vermeintlichen Schuldners von der Anwaltskanzlei anfordern müssen, um eine zweifelsfreie Identifizierung der gesuchten Person zu garantieren. Geeignet hierzu wäre beispielsweise das Geburtsdatum der gesuchten Person.

Die Meldebehörde wurde auf diese notwendigen Identifizierungsanforderungen hingewiesen und informierte ihre Mitarbeiter entsprechend.

Vor im Einzelfall zulässig erteilten Melderegisterauskünften ist es im Interesse des Schutzes der allgemeinen Persönlichkeitsrechte der Bürger notwendig, eine zweifelsfreie Identifizierung der Person sicherzustellen, über deren Daten dann Auskunft erteilt wird.

5.5 Personaldaten

5.5.1 Privater Ermittlungsführer in einem Disziplinarverfahren?

Eine Behörde hat zur Durchführung disziplinarischer Ermittlungen einen externen Rechtsanwalt beauftragt. Durfte sie das?

Das Landesdisziplinargesetz (LDG) sagt nichts darüber aus, wer die tatsächlichen Ermittlungen innerhalb eines Disziplinarverfahrens durchzuführen hat. Laut § 17 LDG stehen die Disziplinarbefugnisse den zuständigen Dienstvorgesetzten in den Behörden und Einrichtungen zu. Es ist strittig, inwieweit mit der Durchführung der Ermittlungstätigkeit auch private Dritte, insbesondere Rechtsanwälte, beauftragt werden können. Teilweise wird die Auffassung vertreten, dass dieses durch einen öffentlich-rechtlichen Vertrag zulässig ist, soweit die Weisungsgebundenheit letztlich bei dem die Ermittlung in Auftrag gebenden Dienstvorgesetzten verbleibt. Begründet wird die Ansicht damit, dass Ermittlungsverfahren nicht die alltägliche Daueraufgabe der Dienststelle und ihr das Vorhalten entsprechender Personalressourcen nicht zumutbar seien.

Wir halten eine solche Beauftragung für unzulässig. Disziplinarverfahren und ihre bis zur Entlassung aus dem Dienstverhältnis reichenden Folgen, sind erhebliche Eingriffe in Grundrechte und dürfen aus diesem Grunde nur dann auf Private delegiert werden, wenn dieses ausdrücklich durch ein Gesetz geregelt ist. Eine entsprechende Regelung findet sich jedoch im Disziplinarrecht nicht.
Gleiches gilt für die mit einem Disziplinarverfahren verbundene Verarbeitung personenbezogener Daten. Sie stellt einen Grundrechtseingriff dar und ist deshalb nur im überwiegenden Allgemeininteresse oder auf Grund eines Gesetzes im Rahmen der darin festgelegten Zwecke zulässig. Dies bedeutet, dass nur derjenige Daten verarbeiten darf, der dazu eine solche Befugnis erhalten hat.

Die dem förmlichen Disziplinarverfahren vorgelagerte Sachaufklärung erfordert gleichfalls das Verarbeiten personenbezogener Daten. Der Dienstvorgesetzte ist nicht gezwungen, diese selbst vorzunehmen. Er kann sie vielmehr delegieren. Der zu diesem Zweck eingesetzte Ermittlungsführer bleibt dann ein nachgeordneter und weisungsgebundener Gehilfe des verantwortlichen Dienstvorgesetzten. Die Übertragung der Ermittlungstätigkeit auf einen selbstständig handelnden Privaten ist von vornherein ausgeschlossen. Das Bundesverwaltungsgericht[46] hat in anderem Zusammenhang entschieden, dass Verträge im öffentlichen Dienstrecht, die die Kernbereiche des Beam-

[46] BVerwGE 91, 200, 203

tenrechts betreffen, unzulässig sind. Die Sachaufklärung im Disziplinarverfahren zielt jedoch letztlich auf eine Entscheidung über den Status des betroffenen Beamten und berührt damit den Kernbereich des Beamtenrechts, ihre Übertragung zur eigenständigen Erledigung ist damit nicht zulässig.

Die Durchführung eines Disziplinarverfahrens ist ein grundrechtlicher Eingriff, der den Kern des Dienstverhältnisses berührt. Die Übertragung der Ermittlungstätigkeit auf einen selbstständigen und weisungsfreien Privaten ist daher unzulässig.

5.5.2 Revierpolizisten im Internet

Das Ministerium des Innern plante, dienstliche Kontaktdaten der Revierpolizisten in das Internetangebot der Polizei, die Internetwache, einzustellen. Vorgesehen war die Veröffentlichung des Namens und Vornamens, des Dienstgrades, der Dienstausweisnummer und eines Passbildes verbunden mit Informationen zur örtlichen und telefonischen Erreichbarkeit.

Mit der Veröffentlichung sollte die Bekanntheit der Revierpolizisten als Ansprechpartner für die lokale Öffentlichkeit in ihrem jeweiligen Zuständigkeitsbereich verbessert und die Kontaktaufnahme erleichtert werden.

Aus datenschutzrechtlicher Sicht ist die mit dem Einstellen in das Internet verbundene Übermittlung der Personaldaten ohne besondere Einwilligung der Beamten nur zulässig, wenn der Empfänger ein rechtliches Interesse an diesen Informationen hat oder der Dienstverkehr die Übermittlung erfordert. Die Veröffentlichung der in Frage stehenden Personaldaten ist insbesondere erforderlich, wenn die Betroffenen auf Grund ihrer besonderen dienstlichen Funktionen persönlich als Ansprechpartner für die Öffentlichkeit zur Verfügung stehen sollen. Diese Voraussetzung ist auf Grund der Aufgaben bei Revierpolizisten grundsätzlich gegeben. Sie fungieren gegenüber Bürgern, Unternehmen, Vereinen oder anderen Institutionen als Ansprechpartner. Gegen die Veröffentlichung von Dienstgrad, Name, Vorname und Angaben zur Erreichbarkeit (einschließlich Telefondurchwahl oder ggf. dienstlicher E-Mail-Adresse) auch ohne eine ausdrückliche Einwilligung bestehen keine datenschutzrechtlichen Bedenken.

Anders verhält es sich mit den Fotos der Revierpolizisten, deren Verbreitung ohne Einwilligung nicht zulässig ist. Ein dienstliches Erfordernis dafür ist nicht erkennbar. Auch das berechtigte Interesse der Polizei, dass ihre Revierpolizisten möglichst einfach erreichbar sein sollen, rechtfertigt nicht die Veröffentlichung von Fotos. Sie ist ein wesentlich stärkerer Eingriff in die Persönlichkeitsrechte als das Bekanntmachen bloßer dienstlicher Kontaktinformationen.

Ohne Einwilligung verletzt sie außerdem auch das durch das Kunsturhebergesetz geschützte Recht am eigenen Bild.

Das Ministerium des Innern hatte es zwar einerseits für notwendig gehalten, die Einwilligung der Revierpolizisten einzuholen. Auf der anderen Seite haben die Polizeipräsidien aber erheblichen Druck auf die Beamten ausgeübt, die Einwilligung auch zu erteilen. Ein Polizeipräsidium hat sogar damit gedroht, die Beamten im Falle ihrer Verweigerung von der Funktion des Revierpolizisten zu entbinden. Eine Einwilligung ist jedoch nur dann wirksam, wenn sie freiwillig und ohne jeden Zwang abgegeben wird und auch jederzeit ohne Gründe für die Zukunft widerrufbar ist. Davon konnte angesichts des Drucks, dem die Beamten ausgesetzt waren, keine Rede mehr sein.

Das Ministerium des Innern teilt unsere Rechtsauffassung und hat durch einen Erlass sichergestellt, dass Passbilder von Revierpolizisten nur noch auf Grund der ausdrücklichen und jederzeit widerrufbaren Einwilligung in das Internetangebot aufgenommen werden. Den Beamten darf bei der Verweigerung oder dem Widerruf der Einwilligung kein Nachteil entstehen. Auch bei bereits erteilten Einwilligungen haben die Revierpolizisten die Möglichkeit, sie zu widerrufen.

Fotos von Beschäftigten dürfen nur mit deren Einwilligung in das Internetangebot eingestellt werden. Die Einwilligung ist nur wirksam, wenn sie ohne jeden Zwang erteilt und jederzeit ohne Angabe von Gründen verweigert oder widerrufen werden kann.

5.6 Statistik und Wahlen: Fusion der Statistikämter von Berlin und Brandenburg

Im Dezember 2003 vereinbarten die Innenverwaltungen von Berlin und Brandenburg eine Neuordnung der Aufgaben Statistik und Informationstechnik. Ende 2004 wurde ein erster Entwurf für einen Staatsvertrages zur Fusion der beiden statistischen Landesämter zu einer gemeinsamen Anstalt des öffentlichen Rechts vorlegt. Im Dezember 2005 wurde der Staatsvertrag von beiden Ländern unterzeichnet.

Hintergrund dieser Zusammenführung waren die Empfehlungen der Rechnungshöfe des Bundes und der Länder zur Wirtschaftlichkeit des öffentlichen Statistikwesens in Deutschland. Derzeit gibt es in fast jedem Bundesland ein eigenes statistisches Landesamt. Dies ist damit begründet, dass die amtliche Statistik nach föderalen Gesichtspunkten aufgebaut ist und die Daten und Analysen auf regionale Erfordernisse abgestellt sind. Mit der Bildung einer gemeinsamen Anstalt sollen die Effizienz der amtlichen Statistik verbessert sowie Personal- und Sachkosten eingespart werden.

Im Jahr 2004 hat eine Projektgruppe beider Innenverwaltungen und der statistischen Landesämter die Umsetzungsmöglichkeit zur Intensivierung der Zusammenarbeit der Statistischen Landesämter von Berlin und Brandenburg untersucht. Ende 2004 lag der erste Entwurf für einen Staatsvertrag mit dem Ziel der Fusion der Landesämter zu einer gemeinsamen Anstalt des öffentlichen Rechts vor. Seit Juli 2005 wurden wir regelmäßig an den Beratungen der Projektgruppe beteiligt. Im Staatsvertrag ist u. a. vorgesehen, dass die gemeinsame Anstalt mit der Bezeichnung „Amt für Statistik Berlin-Brandenburg“ ihren Sitz in Potsdam haben und als weitere Standorte Berlin und Cottbus unterhalten wird. Für die Verarbeitung personenbezogener Daten durch die Anstalt gelten die entsprechenden Vorschriften des Landes Brandenburg. Die Kontrolle des in Berlin gelegenen Teils der Anstalt kann auch durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit erfolgen. Der Vertrag wurde am 13. Dezember 2005 unterschrieben und tritt frühestens am 1. Januar 2007 in Kraft.

Im Staatsvertrag zwischen den Länder Berlin und Brandenburg über die Einrichtung eines gemeinsamen Amtes für Statistik ist das Datenschutzrecht angemessen berücksichtigt worden.

5.7 Kommunales

5.7.1 Verhaltenskontrolle – Übermittlung von Daten eines Stadtverordneten an Arbeitgeber

Ein Stadtverordneter einer kreisfreien Stadt beantragte Einsicht in Unterlagen der Stadtverwaltung. Die Stadt informierte daraufhin unter anderem den ihr bekannten Arbeitgeber des Stadtverordneten über das aus ihrer Sicht nicht angemessene Verhalten des Stadtverordneten. Der Arbeitgeber drohte dem Kommunalvertreter mit arbeitsrechtlichen Schritten.

Die Weitergabe von Informationen über das Verhalten des Stadtverordneten an dessen Arbeitgeber war mangels datenschutzrechtlicher Rechtsgrundlage unzulässig. Weder die Gemeindeordnung noch das Brandenburgische Datenschutzgesetz sehen für eine solche Übermittlung personenbezogener Daten eine Befugnis vor.

Die Übermittlung der Daten an den Arbeitgeber war weder für die Erfüllung der Aufgaben der Stadtverwaltung noch für die des Arbeitgebers erforderlich. Stadtverordnete und Gemeindevertreter müssen die Möglichkeit haben, ihr in der Kommunalverfassung garantiertes Recht auf Akteneinsicht ohne jede Mitwirkung oder Information des Arbeitgebers auszuüben.

Die Kommunalverfassung legt ausdrücklich fest, dass die kommunalen Vertreter aufgrund ihrer Tätigkeit nicht in ihrem Dienst- oder Arbeitsverhältnis benachteiligt werden dürfen. Dieses Benachteiligungsverbot ist für die Ausübung eines Mandates gerade angesichts der grundsätzlich bestehenden wirtschaftlichen Abhängigkeit eines Arbeitnehmers von seinem Arbeitgeber von erheblicher Bedeutung.

Im vorliegenden Fall sind vorhandene personenbezogene Informationen unzulässigerweise für verwaltungsfremde Zwecke eingesetzt worden. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat diesen schwerwiegenden Verstoß gegen datenschutzrechtliche Bestimmungen förmlich beanstandet.

Kommunale Verwaltungen dürfen Arbeitgeber von Mitgliedern kommunaler Vertretungen über deren Verhalten im Zusammenhang mit der Ausübung ihres Mandats nicht informieren.

5.7.2 Datenschutz im Vollstreckungsverfahren

Kommunalverwaltungen sind oft unsicher, in welchem Umfang sie personenbezogene Daten, die in ihrer Kommune an verschiedenen Stellen vorhanden sind, auch zu Zwecken der Vollstreckung öffentlich-rechtlicher Forderungen nutzen dürfen.

Die Kommunen und ihre Verwaltungen haben die Pflicht, offene Forderungen einzutreiben. Sie wollen daher Informationen über ihre Schuldner aus unterschiedlichen Organisationseinheiten der Kommune in einem möglichst weiten Umfang nutzen, etwa um eine aktuelle Anschrift zu erhalten, an die dann ein Kosten- oder Vollstreckungsbescheid zugestellt werden kann.

Personenbezogene Daten unterliegen auch in der Kommunalverwaltung dem Grundsatz der Zweckbindung. Sie können grundsätzlich nur für solche Zwecke verarbeitet werden, für die sie erhoben wurden. Daten aus der Sozialverwaltung einer Gemeinde können daher nicht beliebig umgewidmet und durch andere Stellen der Gemeinde verwendet werden. Das setzt auch der Verarbeitung personenbezogener Daten im Vollstreckungsverfahren enge Grenzen: Vorhandene Daten dürfen bei geringfügigen Außenständen nur der Vollstreckung von Forderungen dienen, die aus dem vorangegangenen Lebenssachverhalt stammen.

Eine Kommune, die ein Bußgeld wegen Falschparkens vollstrecken und hierfür einen Teil des Gehalts des Schuldners pfänden will, darf beispielsweise eine vorliegende Verdienstbescheinigung, die sie auf Grund eines Kindergar-

tenbetreuungsvertrages angefordert hat, nicht nutzen. Die darin enthaltenen Angaben über den Arbeitgeber können daher nicht für die Vollstreckung einer Forderung herangezogen werden, die wegen eines völlig anderen Grundes – hier wegen eines Verstoßes gegen die Straßenverkehrsordnung – besteht. Gleiches gilt im Falle der Vollstreckung von Straßenreinigungsgebühren, wenn die Kontoverbindung durch Erteilung einer Einzugsermächtigung für die Zahlung von Musikschulgebühren bekannt wurde. Auch das ist grundsätzlich unzulässig, da der Schuldner die Kontoverbindung nur zum Zweck der Zahlung bestimmter Gebühren bekannt gab. Wenn ein Landkreis ausstehende Abfallgebühren durch Pfändung eines Kontos vollstreckt, das der Schuldner bereits zu einem früheren Zeitpunkt zur Zahlung von Abfallgebühren angegeben hatte, ist der Sachverhalt dagegen anders zu beurteilen. Hier erfolgt die Nutzung der Daten zu dem gleichen Zweck, für den sie ursprünglich erhoben wurden, nämlich der Zahlung der Abfallgebühren.

Erst wenn die Höhe von Forderungen über ein Mindestmaß hinausgeht und durch ihre Höhe erhebliche Nachteile für das Gemeinwohl drohen, kann die strikte Zweckbindung durchbrochen werden. Dann ist unter Beachtung des Grundsatzes der Verhältnismäßigkeit eine Güterabwägung zwischen den Rechten der Betroffen einerseits und den Interessen der Allgemeinheit sowie dem Gebot der Gleichbehandlung andererseits vorzunehmen. Letzteres verlangt auch, dass alle säumigen Zahler gleichermaßen herangezogen werden. Wann diese Höhe konkret erreicht ist, richtet sich nach dem jeweiligen Einzelfall.

Bei der Vollstreckung öffentlich-rechtlicher Forderungen ist der Grundsatz der Zweckbindung zu beachten. Nur bei hohen Forderungen ist eine Nutzung von personenbezogenen Daten, die ursprünglich einer anderen Zweckbestimmung dienten, zulässig.

5.7.3 Ratsinformationssystem einer Stadtverwaltung

Eine Stadtverwaltung informierte uns über ihre Absicht, ein datenbankgestütztes Informationssystem zur Unterstützung der Arbeit der Stadtverordnetenversammlung, der Ausschüsse und Fraktionen sowie für deren öffentliche Darstellung zu realisieren. Sie bat uns um eine Stellungnahme aus Sicht des Datenschutzes und der Datensicherheit.

Das zu entwickelnde System sollte einerseits als reines Informationssystem personenbezogene Daten der Abgeordneten für die Öffentlichkeit bereitstellen sowie die Tagesordnungen, Vorlagen, Anträge, Anfragen und Protokolle der Sitzungen der Gremien elektronisch verfügbar machen und Verknüpfungen dieser Dokumente untereinander gestatten. Andererseits sollte ein Nachrichtensystem für den Austausch von Mitteilungen und die asynchrone Ko-

operation innerhalb der Gremien eingeführt werden. Eine Besonderheit des Systems war, dass auch nicht öffentliche Dokumente verarbeitet und berechtigten Nutzern über das Internet bereitgestellt werden sollten.

Aus datenschutzrechtlicher Sicht bestehen zumindest bezüglich der Verarbeitung und elektronischen Publikation der öffentlichen Dokumente der Stadtverordnetenversammlung und ihrer Gremien keine Einwände. Gleiches gilt auch für bestimmte personenbezogene Daten der Abgeordneten wie deren Name, Zugehörigkeit zu Parteien, Fraktionen, Ausschüssen und die Funktion innerhalb der Gremien sowie Kontaktdaten (Adresse, Telefon- und Faxnummer), falls diese innerhalb der Stadtverwaltung liegen. Für die Veröffentlichung darüber hinaus gehender persönlicher Daten der Abgeordneten wie Foto, Privatanschrift oder Lebenslauf ist eine Einwilligung der Betroffenen erforderlich. Es ist zu begrüßen, dass die Stadtverwaltung einen Zustimmungsvorbehalt ermöglichte.

Bezüglich der Verfügbarmachung von nicht öffentlichen Dokumenten aus der Arbeit der Stadtverordnetenversammlung ist zu beachten, dass diese Dokumente vor unberechtigter Kenntnisnahme zu schützen sind. Dies erfordert, den Zugriff auf diese Dokumente nur auf berechtigte Nutzer zu beschränken, die sich gegenüber dem System identifizieren und authentifizieren müssen. Weiterhin sind die Dokumente bei ihrer Übertragung über das Internet zu verschlüsseln. Für die Rechner (Client, Webserver, Datenbankserver) sind grundlegende technisch-organisatorische Schutzmaßnahmen zu realisieren (z. B. in Anlehnung an das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik).

Besondere, weiter gehende Sicherheitsmaßnahmen sind dann umzusetzen, wenn die nicht öffentlichen Dokumente personenbezogene Daten hoher Sensitivität enthalten. Dies ist z. B. der Fall bei Personaldaten oder Daten, die unter das Sozial- oder Steuergeheimnis fallen. Die Verarbeitung derartiger Dokumente erfordert z. B. eine verschlüsselte Speicherung in der Datenbank, eine Ende-zu-Ende-Verschlüsselung bis auf Anwendungsebene bei der Netzwerkübertragung sowie eine detaillierte Protokollierung erfolgreicher Zugriffe bzw. misslungener Zugriffsversuche.

Das uns vorgelegte Konzept für das zu entwickelnde Ratsinformationssystem sah keine Einschränkungen bzgl. der genannten Arten von Dokumenten vor. Die entsprechenden Anforderungen zur Gewährleistung des Datenschutzes und der Datensicherheit wurden nur teilweise berücksichtigt. Insbesondere fanden sich keine hinreichenden Vorkehrungen für die Verarbeitung von Dokumenten mit hochsensitiven personenbezogenen Daten (z. B. bei der Behandlung von Personalangelegenheiten).

Nach intensiven Diskussionen mit Vertretern unserer Behörde und der Abwägung verschiedener Lösungsvarianten entschieden die Projektverantwortlichen, mit dem System nur noch öffentliche Dokumente der Stadtverordnetenversammlung zu verarbeiten bzw. personenbezogene Daten der Abgeordneten bereitzustellen. Den Aufwand zur Erfüllung der Sicherheitsanforderungen für den ursprünglich geplanten Funktionsumfang schätzten sie als zu hoch ein. Die Vorteile des Ratsinformationssystems sind damit nur noch für einen Teil der Arbeit der Stadtverordnetenversammlung nutzbar.

Gleichwohl sind natürlich auch bei dem eingeschränkten Datenumfang die Bestimmungen des Brandenburgischen Datenschutzgesetzes zu beachten, insbesondere § 7 Abs. 3 zur Erstellung eines Sicherheitskonzepts. Der Argumentation der Stadtverwaltung, dass nun keine schutzbedürftigen personenbezogenen Daten mehr verarbeitet würden, konnten wir nicht folgen. Personenbezogene Daten sind per Gesetz schutzbedürftig. Nach einem regen Schriftwechsel zu diesem Thema sagte uns die Stadtverwaltung die Erstellung der entsprechenden Unterlagen zu.

Die Klärung der Zulässigkeit der Verarbeitung personenbezogener Daten und deren geringe Sensitivität entheben eine öffentliche Daten verarbeitende Stelle nicht der Verpflichtung, ein Sicherheitskonzept mit technischen und organisatorischen Maßnahmen zur Gewährleistung der Integrität und Verfügbarkeit der Daten zu erarbeiten und umzusetzen.

5.8 Sonstiges: Befugnisse behördlicher Datenschutzbeauftragter

Unsicherheiten bestehen darüber, in welchem Umfang behördliche Datenschutzbeauftragte personenbezogene Daten verarbeiten dürfen. Insbesondere ist offen, ob sie auch ohne die Einwilligung von Betroffenen Zugang zu sensitiven Informationen wie Personalakten, Sozialdaten oder Gesundheitsdaten haben. Darüber hinaus ist gelegentlich nicht klar, welche personelle und sachliche Unterstützung die behördlichen Datenschutzbeauftragten durch die Dienststelle beanspruchen können.

Behördliche Datenschutzbeauftragte sollen sicherstellen, dass die datenschutzrechtlichen Bestimmungen praxisgerecht eingehalten werden. Sie haben gestützt auf § 7a Brandenburgisches Datenschutzgesetz (BgbDSG) die Befugnis, alle personenbezogenen Unterlagen einzusehen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist und keine gesetzlichen Vorschriften entgegenstehen. Danach können dem behördlichen Datenschutzbeauftragten auch keine besonderen Amtsgeheimnisse entgegengehalten werden. Dies bedeutet, dass er im Rahmen seiner Aufgaben das Recht hat, Personalakten einzusehen oder solche Daten zur Kenntnis zu nehmen, die dem Sozialge-

heimnis oder dem Steuergeheimnis unterliegen. Eine Einwilligung der Betroffenen muss er dabei nicht einholen. Gerade bei der Einsichtnahme von Personalakten sollte der behördliche Datenschutzbeauftragte allerdings schon aus vertrauensbildenden Gründen immer auch versuchen, das Einverständnis der Betroffenen einzuholen. Zur Klarstellung sollten die Befugnisse zudem bereits in seinem Bestellungsschreiben benannt werden.

In Unterlagen, die wie die ärztliche Schweigepflicht einem Berufsgeheimnis unterliegen, darf er dagegen nicht ohne weiteres Einsicht nehmen. Die ärztliche Schweigepflicht obliegt als höchstpersönliche berufsbedingte Geheimhaltungspflicht dem Arzt selbst. Wenn die Betroffenen nicht ausdrücklich eingewilligt haben oder die behördlichen Datenschutzbeauftragten nicht als ärztliche Gehilfen mit der Einsichtnahme beauftragt sind, können sie in Krankenhäusern oder Gesundheitsämtern deshalb nur ausnahmsweise Gesundheitsdaten einsehen. Dies könnte etwa gegeben sein, wenn es um die sichere Verwahrung aufgefundener Unterlagen geht, die Gesundheitsdaten enthalten. Die Verschwiegenheitspflicht des behördlichen Datenschutzbeauftragten besteht auch gegenüber der Dienststellenleitung.

Zwar muss die Daten verarbeitende Stelle dem behördlichen Datenschutzbeauftragten die erforderliche personelle und sachliche Unterstützung gewähren, doch ist diese Verpflichtung nicht ausdrücklich im Brandenburgischen Datenschutzgesetz festgelegt. Sie folgt jedoch aus den gesetzlichen Aufgaben des behördlichen Datenschutzbeauftragten. Gerade bei hochkomplexen automatisierten Verfahren oder bei rechtlich schwierigen Sachverhalten kann die Fachkunde des behördlichen Datenschutzbeauftragten nicht immer ausreichen. Er wird deshalb häufig auf die Hilfe des Fachpersonals, z. B. eines Systemverwalters, angewiesen sein. Er muss insoweit befugt sein, diese jederzeit ansprechen und um Rat fragen zu können.

Behördliche Datenschutzbeauftragte dürfen in einem weiten Umfang auch sensitive personenbezogene Daten verarbeiten, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Die öffentlichen Stellen haben sie personell und sachlich zu unterstützen. Weitere Informationen zu diesem Thema können unserem Internetangebot entnommen werden.

6 Justiz

6.1 Auskunft über bei Gericht anhängige Verfahren Dritter

Ein Gläubiger möchte bei der Geschäftsstelle eines Gerichtes erfahren, ob sein Schuldner vor diesem Gericht Prozesse führt. Er beabsichtigt, diese Informationen zur Eintreibung seiner Außenstände zu verwenden.

Der Umstand, dass jemand einen Prozess vor einem Gericht führt, stellt zweifelsfrei ein personenbezogenes Datum dar. Um dieses zu offenbaren, bedarf es einer rechtlichen Grundlage, wofür auch das Akteneinsichts- und Informationszugangsgesetz in Frage kommt. Es gilt prinzipiell auch für die Verwaltungstätigkeit eines Gerichts, die nicht unmittelbar die richterliche Tätigkeit betrifft. Im vorliegenden Fall bezogen sich die gewünschten Angaben aber auf laufende Verfahren, die nicht unter den Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes fallen.

Allerdings ist das Brandenburgische Datenschutzgesetz (BbgDSG) auf die Datenverarbeitung in der Gerichtsverwaltung anzuwenden. Es unterscheidet dabei nicht zwischen abgeschlossenen und laufenden Verfahren. Eine Übermittlung von personenbezogenen Daten ist zulässig, wenn sie „aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte“. Die Namen der Prozessbeteiligten, die Aktenzeichen sowie die den Verfahrensgegenstand betreffenden Angaben, zählen im Rahmen des Grundsatzes der Öffentlichkeit des gerichtlichen Verfahrens nach § 169 Gerichtsverfassungsgesetz zu den unabdingbaren „Rahmendaten“ eines jeden gerichtlichen Verfahrens. Sie werden mindestens per Aushang innerhalb des Gerichts veröffentlicht. Termindaten werden im Rahmen der Öffentlichkeitsarbeit der Gerichte nicht nur in der Presse, sondern auch im Internet (z. B. Amtsgericht Potsdam) verbreitet. Begrenzt wird diese Befugnis lediglich für den Fall, dass das Geheimhaltungsinteresse des Betroffenen offensichtlich überwiegt. Das Vorliegen eines solchen Interesses müsste nach den Maßstäben des Gerichtsverfassungsgesetzes für die Anordnung der Nichtöffentlichkeit eines Verfahrens beurteilt werden. Im Grundsatz ist aber von der Öffentlichkeit der Gerichtsverhandlung auszugehen. Daher stößt die entsprechende Auskunft eines Gerichts nicht auf rechtliche Bedenken. Etwas anderes gilt beispielsweise für Familien- oder Jugendstrafsachen, die besonderen Einschränkungen hinsichtlich der Öffentlichkeit der Verhandlung unterliegen.

Besondere schützenswerte Interessen i. S. v. § 13 Abs. 2 Buchstabe f BbgDSG, die eine andere Wertung im konkreten Einzelfall verlangen, waren im vorliegenden Fall nicht ersichtlich. Das wirtschaftliche Interesse des Auskunftsersuchenden, seine ausstehenden Forderungen einzutreiben, ist gegenüber dem Geheimhaltungsinteresse der Prozessbeteiligten, als höherrangig zu bewerten. Dies gilt umso mehr als die in Frage stehenden Daten ohnehin im Rahmen der Terminankündigung öffentlich bekannt zu geben sind.

Gerichtsverwaltungen dürfen die Beteiligten an öffentlich verhandelten Gerichtsterminen nennen. Dieses folgt aus dem Grundsatz der Öffentlichkeit von Gerichtsverhandlungen und verstößt im Allgemeinen nicht gegen die Rechte der Beteiligten. Ausnahmen können für Verfahren gelten, bei denen wie in Familien- oder Jugendsachen die Öffentlichkeit von der Verhandlung ausgeschlossen ist.

6.2 Versand der vollständigen Schriftsätze aus einem Scheidungsverfahren vom Gericht ans Jugendamt

Anlässlich von Scheidungsverfahren übermittelte ein Gericht in den Fällen, in denen auch minderjährige Kinder betroffen waren, die kompletten Schriftsätze der beteiligten Parteien an die Jugendhilfeabteilungen der jeweils örtlich zuständigen Jugendämter. War dies zulässig?

Es gehört zu den Aufgaben der Jugendhilfe, Eltern zu beraten und ihnen dabei zu helfen, ein partnerschaftliches Zusammenleben in der Familie aufzubauen oder Konflikte zu bewältigen. Im Falle der Trennung oder Scheidung sollen sie Bedingungen für eine dem Wohl des Kindes förderliche Wahrnehmung der elterlichen Sorge schaffen. Deshalb sind die Gerichte entsprechend § 17 Abs. 3 Achtes Buch Sozialgesetzbuch befugt, den Jugendämtern die Anhängigkeit von Scheidungssachen sowie die Namen und Anschriften der Parteien mitzuteilen. Die Jugendämter sollen dadurch die Gelegenheit erhalten, die Eltern über das Beratungsangebot der Jugendhilfe zu informieren. Die Eltern können eigenständig darüber entscheiden, ob sie von dem Angebot Gebrauch machen. Sie treten selbst an die Jugendhilfe heran und bestimmen, was sie von sich und dem Scheidungsverfahren offenbaren wollen. Die Ämter sollen zu diesem frühen Zeitpunkt noch keine näheren Informationen aus dem Scheidungsverfahren erhalten. Die komplette Weitergabe der anwaltlichen Schriftsätze bedeutet dem gegenüber die Preisgabe einer Vielzahl von teilweise sehr persönlichen Details aus dem Leben der Beteiligten und geht damit weit über die zulässige Mitteilung der oben genannten Umstände hinaus.

Das angesprochene Gericht teilte unsere Auffassung zur Auslegung der Vorschriften des Achten Buch Sozialgesetzbuch und stellte durch eine entsprechende interne Weisung für zukünftige Fälle klar, dass im Rahmen eines Scheidungsverfahrens nicht mehr Kopien der kompletten Schriftsätze an die Jugendämter weitergegeben werden.

Um über Beratungsmöglichkeiten zu informieren und in einer Scheidungssituation für betroffene Familien ein Hilfsangebot zu unterbreiten, reichen die Adressen der an einem Scheidungsverfahren beteiligten Eltern aus. Eine routinemäßige Weitergabe kompletter Schriftsätze ist für diesen Zweck weder erforderlich noch zulässig.

7 Bildung, Jugend und Sport

7.1 Modernisierung der Software zur Personalverwaltung in Schulämtern

In mehreren zurückliegenden Tätigkeitsberichten[47] hatten wir zum Einsatz des Personalinformationssystems APSIS – Automatisierte Personalverwaltung und Stellenbewirtschaftung im Schulamt – Stellung genommen. Nun informierte uns das Ministerium für Bildung, Jugend und Sport (MBJS) über die geplante Einführung einer grundlegend überarbeiteten, modernisierten Version dieser Software.

APSIS wird in den sechs staatlichen Schulämtern des Landes Brandenburg zur automatisierten Verarbeitung der Personaldaten von Lehrkräften und der Daten von Bewerbern für den Schuldienst sowie zur Stellenbewirtschaftung eingesetzt. Es dient außerdem zur Erstellung von Statistiken und Berichten für das MBJS.

Die neue Version der Software wurde in enger Kooperation zwischen den Schulämtern und dem Bildungsministerium entwickelt. Entstanden ist ein komplexes, verteiltes Client/Server-System, das sich u. a. durch die Nutzung moderner Elemente der Datenverarbeitung auszeichnet, insbesondere eine Drei-Schichten-Architektur, eine webbasierte Benutzerschnittstelle sowie vielfältige technische Maßnahmen zur Gewährleistung von Datenschutz und IT-Sicherheit. Letzteren kommt bei der Verarbeitung von Personaldaten als sensitiven personenbezogenen Daten mit hohem Schutzbedarf eine besondere Bedeutung zu. Bei APSIS sind in diesem Zusammenhang z. B. hervorzuheben:

- die verschlüsselte Speicherung der Daten in der Datenbank,
- die Verschlüsselung der Daten beim Transport über das Landesverwaltungsnetz,
- die Abschottung von Teilnetzen durch restriktiv konfigurierte Firewalls sowie

[47] vgl. Tätigkeitsbericht 1997/98, A 13.2.1 und Tätigkeitsbericht 1999, A 2.1.2

- die Einrichtung von Nutzergruppen mit differenzierten, aufgabenbezogenen Zugriffsrechten.

Ungeachtet der genannten datenschutzgerechten Eigenschaften von APSIS gab es zunächst noch einige offene Punkte, die jedoch in der Zwischenzeit mit den verantwortlichen Mitarbeitern im Bildungsministerium bzw. in den Schulämtern geklärt werden konnten. Die Fragen betrafen z. B. die Trennung der Personaldatenbestände der sechs Schulämter, die Protokollierung von Zugriffen und die Auswertung der Protokolle sowie die Löschung nicht mehr benötigter personenbezogener Daten. Da die APSIS-Serversoftware physisch auf Rechnern im Landesbetrieb für Datenverarbeitung und Statistik läuft, werden jetzt die bereits bestehenden Servicevereinbarungen für APSIS um vertragliche Festlegungen zur Datenverarbeitung im Auftrag ergänzt. Weiterhin wurde uns zugesagt, Verfahrensweisen zur Wartung und Pflege der Software in den Projektregularien festzuschreiben.

Das Beispiel APSIS zeigt, dass bei der Modernisierung oder Neukonzipierung eines Softwaresystems die Beachtung von Anforderungen des Datenschutzes und der IT-Sicherheit bereits in frühen Projektphasen erhebliche Vorteile gegenüber ihrer nachträglichen Integration bietet.

7.2 Gestaltung von Schuljahrbüchern und deren Veröffentlichung

Im Rahmen der Gestaltung eines Schuljahrbuches wurden wir gefragt, ob für die Veröffentlichung von Bildern von Schülern und Lehrkräften die schriftliche Einwilligung der Abgebildeten vorliegen muss und welche Voraussetzungen bei der Veröffentlichung auf der Schul-Homepage zu beachten sind.

Auch Bilder, die einzelne Personen erkennen lassen, sind personenbezogene Daten. Die Datenverarbeitung in Schulen richtet sich nach § 65 Brandenburgisches Schulgesetz, welches wiederum auf die Vorschriften des Brandenburgischen Datenschutzgesetzes (BbgDSG) verweist.

Die Erstellung von Jahrbüchern und Homepages fallen nicht wie der Unterricht oder die Prüfungen selbst in den Kernbereich der schulischen Tätigkeit. Die Mitwirkung und vor allem die Aufnahme von Bildern darin sind daher freiwillig und bedürfen der ausdrücklichen Zustimmung der Abgebildeten. Es gelten in jedem Einzelfall die Anforderungen für die Einwilligung nach § 4 BbgDSG. Sie bedarf i. d. R. der Schriftform und setzt voraus, dass die Betroffenen ausreichend über die geplante Verwendung der Bilder informiert werden. Selbstverständlich ist sie freiwillig und im Falle ihrer Verweigerung dürfen daraus keine Nachteile entstehen. Bei Minderjährigen ist zusätzlich die

Einwilligung der Eltern einzuholen. Auch kann sie jederzeit widerrufen werden, was im Falle der Verwendung von Bildern im Internetangebot der Schule zu ihrer Löschung führen muss. Damit ist jedoch nicht ausgeschlossen, dass die Bilder nicht bereits auf anderen Wegen im Internet verbreitet wurden.

Für die Gestaltung von Homepages sind neben den datenschutzrechtlichen Aspekten auch urheberrechtliche Vorschriften zu beachten.

Die Verwendung von Bildmaterial in einem Schuljahrbuch oder im Internetangebot einer Schule bedarf der Einwilligung der Abgebildeten. Weitere Tipps zur datenschutzgerechten Gestaltung der Websites von Schulen gibt das Faltblatt „Schulen, Internet und Datenschutz“, das auch unter www.lda.brandenburg.de abgerufen werden kann.

7.3 Der Lebenslauf im Deutschunterricht

Im Unterricht einer Schule wurde das Abfassen von Lebensläufen geübt. Auf Wunsch seiner Eltern verfasste ein Schüler seinen Lebenslauf ohne konkrete Angaben über die weiteren Familienmitglieder. Mit dem Hinweis, dass es im Lebenslauf keinen Datenschutz gibt, wurde die Arbeit schlecht benotet.

Die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern und deren Eltern richtet sich nach § 65 Brandenburgisches Schulgesetz. Personenbezogene Daten dürfen verarbeitet werden, soweit dies zur rechtmäßigen Erfüllung des Erziehungs- und Bildungsauftrages der Schule und zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. In einem so genannten Schülerstammblatt dürfen u. a. auch Name und Vorname der Erziehungsberechtigten und deren Anschriften festgehalten werden. Eine über diesen Umfang hinausgehende Erhebung personenbezogener Daten über die Familienmitglieder der Schülerinnen und Schüler wäre nur dann zulässig, wenn sie zur Erfüllung des Erziehungs- und Bildungsauftrages der Schule erforderlich wäre.

Im vorliegenden Fall fehlte es an dem Tatbestandsmerkmal der Erforderlichkeit. Zwar sind auch Unterrichtseinheiten zulässig, in die Angaben über das persönliche Umfeld der Schüler oder ihrer Familienangehörigen einfließen sollen, doch müssen dabei die Persönlichkeitsrechte der Betroffenen berücksichtigt werden. Wollen die Eltern nicht, dass Daten aus ihren Lebensläufen bekannt werden, ist es ihnen unbenommen, ihre Angaben nicht zur Verfügung zu stellen. Ihnen und vor allem ihren Kindern dürfen, wenn die Abfassung eines Lebenslaufs Gegenstand einer Benotung wird, daraus keinerlei Nachteile entstehen. Die Abfassung eines Lebenslaufs kann ohne weiteres

auch mit Phantasie-Daten trainiert werden. Eine Leistungsbewertung, die sich auf das Fehlen von Echtdaten stützt, ist rechtsfehlerhaft.

Datenschutz umfasst auch Angaben der Familie. Schülerinnen und Schüler sind nicht verpflichtet, in einem zu Übungszwecken angefertigten Lebenslauf Daten von Familienmitgliedern preiszugeben.

8 Wissenschaft, Forschung und Kultur

8.1 Sammlung biographischen Materials für die zeitgeschichtliche Forschung

An einem sozialwissenschaftlich ausgerichteten Institut einer Universität wird ein Archiv mit Interviewmaterial von Zeitzeugen geschaffen. Es ist vorgesehen, deren Lebensgeschichten sowie Aufnahmen von mit ihnen durchgeführten Interviews zu sammeln. Das Material soll für künftige Forschungsvorhaben wissenschaftlich ausgewertet werden.

Das Aufbewahren und Erfragen der Biographien setzt die Einwilligung der Betroffenen voraus. Im Gegensatz zu sonstigen Fällen im Bereich der Forschung ist die geplante Datensammlung nicht auf ein konkretes Projekt bezogen. Vielmehr ist die Sicherung von Aussagen von Zeitzeugen geplant, deren Anzahl naturgemäß für den vordringlich ins Auge gefassten Zeitraum der fünfziger und sechziger Jahre des vergangenen Jahrhunderts immer geringer wird.

Dieser Zweck muss sich in den Einwilligungserklärungen widerspiegeln. Es muss klar beschrieben werden, dass das Material allgemein zur Erforschung und Darstellung von zeitgeschichtlichen Ereignissen und Epochen verwendet werden soll, konkrete Projekte aber noch nicht existieren. Weiter sollte sichergestellt werden, dass es auch nach dem Tod der Betroffenen weiter verwendet werden kann. Schließlich müssen sich die befragten Personen darauf festlegen, auf welche Art und Weise das über sie vorhandene oder erst anzulegende Material genutzt werden darf: ob es unter voller Namensnennung in filmische Dokumentationen oder als Zitat aufzunehmen ist oder lediglich allgemein und ohne konkreten Personenbezug als Quellen- und Hintergrundmaterial für wissenschaftliche Arbeiten dienen soll. Dabei ist auch auf die weiteren Folgen hinzuweisen. Zwar besteht theoretisch immer ein Widerrufsrecht, das es ermöglicht, eine einmal gegebene Einwilligung zurückzunehmen und die weitere Verwendung des Materials zu untersagen. Tatsächlich wirkt es sich lediglich in Bezug auf zukünftige Projekte und solche, die noch nicht zu Veröffentlichungen geführt haben aus. Bereits in Fernseh- oder Rundfunkübertragungen mit konkretem Personenbezug gesendete Doku-

mentationen lassen sich nicht rückgängig machen, ihre Öffentlichkeitswirkung ist bereits eingetreten.

Einwilligungserklärungen sind nicht zu überfrachten. Sie sollten sich bei Vorhaben dieser Art grundsätzlich auf die Veröffentlichung des gesamten Interviews und nicht lediglich auf bestimmte Teile beziehen. Der Umgang mit dem dokumentarischen Material würde sonst erheblich erschwert, zumal zum Zeitpunkt der Entstehung der Sammlung lediglich der grobe Rahmen seiner Nutzung – Verwendung für zeitgeschichtliche Forschung – abgesteckt wird, nicht jedoch schon die Einzelheiten eines konkreten Projekts oder die darin involvierten Personen bestimmbar sind. Wollen Zeitzeugen bestimmte persönliche Aspekte nicht einbringen, müssen sie diese verschweigen.

Umgekehrt sind die Nutzer des Materials verpflichtet, die entsprechenden Bedingungen, die an die Zurverfügungstellung des Materials geknüpft sind, einzuhalten.

Gleichfalls werden die Anschriften der befragten Personen den Nutzern des Materials nicht ohne weiteres zugänglich gemacht. Möchten diese an jemanden herantreten, um ein Interview zu vertiefen oder weitere, sich aus dem konkreten Forschungsvorhaben ergebende Fragestellungen zu klären, müssen sie sich an das Institut wenden, welches den Kontakt dann vermittelt.

Das Verarbeiten von Zeitzeugenaussagen für noch nicht exakt umrissene zeitgeschichtliche Forschungsvorhaben bedarf der Einwilligung der befragten Person. In diesem Rahmen ist auch die Frage einer späteren, personenbezogenen Veröffentlichung zu klären.

8.2 Privatisierung von öffentlichen Archiven

Eine Gemeinde trat an uns mit der Frage heran, ob es auf datenschutzrechtliche Bedenken stößt, ein öffentliches Archiv zu privatisieren und von einer Firma betreiben zu lassen.

Bei den in Frage stehenden Unterlagen handelt es sich um abgeschlossene Altvorgänge, die nicht mehr für das Tagesgeschäft der Verwaltung benötigt werden. Aus datenschutzrechtlicher Sicht sind für das Verwaltungshandeln nicht mehr benötigte personenbezogene Unterlagen gemäß § 19 Abs. 4 Brandenburgisches Datenschutzgesetz (BbgDSG) zu löschen. Dieser Pflicht zum Löschen geht in der öffentlichen Verwaltung nach § 4 Abs. 1 Brandenburgisches Archivgesetz (BbgArchivG) zunächst die Pflicht vor, nicht mehr benötigte Unterlagen unverändert einem öffentlichen Archiv anzubieten. Mit der Übernahme durch ein Archiv sind sie der Nutzung durch die abgebenden Stellen weit gehend entzogen. Sie unterliegen hinsichtlich der besonderen

Geheimhaltungsvorschriften (Sozialgeheimnis, ärztliche Schweigepflicht, Adoptionsgeheimnis) den gleichen Verwendungsbeschränkungen wie zuvor. Die Nutzung durch Bürgerinnen und Bürger ist im Regelfall durch Sperrfristen für viele Jahre (§ 10 BbgArchivG) ausgeschlossen.

Die Aufbewahrung von Archivgut dient der Wahrung des staatlichen Gedächtnisses und der Ermöglichung späterer historischer Forschung. Die langen Sperrfristen schaffen insoweit einen Ausgleich zwischen dem Anspruch des Einzelnen auf Löschung seiner Daten aus datenschutzrechtlichen Gesichtspunkten und dem Interesse der staatlichen Gemeinschaft, sich über die historische Erinnerung zu definieren. Darüber hinaus sind individuelle und durch Verfassungsrechte geschützte Grundrechte, wie das der Forschungsfreiheit aus Art. 5 Abs. 3 Grundgesetz, zu berücksichtigen. Aus ihnen können Ansprüche auf Einsicht in das Archivgut, möglicherweise auch innerhalb verkürzter Sperrfristen, folgen.

Jede Gewährung einer Einsichtnahme in personenbezogene Unterlagen bedeutet einen Eingriff in teilweise von besonderen Schweigepflichten geschützte persönliche Bereiche von Personen, ihre Ablehnung hingegen beschränkt die Informationsrechte der Anfragenden. Alle Entscheidungen müssen stets rechtlich nachprüfbar sein. Sie stellen insoweit hoheitliches Handeln dar. Eine Übertragung dieser Aufgaben an Private, vor allem auch die damit verbundene Pflicht zur Wahrung besonderer Geheimhaltungspflichten, kann daher keinesfalls durch eine einfache vertragliche Vereinbarung erfolgen. Vielmehr bedarf es hierzu einer ausdrücklichen gesetzlichen Regelung, die auch die unterschiedliche Schutzbedürftigkeit verschiedener (Verwaltungs-) Bereiche berücksichtigen und widerspiegeln muss.

Archivgut ist außerdem auf Dauer aufzubewahren. Dem steht entgegen, dass in der Wirtschaft tätige Firmen ihr Fortbestehen nicht garantieren können. Im Ergebnis ist daher nach der geltenden Rechtslage eine Übertragung der Funktion eines öffentlichen Archivs auf eine private Firma unzulässig.

Archive müssen besondere Schweigepflichten – z. B. das Sozialgeheimnis – wahren sowie rechtsfeste Entscheidungen über den Zugang zum Archivgut treffen, die in Grundrechte eingreifen können. Eine Übertragung dieser Funktionen an eine privatrechtliche Firma durch einen Vertrag ist nach der geltenden Rechtslage unzulässig.

8.3 Nutzung der Initialen zum Zweck der Pseudonymisierung oder Anonymisierung

Forschungsvorhaben im medizinischen oder soziologischen Bereich kommen ohne Menschen und deren Daten nicht aus. Nachuntersuchun-

gen erfordern, dass teilweise über lange Zeiträume hinweg die gleichen Personen immer wieder befragt oder untersucht werden. Eingriffe in die Privatsphäre der Betroffenen sind dabei auf ein Minimum zu reduzieren.

Forschung und Wissenschaft sind auf personenbezogene Daten angewiesen. Im Regelfall bedarf es stets der Einwilligung derjenigen, die ihre Daten zur Verfügung stellen. Nur ausnahmsweise dürfen Daten auch ohne den erklärten Willen der Betroffenen für wissenschaftliche Zwecke verwendet werden.

In allen Fällen stellen sich aber grundsätzlich die gleichen Fragen nach dem Schutz der personenbezogenen Daten. Sie sollen stets nur für den Zweck eines konkreten Projekts nutzbar und den dort Tätigen nur so weit wie unbedingt nötig bekannt sein. Häufig genügt es, die Aussagen über einzelne Aspekte eines Menschen auszuwerten, ohne dessen Identität zu kennen, sodass es ausreicht, Datenmaterial anonymisiert zur Verfügung zu stellen.

Als anonym ist ein Datum immer dann anzusehen, wenn es ohne unverhältnismäßig großen Aufwand nicht mehr einer konkreten Person zugeordnet werden kann. Das bloße Weglassen des Namens und der Adresse ist für diesen Zweck untauglich, weil insbesondere bei kleinen Personengruppen die Zuordenbarkeit ohne weiteres erhalten bleibt. Es gilt die Faustformel: je mehr Personen an einer Untersuchung beteiligt werden, desto unwahrscheinlicher ist es, dass ein einzelnes Datum wieder zugeordnet werden kann. In Bereichen der staatlichen Statistik gibt es zum Schutz vor Offenlegung der Daten Einzelner zusätzlich das strafrechtlich bewehrte Verbot der Reanonymisierung.

Viele Forschungsvorhaben können jedoch nicht auf den Personenbezug ihrer Daten verzichten, weil sie darauf angelegt sind, in regelmäßigen Abständen den gleichen Personkreis noch einmal zu untersuchen oder zu befragen, um Veränderungen von Ergebnissen während beobachteter Zeiträume festzustellen. Auch hier sind Schutzvorkehrungen zu treffen. Zur Datenerfassung und -auswertung ist es nicht erforderlich, die konkreten Personen zu kennen. Daher ist es sinnvoll, die Namen durch andere Merkmale, die sog. Pseudonyme, zu ersetzen, die keine Rückschlüsse auf die Identität der Betroffenen zulassen. Die Verwendung von Initialen oder Bestandteilen des Geburtsdatums sollte unterbleiben, da das eine Zuordenbarkeit ermöglichen kann. Die Schlüssellisten, die es gestatten, Personen und Daten wieder zusammenzuführen, sind gesichert zu verwahren. Im Idealfall übernehmen separate Stellen das Anschreiben der zu befragenden Personen, sodass der wissenschaftliche, mit der Auswertung befasste Bereich nur die pseudonymisierten Daten erhält.

Wissenschaftliche Forschungsvorhaben benötigen häufig personenbezogene Daten. Die Forscher müssen jedoch nicht die konkreten Personen kennen, sodass es ausreicht, ihnen die Daten anonymisiert oder pseudonymisiert bereitzustellen. Ein Bezug zur Person darf dabei nicht ohne weiteres möglich sein.

9 Arbeit, Soziales, Gesundheit und Familie

9.1 Grenzen der Gendiagnostik

Gentests geben u. a. Aufschluss über die gesundheitliche Disposition oder über Abstammungsverhältnisse. Ein verantwortungsbewusster Umgang mit diesen Gesundheitsdaten erscheint schwierig.

Wie die neuen medizinischen Möglichkeiten in unser Leben drängen, zeigt sich u. a. an in der Öffentlichkeit diskutierten Gerichtsentscheidungen zur Verwertbarkeit heimlicher Vaterschaftstests. Danach hat das Recht des Vaters auf Klärung der biologischen Vaterschaft hinter dem Recht des Kindes auf informationelle Selbstbestimmung zurückzutreten. Heimliche Tests sind als rechtswidrige Eingriffe nicht vor Gericht verwertbar.

Um Missbrauch zu verhindern, dürfen Gentests nur durchgeführt werden, wenn die Betroffenen nach umfassender Aufklärung über Zweck und mögliche Konsequenzen in eine solche Untersuchung eingewilligt haben. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen. Heimliche Gentests müssen ebenso verhindert werden wie die missbräuchliche Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis.

Der Nationale Ethikrat legte im August 2005 seine Stellungnahme zu „Prädiktiven Gesundheitsinformationen bei Einstellungsuntersuchungen“ vor. Sie betrifft die Frage, inwieweit es zulässig sein soll, die Einstellung in Arbeitsverhältnisse von Informationen abhängig zu machen, die Aufschluss über den weiteren potenziellen Gesundheitsverlauf der Untersuchten geben. Derartige Wahrscheinlichkeitsaussagen können zunehmend genauer getroffen werden. Es besteht die Sorge, dass Arbeitgeber die Möglichkeiten der prädiktiven Diagnostik bei Entscheidungen über die Besetzung eines Arbeitsplatzes nutzen könnten.

Ähnliche Befürchtungen bestehen für die Gestaltung der Verträge in der Versicherungsbranche. Um sie auszuräumen, haben die Mitglieder des Gesamtverbandes der Deutschen Versicherungswirtschaft sich mit einer zunächst bis 2011 befristenden Selbstbindungserklärung verpflichtet, Gentests nicht zur

Voraussetzung für den Abschluss einer normalen privaten Versicherungspolice zu machen. Wir halten eine freiwillige Regelung nicht für ausreichend. Die in Rede stehenden Daten sind äußerst sensitiv und sollten nicht nur mittels freiwilliger Selbstverpflichtung vor Missbrauch geschützt werden.

In seiner Stellungnahme führte der Nationale Ethikrat aus, dass es legitim sei, dass ein Arbeitgeber vor seiner Entscheidung über die Einstellung eines Bewerbers berücksichtigt, ob dieser für die vorgesehene Tätigkeit körperlich, geistig und gesundheitlich geeignet ist. Fragen nach dem Gesundheitszustand eines Bewerbers und medizinische Untersuchungen sind daher zulässig, sofern sie erforderlich sind, zum Zeitpunkt der Einstellung die Tauglichkeit für die vorgesehene Tätigkeit festzustellen. Dagegen dürfen voraussagende Untersuchungsergebnisse, die sich auf die zukünftige Eignung eines Bewerbers beziehen, nur begrenzt verwertet werden. Prognostizierte Krankheiten seien nur zu berücksichtigen, wenn sie mit überwiegender Wahrscheinlichkeit kurz nach der Arbeitsaufnahme ausbrechen und erhebliches Ausmaß auf die Eignung des Betroffenen für den Arbeitsplatz haben. Begründet wird diese Haltung damit, dass zwar die Veranlagung für eine mögliche spätere Erkrankung feststellbar ist, nicht jedoch das Ob oder Wann ihres tatsächlichen Ausbruchs. Darüber hinaus sollen Bewerber nicht gezielt abgelehnt werden dürfen, sondern lediglich bei bestehenden konkreten Anhaltspunkten für eine bestimmte Krankheit oder Krankheitsanlage daraufhin untersucht werden können. Weiter gehende Untersuchungen seien allenfalls zulässig, wenn sich ohne ihre Erkenntnisse besondere Risiken für Dritte ergeben würden, wie dies beispielsweise bei Piloten und Busfahrern der Fall sein könnte.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte bereits auf ihrer 62. Konferenz im Oktober 2001 in einer Entschließung eine eindeutig restriktive Haltung zur Erhebung von Gesundheitsdaten mithilfe von Gentests vertreten und eine gesetzliche Regelung gefordert. Zur Feststellung der gesundheitlichen Eignung eines Arbeitnehmers soll nicht auf die Erhebung von Gesundheitsdaten aus der Familienanamnese zurückgegriffen werden. Ferner muss den Bewerbern die Möglichkeit eröffnet werden, negative ärztliche Bewertungen zu entkräften.

Die Verwendung genetischer Daten birgt ein besonderes Risiko der Diskriminierung. Gentests sollten nur mit dem Einverständnis des Betroffenen und nach vorheriger Aufklärung über die Folgen eventuell negativer Ergebnisse durchgeführt werden. Eine gesetzliche Regelung ist dringend notwendig.

9.2 Kinderärztliche Reihenuntersuchungen durch eine private Klinik?

Der Landkreis Havelland beabsichtigt, die kinderärztlichen Reihenuntersuchungen in den Klassenstufen 6 und 10 auf ein privatrechtlich organisiertes Krankenhaus, die Havelland Kliniken GmbH, zu übertragen. Die Ärzte der Havelland Kliniken GmbH sollen für die Untersuchungsdaten Laptops des Gesundheitsamtes nutzen.

Die kinderärztlichen Reihenuntersuchungen gehören zu den Pflichtaufgaben der Landkreise und kreisfreien Städte. Die Kinder- und Jugendgesundheitsdienst-Verordnung regelt die Einzelheiten der Durchführung dieser Reihenuntersuchungen. Danach ist ausschließlich der Kinder- und Jugendgesundheitsdienst der Gesundheitsämter für die Durchführung der Reihenuntersuchung zuständig. Somit gibt es keine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten durch Ärzte im Rahmen einer Pflichtuntersuchung außerhalb des Gesundheitsdienstes. Einer Klinik in privater Rechtsform könnten diese Aufgaben und hoheitlichen Befugnisse nur im Wege der Beleihung übertragen werden, was das Brandenburgische Gesundheitsdienstgesetz und das Brandenburgische Schulgesetz bisher jedoch nicht zulassen.

In einem auf ein Jahr befristeten Modellversuch des Landkreises werden nunmehr Kinder auf freiwilliger Basis durch einen Arzt der Havelland-Klinik untersucht. Bei Kindern, deren Eltern keine Einwilligung erteilen, wird die Untersuchung weiterhin durch Bedienstete des Gesundheitsamtes vorgenommen werden. Grundlage des Modellprojekts ist ein Vertrag, der unter der Beibehaltung der Verantwortlichkeit des Landkreises lediglich die Durchführung der ärztlichen Untersuchung dem Arzt der Havelland-Klinik überlässt. Sowohl die Terminvergabe als auch die Ausstellung amtlicher Bescheinigungen und Zeugnisse erfolgen weiterhin durch das Gesundheitsamt.

Im Rahmen der datenschutzrechtlichen Kontrolle des Modellprojekts „Gesundheitsamt der Zukunft“ wurde der folgende Ablauf vorgefunden: Die Untersuchung fand in zwei separaten Räumen der Schule statt. Auf einem Laptop waren bereits die Daten aller Schüler der zu untersuchenden Klassenstufe aus den früheren Reihenuntersuchungen gespeichert. Die Einwilligungserklärung wurde von den Schülern zur Untersuchung mitgebracht und gemeinsam mit dem Impfausweis sowie einem vorab zugesandten Fragebogen dem medizinischen Personal übergeben. Nach der Aktualisierung der Daten erfolgte die eigentliche ärztliche Untersuchung in einem anderen Raum. Die Ergebnisse wurden in einen zweiten Laptop eingegeben, der über eine Funkschnittstelle mit dem ersten verbunden war.

Nach Abschluss der Untersuchung gaben die Ärzte der Havelland-Klinik die Laptops im Gesundheitsamt ab. Dort wurden die Daten in das System eingespielt und auf den Laptops gelöscht.

Problematisch war zunächst auch die Tatsache, dass Daten vom Gesundheitsamt an die Mitarbeiter der Havelland-Klinik übermittelt wurden, bevor eine Einwilligung der Eltern zur Teilnahme an der von den Ärzten der Havelland Kliniken durchgeführten Reihenuntersuchung vorlag. Auf den Laptops befanden sich die Daten aller Schüler der Klassenstufe, die reihenärztlich zu untersuchen waren, und zwar unabhängig von einer erteilten Einwilligung. Bei einer Versagung der Zustimmung hätte es für diese Datenübermittlung keine rechtliche Grundlage gegeben. In Abänderung der bisherigen organisatorischen Abläufe holen die Mitarbeiter des Gesundheitsamtes jetzt jedoch vor dem Untersuchungstermin die Einwilligungserklärungen in den Schulen ein und speichern nur noch die Daten der Schüler, deren Eltern eingewilligt haben auf den Laptop, der den Ärzten zur Verfügung gestellt wird.

Die von uns vorgefundenen technisch-organisatorischen Maßnahmen waren aus datenschutzrechtlicher Sicht zunächst nicht zufrieden stellend. Um ein datenschutzgerechteres Verfahren zu gewährleisten bedurfte es

- der Erstellung einer Dienstanweisung zum Laptop-Einsatz,
- der Verpflichtung der Ärzte der Havelland Kliniken GmbH auf das Datengeheimnis,
- des Führens eines Übergabeprotokolls,
- eines formalen Freigabeverfahrens für Laptops,
- eines Berechtigungskonzepts für den Laptop-Einsatz,
- der Verschlüsselung der Daten auf dem Laptop,
- des Sicherns der Funkübertragung,
- einer Passwortsicherung des Rechners und der Anwendung,
- des Sperrens aller nicht erforderlichen Schnittstellen,
- des Verplombens der Geräte sowie
- eines Sicherheitskonzeptes.

Unsere Forderungen und Empfehlungen wurden vom Landkreis berücksichtigt und weit gehend umgesetzt.

Ohne Änderung gesetzlicher Bestimmungen ist die Übertragung kinderärztlicher Reihenuntersuchungen auf private Klinken nicht möglich. Mit einem auf freiwilliger Mitwirkung basierenden Modellversuch wird die Wirtschaftlichkeit der Übertragung ärztlicher Untersuchungen auf Private erprobt. Hinsichtlich der Einhaltung der aus datenschutzrechtlicher Sicht erforderlichen technisch-organisatorischen Maßnahmen begleiten wir das Pilotprojekt weiterhin.

10 Ländliche Entwicklung, Umwelt und Verbraucherschutz

Zentrale Datenbank BALVI iP

BALVI iP[48] ist eine ressortübergreifende Datenbank, die allen mit Lebensmittelüberwachung und Veterinäraufgaben befassten Verwaltungen zur Verfügung steht. Sie ist zentral beim Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz installiert. Einige Veterinär- und Lebensmittelüberwachungsämter bezweifeln die datenschutzrechtliche Zulässigkeit einer solchen Datenbank beim Ministerium.

Bei den Aufgaben der Veterinär- und Lebensmittelüberwachungsämter der Landkreise und kreisfreien Städte, die mithilfe der zentralen Datenbank erfüllt werden, handelt es sich um so genannte Pflichtaufgaben zur Erfüllung nach Weisung. Das Ministerium hat im Zusammenhang mit der Ausführung der den Landkreisen und kreisfreien Städten übertragenen Aufgaben Aufsichtsbefugnisse, die sich zum Teil nach dem speziellen Fachrecht, zum Teil nach dem allgemeinen Ordnungsbehördengesetz richten.

Die Ämter sind damit in ihren rechtlichen und fachlichen Entscheidungen nicht frei, aber im Sinne des § 3 Abs. 4 Nr. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) trotzdem als eigenständige Daten verarbeitende Stellen zu betrachten, die selbst für die Rechtmäßigkeit der Datenverarbeitung verantwortlich sind. Beim Betrieb der zentralen Datenbank handelt es sich deshalb nicht um eine Datenverarbeitung des Ministeriums selbst, sondern eine Datenverarbeitung im Auftrag der Lebensmittelüberwachungsämter. Hier gilt § 11 BbgDSG. Die Ämter bleiben Herr der Daten und damit für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich. Das Ministerium führt bei der Datenverarbeitung insofern lediglich Hilfsaufgaben im Auftrag aus. Das übrige, nicht die Datenverarbeitung betreffende Weisungsverhältnis auf Grund anderer Rechtsvorschriften bleibt erhalten.

Eine ordnungsgemäße Datenverarbeitung im Auftrag setzt voraus, dass sie gemäß § 11 Abs. 2 Satz 1 BbgDSG unter Festlegung des Gegenstandes und des Umfangs der Datenverarbeitung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich geregelt wird.

Es ist sicherzustellen, dass die einzelnen Lebensmittelüberwachungsämter jeweils nur Zugriff auf die von ihnen im Rahmen ihrer Aufgabenerfüllung benötigten Daten haben. Das Gleiche gilt auch für generelle Zugriffe des Ministeriums für Ländliche Entwicklung, Umwelt und Verbraucherschutz. Die recht-

[48] Bundeseinheitliche Anwendung zur Lebensmittel- und Veterinär-Information, integriertes Programm

liche Beschränkung der Datenzugriffsbefugnisse muss sich in den technischen und organisatorischen Maßnahmen insbesondere durch die entsprechende Vergabe der Zugriffsrechte widerspiegeln. Bei der Übertragung personenbezogener Daten zwischen den Ämtern und dem Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz über offene Netze wie das Internet oder das Landesverwaltungsnetz, ist durch den Einsatz von Verschlüsselungsverfahren die Vertraulichkeit der Daten sicherzustellen.

Sämtliche technische und organisatorische Maßnahmen sollten Bestandteil eines Sicherheitskonzepts werden, das nach einer entsprechenden Risikoanalyse im Rahmen von § 7 Abs. 3 BbgDSG zu erstellen ist. Das Erstellen der Sicherheitskonzepte liegt zwar formal in der Verantwortung der einzelnen Auftrag gebenden Stellen. Angesichts der gewünschten Zentralisierung der Datenverarbeitung beim Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz sollte jedoch von allen beteiligten Stellen ein gemeinsames, einheitliches Konzept entwickelt werden.

Auch ein die Fach- und Rechtsaufsicht führendes Ministerium kann im Auftrag der Landkreise und kreisfreien Städte, über das es die Aufsicht hat, personenbezogene Daten zentral verarbeiten. Es gelten dann die allgemeinen Regeln der Datenverarbeitung im Auftrag.

11 Finanzen

Kontendatenabruf

Eine Änderung in der Abgabenordnung (AO) durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003[49] erlaubt den Finanzbehörden seit dem 1. April 2005 den Abruf einzelner Kontodaten und ggf. auch den Zugriff auf den Kontostand steuerpflichtiger Bürger.

Der Kontodatenabruf ist nach § 93 Absatz 7 AO zulässig, wenn er zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht. Neben den Finanzbehörden sind über § 93 Absatz 8 AO noch eine Vielzahl weiterer Behörden und Gerichte zum Einholen von Kontoinformationen berechtigt, soweit die oben genannten Voraussetzungen geltend gemacht werden. Die Finanzbehörden sollen auf Aufforderung von Behörden und Gerichten über das Bundeszentralamt für Steuern[50] einzelne Daten abrufen und der ersuchenden Behörde bzw. dem ersuchenden Gericht mitteilen.

[49] siehe BGBl. I, S. 2928

[50] bis zum 31.12.2005 Bundesamt für Finanzen

Datenschutzrechtlich bestehen hinsichtlich der Neuregelungen in der Abgabenordnung erhebliche Bedenken. Insbesondere der unbestimmte Kreis der Behörden, die Kontodaten erhalten können, geht zulasten der Betroffenen und ist mit dem gesetzlichen Bestimmtheitsgebot nicht vereinbar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte bereits im Jahre 2004 in der Entschließung „Staatliche Kontoabfrage auf den Prüfstand“ gefordert, das Gesetz mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten.[51] Besonderes Augenmerk sollte auf die Normenklarheit des Gesetzes gelegt werden. Die Entschließung hatte massive Kritik an der vorgesehen Praxis geübt, betroffene Bürger nicht von einer durchgeführten Kontodatenabfrage zu informieren. Die betroffenen Bürger sind vielmehr „von der Speicherung und über die Identität der verantwortlichen Stelle, sowie über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung zu unterrichten“. Wird auf eine solche Regelung im Gesetz verzichtet, ist die verfassungsrechtlich gewährte Rechtweggarantie des Artikels 19 Absatz 4 Grundgesetz verletzt.

Auf Grund der datenschutzrechtlichen Bedenken haben einige Einzelpersonen und eine Bank Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben und den Erlass einer einstweiligen Anordnung beantragt, um das In-Kraft-Treten der gesetzlichen Regelungen zum 1. April 2005 zu verhindern. Diese Anträge wurden vom Bundesverfassungsgericht mit Entscheidung vom 22. März 2005 abgelehnt.

Die Entscheidung war auch beeinflusst durch einen Anwendungserlass des Bundesministeriums der Finanzen vom 10. März 2005. Darin werden die Schutzvorkehrungen für die betroffenen Bürger konkretisiert und die Belastungen der Kontodatenabfrage gemildert. So sind nach dem Erlass die betroffenen Bürger darüber zu informieren, dass ihre Daten abgefragt wurden. Auch wurde ein Katalog von konkreten Tatbeständen aufgenommen, der es anderen Behörden gestattet, über die Finanzämter Zugang zu den Kontodaten einzelner Bürger zu erhalten. Dies soll jetzt nur noch in Angelegenheiten der Sozialversicherung, bei der Gewährung von Sozialhilfe, bei der sozialen Wohnraumförderung, der Ausbildungsförderung, der Aufstiegsförderung, der Gewährung von Wohngeld und Erziehungsgeld sowie bei der Gewährung von Leistungen zur Unterhaltssicherung möglich sein.

Dieser Versuch der Schadensbegrenzung durch das Bundesministerium für Finanzen ist grundsätzlich positiv zu bewerten. Darüber hinaus bedarf es jedoch einer gesetzlichen Regelung, um den datenschutz- und verfassungsrechtlichen Grundsätzen von Bestimmtheit und Normenklarheit zu entsprechen. Eine verwaltungsinterne Vorschrift allein ist nicht ausreichend.

[51] siehe Dokumente zu Datenschutz und Informationsfreiheit 2004, A I 4

Das Bundesverfassungsgericht hat ausdrücklich mitgeteilt, dass seine Entscheidung im Eilverfahren noch keinen Vorgriff auf die Hauptsachenentscheidung darstellt. Das Hauptsachenverfahren ist derzeit noch anhängig.

Die Finanzämter im Land Brandenburg haben im Zeitraum vom 1. April bis zum 30. September 2005 in 28 Fällen von der durch die Änderung der Abgabenordnung geschaffenen Möglichkeit zur Kontodatenabfrage Gebrauch gemacht.

Im Jahr 2006 werden wir die praktische Handhabung der Kontodatenabfrage im Land Brandenburg besonders aufmerksam verfolgen. Dazu werden stichprobenartige Kontrollen in den Finanzbehörden sowie eine Ermittlung der Gesamtzahl und Gründe der Abfragen durchgeführt.

Teil B

Akteneinsicht und Informationszugang

1 Entwicklung des Informationszugangsrechts

1.1 Bundesrepublik Deutschland

1.1.1 Informationsfreiheitsgesetz

Als eines der letzten Gesetze verabschiedete der Bundestag in der abgelaufenen 15. Legislaturperiode das Gesetz zur Regelung des Zugangs zu Informationen des Bundes – kurz: Informationsfreiheitsgesetz. Seit seiner ersten Ankündigung war es zunächst auch unter den damaligen Koalitionären selbst heftig umstritten. Vor allem auf Drängen engagierter Bürgerrechtler gelangte schließlich ein konsensfähiger Entwurf zur Abstimmung. Das Informationsfreiheitsgesetz trat am 1. Januar 2006 in Kraft. Als einer der letzten Staaten in Europa verschafft die Bundesrepublik Deutschland damit den Bürgerinnen und Bürgern freien Zugang zu öffentlichen Informationen. Allerdings verpflichtet es nur Bundesbehörden zur Gewährung von Auskunft und Einsicht und enthält zahlreiche Einschränkungen, die den Erwartungen an ein wirkungsvolles Instrument zur Erlangung öffentlicher Informationen nicht gerecht werden. Fiskalische und andere privatrechtliche Tätigkeiten der öffentlichen Hand sind beispielsweise vom Informationszugang weiterhin ausgenommen. Der Schutz öffentlicher Belange geht über den erforderlichen Ausschluss einer konkreten Gefährdung öffentlicher Interessen hinaus. Ob Unternehmensdaten offen gelegt werden können, hängt in weiten Teilen vom Willen des Unternehmens anstatt von der Schutzbedürftigkeit der Informationen ab. Trotz aller Kritik an den Einzelheiten ist das Gesetz jedoch grundsätzlich positiv zu bewerten. Es ist in jedem Fall auch ein Signal für alle Bundesländer, die noch kein solches Gesetz haben, ein voraussetzungsloses Recht auf Informationszugang zu schaffen.

1.1.2 Umweltinformationsgesetz

Die Europäische Gemeinschaft hat bereits vor fünfzehn Jahren mit der ersten Umweltinformationsrichtlinie ein allgemeines Recht auf den voraussetzungslosen Zugang zu Umweltinformationen geschaffen. Sie sollte die Beteiligungsmöglichkeiten der Bürger an umweltbezogenen Entscheidungen verbessern. Eine Novellierung der Richtlinie verpflichtete schließlich die Mitgliedsstaaten zur Umsetzung der darin enthaltenen Ausweitung des Umweltinformationsrechts in nationales Recht bis zum 14. Februar 2005. Die Bun-

desrepublik kam dieser Verpflichtung mit der Verabschiedung eines neuen Umweltinformationsgesetzes nach, das allerdings im Gegensatz zu früher nur für die Bundesbehörden gilt. Die Länder sind nunmehr verpflichtet, die Umweltinformationsrichtlinie mittels eigener Gesetze umzusetzen.

Das neue Bundesgesetz weitet den Geltungsbereich im Vergleich zur vorangegangenen Regelung erheblich aus. Nunmehr hängt das Informationsrecht des Einzelnen nicht mehr davon ab, ob eine Behörde Umweltaufgaben erledigt, sondern es gilt grundsätzlich gegenüber allen im Sinne des Gesetzes informationspflichtigen Stellen. Dazu zählen neben den Behörden auch privatrechtlich organisierte Unternehmen der Daseinsvorsorge, die der Kontrolle des Bundes unterliegen. Der Begriff der „Umweltinformation“ wird durch das neue Gesetz im Einzelnen definiert und umfasst neben offensichtlichen Umweltinformationen auch Angaben zu Maßnahmen oder Tätigkeiten mit Umweltauswirkungen sowie Informationen über Maßnahmen und Tätigkeiten, die Auswirkungen auf die menschliche Gesundheit – etwa auf Lebensmittel – haben könnten. Die informationspflichtigen Stellen müssen darüber hinaus auch von sich aus Informationen über die Umwelt bereitstellen. Auch sind die Kostenregelungen bürgerfreundlicher geworden: Auskünfte sowie die Einsichtnahme vor Ort sind kostenlos, im Übrigen dürfen Gebühren nicht in einer Weise erhoben werden, dass sie von einer Antragstellung abschrecken.

1.1.3 Verbraucherinformationen

Nach einer Reihe von Lebensmittelskandalen ist der Bedarf der Bevölkerung an Informationen über Produkte erheblich gestiegen. Die bereits bestehenden Kennzeichnungspflichten genügen diesen Anforderungen oftmals nicht. Die Informationsbedürfnisse haben zudem häufig einen konkreten Unternehmensbezug oder aber stehen in keinem direkten Zusammenhang mit Umwelteinflüssen, sodass weder das Informationsfreiheitsgesetz noch das Umweltinformationsgesetz einen eindeutigen Anspruch auf Informationszugang gewähren. Beide Gesetze können ein weiter gehendes Verbraucherinformationsgesetz daher nicht ersetzen. Ein erster vorgelegter Entwurf der letzten Bundesregierung scheiterte 2002 am Einspruch des Bundesrates. Die große Koalition aus CDU und SPD hat sich nun jedoch in ihrem Koalitionsvertrag darauf geeinigt, einen neuen Anlauf zu nehmen, um eine größere Transparenz auf dem Gebiet der gesundheitsgefährdenden oder risikobehafteten Produkte herzustellen.

1.1.4 Weiterverwendung öffentlicher Informationen

Durch die Richtlinie des Europäischen Parlaments und des Rates über die Weiterverwendung von Dokumenten des öffentlichen Sektors aus dem Jahre 2004, die noch in nationales Recht umgesetzt werden muss, sollen vor allem

für die kommerzielle Verarbeitung öffentlicher Informationen europaweit gleiche Bedingungen hergestellt werden. Dabei geht es in erster Linie um große Datenbanken öffentlicher Stellen, die von privatwirtschaftlichen Unternehmen erworben, weiterentwickelt und schließlich gewinnbringend vermarktet werden. Die Regelungen eröffnen keinen eigenen Zugangsanspruch, sondern basieren lediglich auf bestehenden Zugangsregelungen wie dem Informationsfreiheitsgesetz. Sie gestatten lediglich die Weiterverwendung von Dokumenten unter urheberrechtlichen Gesichtspunkten. Die Richtlinie kann ihre volle Wirkung daher nur entfalten, wenn die Informationen, die vermarktet werden sollen, auch zugänglich sind. Das künftige Bundesgesetz, das die Richtlinie umsetzen soll, muss eine Balance finden zwischen den wirtschaftsfördernden Zielen der Richtlinie einerseits und einer Abgrenzung von den Informationsfreiheitsgesetzen andererseits. Die kommerzielle und damit gebührenpflichtige Nutzung öffentlicher Informationen darf nicht dazu führen, dass deren Verwendung für private Zwecke bzw. für solche der politischen Mitgestaltung eingeschränkt wird. Auch darf der Antragsteller über den Umweg der Feststellung, ob eine Information zu kommerziellen Zwecken und damit entgeltpflichtig genutzt werden soll, nicht gezwungen werden, ein bislang voraussetzungsloses Informationsbegehren begründen zu müssen.

1.1.5 Transparenz öffentlicher Unternehmen

Private, börsennotierte Aktiengesellschaften sind seit kurzem verpflichtet, die Vergütungen ihrer Vorstandsmitglieder offen zu legen. Aktionäre können somit erfahren, welche Gehälter der Vorstand einer Aktiengesellschaft bezieht. Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland, der auch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht angehört, hat im November 2005 gefordert, dass dieselben Rechte auch Bürgern gegenüber öffentlichen und öffentlich kontrollierten Unternehmen zustehen sollen. Eine Veröffentlichung der Bezüge in den Jahresabschlüssen und in den Beteiligungsberichten der öffentlich-rechtlichen Körperschaften würde die Transparenz über die Verwendung von Steuergeldern entscheidend verbessern. Die jüngst verabschiedeten Regelungen für private Aktiengesellschaften können hierfür als Maßstab dienen.

1.1.6 Öffentlichkeit von Gremiensitzungen

Transparenz der öffentlichen Hand wird bislang vor allem mit dem Recht auf Zugang zu Akten oder anderen Datenträgern in Verbindung gebracht. Von ebenso großer Bedeutung für die Gewinnung von Kenntnissen über staatliche Entscheidungsprozesse ist jedoch auch die Möglichkeit, an Sitzungen von Gremien teilzunehmen. Während dies bei Gerichtsverhandlungen und Parlamentssitzungen selbstverständlich ist, tagen in Brandenburg beispielsweise die Landtagsausschüsse nicht öffentlich. Auch bei anderen öffentlichen

Stellen, deren Entscheidungen durch demokratische Mitwirkungsgremien legitimiert werden, wie z. B. Bildungs-, Sozial- oder Versorgungseinrichtungen, sind nicht öffentliche Sitzungen eher die Regel. Gleiches gilt auf der kommunalen Ebene. In den Vereinigten Staaten von Amerika ist dagegen sowohl auf der Ebene des Bundes als auch der Einzelstaaten der Meinungsaustausch in behördlichen Kollegialsitzungen öffentlich. Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland hat nun Regelungen für die Öffentlichkeit von Sitzungen, die in Ausnahmefällen auch den Ausschluss der Öffentlichkeit zum Schutz überwiegender öffentlicher oder privater Interessen ermöglichen müssen, auch für die Bundesrepublik Deutschland gefordert. Die Arbeitsgemeinschaft hat selbst einen ersten Schritt für mehr Transparenz getan, indem sie die interessierte Öffentlichkeit künftig zu ihren eigenen Sitzungen zulässt sowie Tagesordnungen und Niederschriften der Sitzungen im Internet veröffentlicht.

1.2 Brandenburg

1.2.1 Umsetzung der Umweltinformationsrichtlinie der Europäischen Union

Die 2003 novellierte Umweltinformationsrichtlinie der Europäischen Union sieht für die Umsetzung in nationales Recht eine Frist bis zum 14. Februar 2005 vor. Während der Bundesgesetzgeber für seinen Zuständigkeitsbereich rechtzeitig ein Umweltinformationsgesetz verabschiedet hat, ist die Umsetzungsfrist in Brandenburg ergebnislos verstrichen. Nach europarechtlichen Grundsätzen ist die Umweltinformationsrichtlinie in diesem Fall unmittelbar anzuwenden, bis ein Umweltinformationsgesetz auf Landesebene in Kraft tritt.

Allerdings unterliegt die unmittelbare Anwendung zwei wesentlichen Einschränkungen: Da sich die Richtlinie nur an die Mitgliedsstaaten der Europäischen Union wendet, dürfen zum einen private Dritte auf ihrer Grundlage nicht belastet werden. Das bedeutet, dass der Zugang zu Umweltinformationen dann nicht möglich ist, wenn sich personen- oder unternehmensbezogene Daten in den Unterlagen befinden. Gerade bei Akten, die Auskunft über Umweltschutzfragen oder Umweltdaten geben, ist dies aber oft der Fall. Darüber hinaus kommt eine direkte Anwendung der Richtlinie nur in Frage, soweit ihre Regelungen konkret genug sind. Diese Voraussetzung ist oft schon deshalb nicht gegeben, weil eine Richtlinie häufig nur den Rahmen für eine Umsetzung festsetzt und ihre Regelungen daher einen weiten Spielraum enthalten.

Die Landesbeauftragte befasst sich häufig mit Beschwerden und Anfragen, in denen neben dem Akteneinsichts- und Informationszugangsgesetz auch der

Umweltinformationszugang eine Rolle spielt. Auf Grund der durch das Nichttätigwerden des Gesetzgebers unklaren Rechtslage bleibt der Zugang zu Umweltinformationen trotz der europäischen Richtlinie stark eingeschränkt.

1.2.2 Neufassung der Akteneinsichts- und Informationszugangsgebührenordnung

Die ursprüngliche Akteneinsichts- und Informationszugangsgebührenordnung war bis Ende des Jahres 2003 befristet. Danach sollte anhand der gewonnenen Erfahrungen der Verwaltungen eine Neuregelung vorgenommen werden. Auf Grund einer bevorstehenden Änderung des Akteneinsichts- und Informationszugangsgesetzes wurde 2003 die Geltung der bestehenden Regelung unter Umrechnung der Beträge in Euro zunächst auf zwei weitere Jahre befristet. Ohne Erfolg forderte damals die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht unter anderem die Reduzierung der jeweiligen Höchstbeträge für Gebühren, die explizite Regelung eines Verzichts auf Bagatellbeträge sowie eine Klarstellung dahingehend, dass ein angemessenes Verhältnis zwischen den erhobenen Kosten und dem tatsächlich vorhandenen Verwaltungsaufwand bestehen muss. Vor der Neufassung der Verordnung 2005 wiederholten wir unsere Empfehlungen und sprachen uns zudem für eine Harmonisierung mit der ebenfalls bevorstehenden Kostenregelung für den Umweltinformationszugang aus. Aus Gründen der Bürgerfreundlichkeit, aber auch der Verwaltungsvereinfachung sollten sich die Kostenregelungen für den allgemeinen Informationszugang nicht von jenen des Umweltinformationszuganges unterscheiden. Das Ministerium des Innern setzte unsere Anregungen nicht um. Inwieweit die ursprünglich vorgesehene Evaluation stattgefunden hat, ist nicht zu erkennen. Die neue Akteneinsichts- und Informationszugangsgebührenordnung trat am 1. Januar 2006 in Kraft und gilt ohne Befristung.[52]

1.2.3 BRAVORS

Die Abkürzung BRAVORS steht für die seit 2005 im Internet verfügbare „Brandenburgische Vorschriftensammlung“ und beinhaltet neben Gesetzen und Verordnungen auch Verwaltungsvorschriften[53]. Bei letzteren handelt es sich um Erlasse und Rundschreiben, die beispielsweise von Ministerien an deren nachgeordnete Behörden gerichtet sind. Sie enthalten Vorgaben, wie bei der Umsetzung gesetzlicher Vorschriften zu verfahren ist und sollen so eine einheitliche Verwaltungspraxis gewährleisten. Zwar richten sich die Verwaltungsvorschriften lediglich an die Behörden und geben den Bürgern keine unmittelbaren Rechtsansprüche. Allerdings ist die Verwaltung verpflichtet, diese Vorgaben gegenüber allen Bürgern in gleicher Weise zu berücksichti-

[52] GVBl. II 2005, S. 596

[53] siehe http://www.landesrecht.brandenburg.de

gen, sodass ihr Inhalt für die Betroffenen von erheblicher Bedeutung ist und im Ergebnis auch gerichtlich überprüft werden kann. Durch BRAVORS hat die Öffentlichkeit nun erstmals Zugang zu den bislang als verwaltungsintern behandelten Vorschriften. Die Transparenz des Handelns der brandenburgischen Verwaltung wird dadurch wesentlich erhöht.

1.2.4 Bekanntgabe von Aktivitäten und Bezügen öffentlicher Entscheidungsträger

Von jemandem, der an herausragender Stelle der Regierung, als Abgeordneter oder als Mitglied einer kommunalen Vertretung tätig ist, erwarten die Bürger, dass er seine Entscheidungen ausschließlich im Interesse der Allgemeinheit trifft. Wie aber können Bürger erkennen, ob eventuell andere Interessen im Spiel sind? Ist ein Entscheidungsträger im Aufsichtsrat eines Unternehmens tätig oder führt er den Vorsitz eines bestimmten Verbandes oder Vereines, könnten Interessenkollisionen gegeben sein, die auch in amtlicher Funktion getroffene Entscheidungen beeinflussen könnten. Dies gilt insbesondere, wenn eine „nebenamtliche“ Tätigkeit vergütet wird. Interessenverflechtungen dieser Art sind gerade auf der kommunalen Ebene nicht selten. Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland hat daher gefordert, die Bekanntgabe von Aktivitäten und Bezügen öffentlicher Entscheidungsträger verpflichtend zu regeln. Während Informationen über die Aktivitäten und Bezüge der Mitglieder des Landtages Brandenburg veröffentlicht werden, stellt die brandenburgische Gemeindeordnung eine derartige Offenlegung und damit ein wichtiges Kontrollinstrument für die Bürger lediglich in das Ermessen der Gemeinden. Um die Transparenz von Entscheidungsprozessen und damit auch die Akzeptanz der Entscheidungen öffentlicher Stellen zu erhöhen, empfiehlt die Landesbeauftragte den Kommunen, dies bereits jetzt zwingend in ihren Hauptsatzungen vorzusehen.

2 Umsetzung des Akteneinsichts- und Informationszugangsgesetzes

2.1 Erlass zur Verkehrsüberwachung – ein Geheimnis?

Ein Polizeipräsidium verweigerte die Einsicht in einen Erlass zur Verkehrsüberwachung mit der Begründung, dass das Ministerium des Innern solche Verwaltungsvorschriften im Rahmen der Fach- und Dienstaufsicht gegenüber den Polizeibehörden erlassen würde. Sie seien daher als Aufsichtsakten anzusehen und geheim zu halten.

Durch Verwaltungsvorschriften (z. B. Erlasse oder Rundschreiben) legt sich die Verwaltung in ihrer Ermessensausübung fest und kann hiervon nur aus-

nahmsweise abweichen. Aus ihnen entstehen zwar keine direkten Ansprüche, sie verpflichten die Behörden, aber alle gleich gelagerten Fälle auch gleich zu behandeln. Dies ist vom Bürger gerichtlich durchsetzbar. Der zur Einsicht beantragte Erlass beinhaltet lediglich allgemeine Regelungen zur Aufstellung von Messgeräten und zur Durchführung von Geschwindigkeitskontrollen im Straßenverkehr; seine Offenlegung bedeutet keine Gefahr für den Erfolg konkreter Überwachungsmaßnahmen.

Der im Akteneinsichts- und Informationszugangsgesetz verwendete Begriff der „Aufsicht“ ist begrenzt auf Vorgänge, in denen die Aufsichtsbehörde gegenüber den der Aufsicht unterworfenen Stellen einschreitet bzw. eine Prüfung durchführt. Die bloße Tatsache, dass zwei Behörden in einem hierarchischen Verhältnis zueinander stehen, führt nicht dazu, dass alle Unterlagen einer nachgeordneten Behörde automatisch als „Aufsichtsakten“ zu klassifizieren sind. Anderenfalls wäre kaum ein Fall denkbar, in dem einem Antrag auf Akteneinsicht stattzugeben wäre.

Das Polizeipräsidium verstieß mit der Geheimhaltung des Erlasses aber nicht nur gegen die Vorschriften des Akteneinsichts- und Informationszugangsgesetzes, sondern beachtete darüber hinaus nicht den Beschluss der Landesregierung, auch bislang nicht ohne weiteres zugängliche Verwaltungsvorschriften der Öffentlichkeit zugänglich zu machen und im Internet zu veröffentlichen. Eine Aufstellung der brandenburgischen Vorschriften (BRAVORS) steht unter www.landesrecht.brandenburg.de zur Verfügung.

Nachdem wir die Behörde darauf aufmerksam gemacht haben, dass der strittige Erlass zur Verkehrsüberwachung durch die Polizei dort bereits bekannt gemacht wurde, hat sie dem Antragsteller die Informationen zur Verfügung gestellt.

Seit Beginn des Jahres 2005 stehen neben den Gesetzen und Verordnungen auch Verwaltungsvorschriften des Landes Brandenburg im Internet zur Verfügung. Die Transparenz und Nachvollziehbarkeit des Verwaltungshandelns wird dadurch erheblich verbessert.

2.2 Eigene personenbezogene Daten in nicht öffentlichen Sitzungen

Der Betreiber einer Tankstelle, dessen Pachtvertrag mit einer Stadt nach einer Diskussion im Hauptausschuss der Stadtverordnetenversammlung nicht verlängert wurde, beabsichtigte, diese Entscheidung auf dem Wege der Akteneinsicht nachzuvollziehen. Da die Sitzung nicht öffentlich stattfand, wurde er zunächst gebeten, sein Offenbarungsinteresse darzulegen.

Der Tankstellenbetreiber führte ein Ein-Personen-Unternehmen, d. h. die Angaben zu seinem Betrieb waren gleichzeitig personenbezogene Daten. Um seine Persönlichkeitsrechte zu wahren, wurde die Öffentlichkeit von dem Teil der Sitzung des Hauptausschusses, der ihn betraf, ausgeschlossen. Der Unternehmer stellte einen Antrag auf Informationszugang, um genau jene Angaben zu erlangen, die ihn selbst bzw. seinen eigenen Betrieb betreffen.

Das Akteneinsichts- und Informationszugangsgesetz sieht die Ablehnung eines Einsichtsantrages im Falle einer nicht öffentlichen Sitzung vor, es sei denn, dass das Einsichtsinteresse das entgegenstehende öffentliche Interesse im Einzelfall überwiegt. Ein öffentliches Interesse machte die Stadt nicht geltend; vielmehr schloss sie die Öffentlichkeit ausschließlich auf Grund des privaten Schutzinteresses des Antragstellers aus. Eine Anhörung, die der Interessenabwägung dienen soll, wäre somit nicht notwendig gewesen. Schließlich bezweckt das Akteneinsichts- und Informationszugangsgesetz nicht, den Antragsteller vor seinen eigenen Daten zu schützen.

Das Akteneinsichts- und Informationszugangsgesetz kommt in diesem Fall allerdings nicht zur Anwendung, da der Betroffene lediglich Informationen begehrt, die auf seine Person bezogen sind. Der Antrag auf Informationszugang war somit rein datenschutzrechtlicher Natur und auf der Grundlage des § 18 Brandenburgisches Datenschutzgesetz zu bearbeiten. Danach hat jeder das Recht, zu erfahren, welche Informationen öffentliche Stelle zu der eigenen Person verarbeiten. Die Stadt hat zugesichert, dies zu beachten.

Interessiert sich ein Antragsteller für Daten, die einen Bezug zu seiner eigenen Person aufweisen, so macht er einen datenschutzrechtlichen Informationsanspruch geltend. Dieser ist auf der Grundlage des Brandenburgischen Datenschutzgesetzes zu bearbeiten. Es besteht grundsätzlich kein Anlass, Antragsteller vor ihren eigenen Daten zu schützen.

2.3 Aufbewahrungspflichten amtlicher Unterlagen

Ein Landesbetrieb verweigerte die Herausgabe von Unterlagen mit dem Hinweis, dass diese vernichtet worden seien. Wann darf eine öffentliche Stelle ihre Akten vernichten?

Die beantragten Informationen beinhalteten unter anderem die Bewertung von Planungsvorhaben zum Bau von Ortsdurchfahrten aus den Jahren 1995 und 1996. Die Akten führende Stelle erklärte, dass nur noch das Ergebnis (Bedarfsliste für Ortsdurchfahrten) vorliege, die Einzelbewertungen der jeweiligen Planungsvorhaben (Bewertungstabellen) aber vernichtet worden seien.

Sowohl das Akteneinsichts- und Informationszugangsgesetz, als auch das Umweltinformationsrecht geben dem Antragsteller ein Recht auf Zugang zu vorhandenen Informationen. Beide Gesetze enthalten weder die Verpflichtung, bestimmte Akten zu führen, noch eine konkrete Regelung zur Aufbewahrung von Unterlagen. Dennoch kann eine Behörde nicht ohne weiteres selbst bestimmen, welche Akten sie vernichtet, da sonst die Gefahr bestünde, dass sie sich ihren gesetzlichen Offenlegungspflichten entzöge.

Konkrete Aufbewahrungspflichten und -fristen bestehen beispielsweise für Sozial- und Personaldaten oder für Unterlagen der Haushaltsführung. Für alle übrigen Informationen – wie auch für die eben genannten nach Ablauf der Aufbewahrungsfristen – bestimmt das Brandenburgische Archivgesetz, dass Akten, die zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden, dem zuständigen öffentlichen Archiv unverändert anzubieten sind. Dieses bewertet die Unterlagen und entscheidet darüber, ob sie auf Dauer aufbewahrt werden sollen. Die Akten führende Stelle entscheidet demgegenüber nur, ob die Unterlagen noch für das „Tagesgeschäft“ benötigt werden. Hält das Archiv sie nicht für archivwürdig, können sie vernichtet werden. Enthalten sie personenbezogene Daten, müssen sie nach § 19 Abs. 2 Brandenburgisches Datenschutzgesetz dann sogar vernichtet werden. Die Vernichtung sollte protokolliert und die Protokolle aufbewahrt werden.

Nach unseren entsprechenden Hinweisen an den Landesbetrieb veranlasste dieser eine erneute Recherche. Die zur Einsicht begehrten Unterlagen wurden gefunden und dem Antragsteller offen gelegt.

Auch wenn Akten zur Aufgabenerfüllung nicht mehr benötigt werden, darf eine öffentliche Stelle sie nicht ohne weiteres vernichten. Sie sind vielmehr dem zuständigen Archiv anzubieten. Hält dieses die Unterlagen nicht für archivwürdig, können sie vernichtet werden. Enthalten sie personenbezogene Daten besteht die Pflicht, die vom Archiv nicht übernommenen Akten zu vernichten. Dies sollte protokolliert werden.

2.4 Vertrag für Windkraftanlagen

Um Einzelheiten zu der geplanten Errichtung von Windkrafträdern zu erfahren, beantragte eine Bürgerinitiative Einsicht in den Entwurf eines Vertrages zwischen der Stadt und einer Betreibergesellschaft. Die Stadt versuchte, dies zu verhindern.

Nachdem der Informationszugang zunächst mündlich und ohne Begründung verweigert wurde, erklärte die Stadt später, sie handele beim Abschließen von Verträgen nicht in hoheitlicher Funktion, sondern als Privatperson. Bei Vereinbarungen über städtische Grundstücke seien damit ihre Interessen auf

Vertraulichkeit zu schützen. Außerdem habe sich die Bürgerinitiative bereits aus anderen Quellen einen Vertragsentwurf beschafft.

Wir baten die Stadt um eine Stellungnahme sowie um Unterlagen, die uns eine Beurteilung des Sachverhalts ermöglichen sollten. Auch auf mehrfaches Nachfragen erfolgte zunächst keinerlei Reaktion. Im weiteren Fortgang des Geschehens erklärte die Stadt auf informationszugangsrechtliche Hinweise, insbesondere auch auf die uns gegenüber bestehende Mitwirkungspflicht, dass sie die Angelegenheit als abgeschlossen betrachte.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kann ihre Aufgabe nur wahrnehmen, wenn alle Beteiligten sie unterstützen, sodass sie sich ein ausgewogenes Bild des Sachverhaltes machen kann. Die einseitige Erklärung hat sie in diesem Fall als Verweigerung der gesetzlichen Unterstützungspflicht angesehen. Das Verhalten beanstandete die Landesbeauftragte als Verstoß gegen das Akteneinsichts- und Informationszugangsgesetz. Die Stadt übersandte uns zwar daraufhin die Entwurfstexte, erklärte aber erneut, dass die Angelegenheit als endgültig erledigt zu betrachten sei. Tatsächlich kam die Stadt mit der Herausgabe der Unterlagen nur der gesetzlichen Unterstützungspflicht uns gegenüber nach. Eine inhaltliche Prüfung des Einsichtsbegehrens unterblieb aber nach wie vor.

Als Rechtsgrundlage für die Einsicht kamen das Akteneinsichts- und Informationszugangsgesetz oder das Umweltinformationsgesetz in Frage. Beide Gesetze unterscheiden nicht zwischen öffentlich-rechtlichen und privatrechtlichen Aufgaben. Auf die Rechtsform des Handelns einer öffentlichen Stelle kommt es beim Informationszugang daher nicht an. Sie ist unabhängig davon immer auskunftspflichtig. Auch auf das Argument, der Antragsteller verfüge bereits über den Text, kommt es hier nicht an, da er das bestritt und behauptete, lediglich über einen früheren Entwurfstext zu verfügen. Im Übrigen steht es im Belieben eines Antragstellers, seine Unterlagen mit denen der auskunftspflichtigen Stelle hinsichtlich deren Aktualität abzugleichen. Unsere Prüfung der Akte ergab, dass der Antrag auf der Grundlage des Umweltinformationsgesetzes und ggf. unter Anhörung der von der Akteneinsicht betroffenen Betreibergesellschaft hätte bearbeitet werden müssen.

Da das Amt auf unsere entsprechende Bitte wiederum nicht reagierte, die rechtlichen Kompetenzen der Landesbeauftragten damit aber erschöpft waren, baten wir die Kommunalaufsicht des Landeskreises um eine Beurteilung der Angelegenheit. Diese stimmte unserer Auffassung grundsätzlich zu und wies das Amt auf seine Informationspflichten hin. Auf Grund der langen Verzögerung waren die Informationen für die Bürgerinitiative allerdings inzwischen wertlos geworden. Dies zeigt erneut die Notwendigkeit der Einhaltung der gesetzlichen Bearbeitungsfristen.

Das Akteneinsichts- und Informationszugangsgesetz sieht eine gesetzliche Pflicht zur Unterstützung der Landesbeauftragten vor. Öffentliche Stellen werden dadurch verpflichtet, Fragen zu beantworten und ihr die Einsicht in Unterlagen zu gewähren, deren Offenlegung strittig ist. Nur so kann sie sich in Zweifelsfällen ein ausgewogenes Bild der einander entgegenstehenden Interessen machen.

2.5 Zugang einer Eigentümerin zu Grundstücksinformationen

Die Eigentümerin eines Grundstücks, das bis vor dreizehn Jahren einer Stadt gehörte, beantragte Einsicht in Unterlagen zur damaligen Genehmigung des Kaufvertrages zwischen ihr und der Stadt. Insbesondere interessierte sie sich für die Angaben zum Wert des Grundstücks. Das Ministerium des Innern sah öffentliche Interessen durch eine Herausgabe der Informationen gefährdet und bat uns um eine Einschätzung.

Nach den Vorschriften der Gemeindeordnung bedarf es für den Verkauf kommunaler Grundstücke einer Genehmigung durch die Aufsichtsbehörde. Die Unterlagen des Ministeriums, die der Aufsicht dienen, können nicht auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes eingesehen werden. Soweit allerdings der Zugang zu Daten mit Bezug zur eigenen Person beantragt wird, handelt es sich zugleich um einen datenschutzrechtlichen Informationsanspruch auf Grundlage des Brandenburgischen Datenschutzgesetzes.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse eines Betroffenen. Darunter fallen auch Angaben über den Wert eines Grundstücks. Es kommt darauf an, dass sich das Grundstück zum Zeitpunkt des Antrags auf Auskunftserteilung im Eigentum der Antragstellerin befindet. Da dies zutraf, haben auch die Wertangaben aus der Zeit, als sie noch nicht Eigentümerin war, Bezug zu den heutigen sachlichen Verhältnissen ihrer Person und sind vom datenschutzrechtlichen Auskunftsrecht umfasst.

Dem Ergebnis schloss sich das Ministerium an und gewährte Einsichtnahme in die Teile der Genehmigungsakte, die Daten zur Person der Antragstellerin beinhalteten.

Auch Grundstücksinformationen, die vor dem Erwerb des Eigentums angefallen sind, gelten als Daten mit Bezug zum derzeitigen Eigentümer. Sie sind auf der Grundlage des Brandenburgischen Datenschutzgesetzes an diesen herauszugeben.

2.6 Genehmigung einer Müllverbrennungsanlage

Ein Landkreis lehnte im Rahmen eines Genehmigungsverfahrens für eine Müllverbrennungsanlage den Antrag auf Akteneinsicht in den Vertrag mit einem Entsorgungsunternehmen ab. Nach dem Akteneinsichts- und Informationszugangsgesetz seien die überwiegenden privaten Interessen des Unternehmens zu schützen. Außerdem bestritt die Behörde, dass es sich um Umweltinformationen handelt und das Amt für Abfallwirtschaft als Umweltbehörde anzusehen ist. Das damals noch geltende Umweltinformationsgesetz habe daher nicht angewandt werden können.

Wir wiesen den Landkreis darauf hin, dass gerade ein Amt für Abfallwirtschaft auf dem Gebiet des Umweltschutzes tätig wird und es nicht der förmlichen Bezeichnung „Umweltbehörde“ bedarf, um unter den Anwendungsbereich des Umweltinformationsgesetzes zu fallen. Es genügt, dass Aufgaben des Umweltschutzes wahrgenommen werden. Ein Entsorgungsvertrag, der Angaben zum Leistungsumfang einer Abfallverwertung sowie zu den Abfallmengen beinhaltet, ist in diesem Sinne unzweifelhaft als Umweltinformation zu bewerten. Als Rechtsgrundlage hatte somit das speziellere Umweltinformationsgesetz Vorrang vor dem allgemeineren Akteneinsichts- und Informationszugangsgesetz. Danach hätte zumindest eine Abwägung zwischen dem Einsichtsinteresse der Antragsteller und dem Geheimhaltungsinteresse des Unternehmens vorgenommen werden müssen.

Da der Landkreis bei seiner Auffassung blieb, strengte der Antragsteller ein Rechtsschutzverfahren beim Verwaltungsgericht an. Das Gericht ging davon aus, dass der Antragsteller in der Hauptsache wahrscheinlich Recht bekommen würde, die Entscheidung allerdings zu spät erginge und die begehrten Informationen dann insbesondere im Hinblick auf die Absicht zur politischen Mitgestaltung wertlos wären. Zu diesem Zeitpunkt war auch das bisherige Umweltinformationsgesetz bereits außer Kraft getreten ohne dass das Land Brandenburg die neue europäische Umweltinformationsrichtlinie bereits in ein entsprechendes Landesgesetz umgesetzt hatte. Den daraus für den konkreten Fall resultierenden Rechtsunsicherheiten begegnete das Gericht mit einem Vergleich. Es schlug vor, bestimmte, als Betriebs- und Geschäftsgeheimnis zu betrachtende Regelungen des Vertrags von der Akteneinsicht auszunehmen und den Rest der Informationen zu offenbaren. Die Beteiligten haben diesem Vorschlag zugestimmt.

Das Umweltinformationsrecht geht dem Akteneinsichts- und Informationszugangsgesetz vor, wenn es sich bei den beantragten Unterlagen um Umweltinformationen handelt. Durch die noch immer ausstehende Umsetzung der europäischen Umweltinformationsrichtlinie in Landesrecht entstehen Unklarheiten.

Teil C

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Auch im zurückliegenden Berichtszeitraum hat die Dienststelle einen Aufgabenzuwachs mit gleich bleibenden Personal- und Sachmitteln bewältigen müssen. Die Zunahme der Aufgaben wird besonders deutlich an der großen Zahl der neuen IT-Vorhaben der Landesregierung, die von Projektgruppen begleitet werden, wie beispielsweise dem projektbegleitenden Ausschuss zur Kosten- und Leistungsrechnung, der Projektgruppe Meldedaten-Online, der Projektgruppe für die Errichtung eines zentralen IT-Dienstleisters oder der Arbeitsgruppe des IMA-IT zur Erarbeitung einer zentralen IT-Sicherheitsleitlinie für die Landesverwaltung. Hier ist es wichtig, bereits frühzeitig datenschutzrechtliche Fragen zu stellen und Lösungen zu erarbeiten. Auch für den Erfolg der Aktivitäten der Landesregierung zum E-Government stellt die Gewährleistung des Datenschutzes einen wesentlichen Faktor dar. Entsprechende Projekte werden von unserer Dienststelle auch in Zukunft begleitet. Es ist davon auszugehen, dass der Aufwand hierfür auf Grund der Anzahl und Komplexität der Verfahren steigen wird.

Die Umsetzung des so genannten Hartz IV-Gesetzes hat ebenfalls zu einer erheblichen Aufgabensteigerung geführt. Die Zahl der Bürgerbeschwerden ist in diesem Bereich stark angestiegen und damit auch die Notwendigkeit von Vor-Ort-Besuchen in den betroffenen Arbeitsgemeinschaften oder optierenden Gemeinden. Die unzureichenden gesetzlichen Regelungen führen zudem zu einem starken Abstimmungsbedarf mit den anderen Datenschutzbeauftragten des Bundes und der anderen Länder sowie der Bundesagentur für Arbeit. Die datenschutzrechtlichen Probleme im Bereich der Grundsicherung werden noch lange einen Schwerpunkt unserer Tätigkeit darstellen.

Personell fanden ebenfalls einige Veränderungen in der Dienststelle statt. Zum 1. April 2004 konnte eine freie Stelle durch einen erfahrenen Informatiker aus dem Hochschulbereich wieder besetzt werden. Darüber hinaus wechselte im Mai 2004 eine Mitarbeiterin der Landesverwaltung in unsere Dienststelle.

Am 2. Juni 2005 schließlich fand an der Spitze des Hauses ein Wechsel statt. Nach Ablauf seiner Amtszeit wechselte der langjährige Datenschutzbeauftragte Dr. Alexander Dix als neuer Beauftragter für Datenschutz und Informationsfreiheit nach Berlin und Dagmar Hartge trat seine Nachfolge als Landes-

beauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg an.

2 Zusammenarbeit mit dem Landtag

Der 12. Tätigkeitsbericht (2003) des Landesbeauftragten wurde im Januar und März 2005 auf der Grundlage der Stellungnahme der Landesregierung im Innenausschuss des Landtages beraten. Schwerpunkte waren die Berücksichtigung der datenschutzrechtlichen Bestimmungen zur Auftragsdatenverarbeitung in Verträgen mit Dritten und der Einsatz datenschutzfreundlicher Produkte und Verfahren in der öffentlichen Verwaltung des Landes Brandenburg. Wir setzen uns dafür ein, Produkte, die ein Gütesiegel erhalten haben, vorrangig zu berücksichtigen. Weitere Themen waren die Schaffung eines Landesumweltinformationsgesetzes sowie eine Aufforderung an die Landesregierung, sich für die Beibehaltung der differenzierten Eingriffsvoraussetzungen für die Abnahme eines Fingerabdrucks einerseits und des so genannten genetischen Fingerabdrucks andererseits in Strafverfahren einzusetzen.

Im September 2005 bat der vom Landtag eingesetzte Sonderausschuss „Normen und Standards“ die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht um einen Bericht, der sich mit der Möglichkeit einer Vereinfachung der datenschutzrechtlichen Vorschriften im Brandenburgischen Datenschutzgesetz befasst. Ziel des Sonderausschusses ist es, die Entbürokratisierung in der Verwaltung des Landes Brandenburg zu unterstützen. In unserer Stellungnahme haben wir Möglichkeiten der Vereinfachung von datenschutzrechtlichen Vorschriften aufgezeigt und Anpassungen an aktuelle Entwicklungen im Bereich der technischen Vorschriften angeregt. Das Ziel muss eine Vereinfachung und bessere Umsetzbarkeit des Datenschutzes sein. Entbürokratisierung heißt jedoch nicht, den Abbau von Datenschutz zu erreichen. Die datenschutzrechtlichen Vorschriften sind vielmehr den rechtlichen und technischen Entwicklungen regelmäßig anzupassen, denn kaum ein anderes Rechtsgebiet wird so sehr durch den schnellen technischen Fortschritt beeinflusst.

3 Kooperation mit den behördlichen Datenschutzbeauftragten

3.1 Beratung mit den behördlichen Datenschutzbeauftragten

Erneut führten wir Beratungen mit den behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größerer kreisangehöriger Gemeinden

durch. Den Beauftragten wird damit ein Forum zur Erörterung von datenschutzrechtlichen Fragen der täglichen Praxis geboten. Unsere Dienststelle erhält im Gegenzug einen Einblick in die Probleme der praktischen Umsetzung des Brandenburgischen Datenschutzgesetzes. Um den Informationsaustausch der behördlichen Datenschutzbeauftragten untereinander zu verbessern, haben wir beim Virtuellen Datenschutzbüro eine geschlossene Mailing-Liste eingerichtet, die von der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht moderiert und administriert wird.[54]

3.2 Schulung behördlicher Datenschutzbeauftragter in den Gemeinden

Auf der Ebene der Ämter und amtsfreien Gemeinden besteht bei den behördlichen Datenschutzbeauftragten zum Teil erheblicher Bedarf an Fortbildungen und Schulungen. Wir bieten daher praxisbezogene Schulungen jeweils für einen gesamten Landkreis an. Bisher haben wir Einführungslehrgänge in drei Landkreisen durchgeführt. In diesem Zusammenhang zeigte sich, dass einige Bürgermeister und Amtsdirektoren dem Datenschutz nur eine untergeordnete Bedeutung beimessen und trotz der seit 1999 bestehenden Verpflichtung immer noch keine behördlichen Datenschutzbeauftragten bestellt hatten.

Die Schulungen werden im kommenden Jahr in weiteren Landkreisen fortgesetzt. Dabei sollen auch die Zweckverbände einbezogen werden.

4 Zusammenarbeit auf nationaler und internationaler Ebene

4.1 Datenschutzbehörden

Im Berichtszeitraum fanden regelmäßig Kooperationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich – dem Ministerium des Innern – statt. Die Zusammenarbeit der beiden Aufsichtsbehörden gewinnt u. a. mit der Privatisierung öffentlicher Aufgaben immer mehr an Bedeutung. Beispielhaft sei hier die Angleichung des Datenschutzniveaus in Krankenhäusern unterschiedlicher Rechtsform genannt. Auch im Zusammenhang mit der anstehenden Novellierung des Brandenburgischen Datenschutzgesetzes fand ein intensiver Gedankenaustausch mit dem Ministerium statt.

Die gute Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde fortgeführt. Die Zusammenlegung von Landesbe-

[54] siehe http://www.datenschutz.de

hörden wie beispielsweise den Obergerichten, dem Amt für Mess- und Eichwesen oder die anstehende Fusion der statistischen Landesämter der beiden Bundesländer und die damit einhergehenden länderübergreifenden Prüfbefugnisse des jeweils zuständigen Datenschutzbeauftragten machen eine enge Abstimmung zwischen den Aufsichtsbehörden erforderlich. Auch bei inhaltlichen Fragestellungen wurde die Zusammenarbeit intensiviert, insbesondere im Bereich des Hartz IV-Gesetzes. Nur so wird es in Zukunft möglich sein, den wachsenden Aufgaben gerecht zu werden, die aus immer neuen datenschutzrechtlich relevanten Gesetzen entstehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Jahr 2004 im Frühjahr und Herbst im Saarland, im Frühjahr unter dem Vorsitz von Karl Albert und im Herbst unter dem Vorsitz seines Nachfolgers im Amt Roland Lorenz. Im Jahr 2005 tagte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Schleswig-Holstein unter dem Vorsitz von Dr. Thilo Weichert. Die Entschließungen sind in den „Dokumenten zu Datenschutz und Informationsfreiheit“ 2004 und 2005 abgedruckt, die wir gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit herausgegeben haben.

Der länderübergreifende Arbeitskreis Medien tagte in den Jahren 2004 und 2005 einmal in München und dreimal in Potsdam unter dem Vorsitz der Landesbeauftragten. Unter anderem gab er im September 2004 gegenüber der EU-Kommission in Brüssel eine Stellungnahme zur Vorratsdatenspeicherung ab.

In zahlreichen Arbeitsgruppen der Arbeitskreise der Datenschutzbeauftragten des Bundes und der Länder haben Beschäftigte der Landesbeauftragten im Berichtszeitraum mitgewirkt. Die Arbeitsgruppe Funknetze des Arbeitskreises „Technik“ erstellte unter der Leitung eines technischen Mitarbeiters der Landesbeauftragten eine Orientierungshilfe. Außerdem beteiligten sich Mitarbeiter an folgenden Arbeitsgruppen:

- Arbeitsgruppe JobCard
- Arbeitsgruppe RFID
- Arbeitsgruppe Voice over IP
- Arbeitsgruppe Gesundheitskarte
- Arbeitsgruppe E-Government
- Arbeitsgruppe Hartz-IV-Gesetze

In den genannten Arbeitsgruppen werden Orientierungshilfen verfasst oder Stellungnahmen zu bundesweiten Verfahren abgegeben. Die Arbeitsgruppen unterstützen die Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Die Zusammenarbeit der Datenschutzbeauftragten auf europäischer und internationaler Ebene wurde weiter fortgeführt. Gerade an den europäischen Richtlinien zu Ausweisen und Pässen mit biometrischen Daten oder im Bereich der Telekommunikation zu dem Thema Vorratsdatenspeicherung zeigt sich die Bedeutung der internationalen Erörterung von Datenschutzfragen. Die Zusammenarbeit auf europäischer Ebene ist für den Datenschutz nicht mehr wegzudenken.

Im Berichtszeitraum fanden im Rahmen der europäischen Konferenz der Datenschutzbeauftragten wieder regelmäßige Arbeitssitzungen des Case Handling Workshops statt, bei denen Mitarbeiter der Datenschutzbehörden Probleme der Bearbeitung von Beschwerden und Einzelfällen erörtern und sich über Lösungen zu datenschutzrechtlichen Fragestellungen austauschen. Gerade auch die Datenschutzbeauftragten der neuen EU-Mitgliedstaaten nutzen die Möglichkeiten des Erfahrungsaustausches, sodass die Teilnehmerzahl der Arbeitsgruppe in den letzten Jahren weiter angestiegen ist. Ein Mitarbeiter der Landesbeauftragten hat an allen vier Arbeitssitzungen des Workshops in den Jahren 2004 und 2005 teilgenommen.

4.2 Informationsfreiheitsbeauftragte

Die Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland, bestehend aus den Informationsfreiheitsbeauftragten der Bundesländer Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein, hat sich im Berichtszeitraum unter wechselndem Vorsitz zu vier Sitzungen getroffen und insgesamt sechs Entschließungen verabschiedet. Alle Entschließungen sind in den „Dokumenten zu Datenschutz und Informationsfreiheit“ abgedruckt. Im März 2005 hat die Arbeitsgemeinschaft unter dem Vorsitz des Landesbeauftragten, Dr. Dix, eine Stellungnahme zum Entwurf eines Informationsfreiheitsgesetzes abgegeben und im Anhörungsverfahren vor dem Innenausschuss des Bundestages vorgetragen. Nachdem das Informationsfreiheitsgesetz im Sommer 2005 verabschiedet wurde, trat der Bundesbeauftragte für den Datenschutz in die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland ein. Das Informationsfreiheitsgesetz des Bundes ist am 1. Januar 2006 in Kraft getreten.

Am 25. November 2005 wurde in Berlin die Konferenz der europäischen Informationsfreiheitsbeauftragten gegründet. Die Landesbeauftragte ist eines der Gründungsmitglieder der europäischen Konferenz. Die Konferenz hat sich u. a. zum Ziel gesetzt, die Informationsfreiheit in Europa zu fördern und das Recht auf freien Informationszugang zu harmonisieren. Das Gründungspapier ist in den „Dokumenten zu Datenschutz und Informationsfreiheit 2005“ abgedruckt.

5 Öffentlichkeitsarbeit

5.1 Internationales Symposium zur Informationsfreiheit

Am 28. und 29. September 2005 veranstaltete die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht erneut ein Internationales Symposium in Potsdam. Diese alle zwei Jahre stattfindende Veranstaltungsreihe dient dem Erfahrungsaustausch zwischen Brandenburg und den Nachbarländern Ost- und Mitteleuropas unter Einbeziehung der Ebene der Europäischen Union. Das diesjährige Symposium stand unter dem Titel „Informationsfreiheit in Deutschland und Europa“. Ein Schwerpunkt war das bevorstehende In-Kraft-Treten des Informationsfreiheitsgesetzes der Bundesrepublik Deutschland. Brandenburg konnte auf der Veranstaltung als „Pionierland“ des Informationszugangs in Deutschland seine Erfahrungen einbringen.

Experten aus Brandenburg, der Bundesrepublik, den jüngst der Europäischen Union beigetretenen Staaten sowie aus Bulgarien und der Ukraine stellten die aktuellen Entwicklungen des Informationsfreiheitsrechts in ihren Ländern dar. Der Umgang mit Umweltinformationen kam ebenso zur Sprache wie Grundsätze zur Transparenz staatlichen Handelns in der Europäischen Union und die Kommerzialisierung öffentlicher Informationen. Auch die Bedeutung der Informationsfreiheit für den Journalismus sowie als Instrument der Korruptionsbekämpfung war Gegenstand von eigenen Beiträgen. So unterschiedlich wie die Herkunft und Aufgabe der Referenten waren auch deren Vorstellungen und Ziele. Dies führte zu einer lebhaften Diskussion, an der sich Vertreter von Bürgerinitiativen und Verbänden sowie Regierungsvertreter und Wissenschaftler beteiligten.

Das zweitägige Internationale Symposium mit seinen rund 120 Teilnehmern wurde gemeinsam mit der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik e. V. veranstaltet. Die Vorträge des Symposiums werden in einer Broschüre und auf unserer Website veröffentlicht.

5.2 Die Landesbeauftragte auf dem Brandenburg-Tag und dem Bürgerfest am Tag der Deutschen Einheit

Im Jahr 2004 fand der Brandenburg-Tag in Eberswalde statt. Rund um das Gelände der ehemaligen Landesgartenschau präsentierten sich die brandenburgischen Regionen, ihre Wirtschaft sowie Handwerk, Bildung, Wissenschaft und Kultur. Vertreter aus Vereinen, Verbänden und der öffentlichen Hand informierten über ihre Aufgaben. Auch die Landesbeauftragte war in Eberswalde präsent, um mit Bürgerinnen und Bürgern ins Gespräch zu kommen.

Fünfzehn Jahre nach der Wiedervereinigung Deutschlands war die Landeshauptstadt Potsdam 2005 Gastgeberin der zentralen Feierlichkeiten zum Tag der Deutschen Einheit. Das Bürgerfest am 2. und 3. Oktober 2005 in Potsdam erfreute sich eines noch stärkeren Besucherzustroms als der Brandenburg-Tag im Vorjahr. Dementsprechend war der Stand der Landesbeauftragten gut besucht. Eine Vielzahl von Gästen nutzte die Gelegenheit, sich nach ihrem Recht auf Datenschutz und Akteneinsicht zu erkundigen. Häufig wurden wir Folgendes gefragt:

- Was tun gegen unerwünschte Werbung?
- Darf die GEZ meine Daten verarbeiten, wenn ich gar keinen Fernseher habe?
- Was hat es mit der geplanten Gesundheitskarte auf sich?
- Muss ich bei der Beantragung von Arbeitslosengeld II wirklich alle Fragen beantworten?
- Wie kann ich ohne Gefahren für die Vertraulichkeit und Sicherheit meiner Daten im Internet surfen?

Der nächste Brandenburg-Tag findet am 2. September 2006 in Forst (Lausitz) statt. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird dort wieder mit einem Informationszelt präsent sein und sich den Fragen interessierter Brandenburgerinnen und Brandenburger stellen.

5.3 Barrierefreie Website der Landesbeauftragten

Nachdem die Neugestaltung der Website der Landesbeauftragten bereits im Dezember 2003 abgeschlossen war und sie seitdem mit einem neuen Layout und einer übersichtlicheren Navigation zur Verfügung steht, wurden nun noch einige technische Barrieren für eine ungehinderte Nutzung aus dem Weg geräumt. Insbesondere ging es darum, auch Sehbehinderten den Zugang zu unseren Informationen im Internet zu ermöglichen.

Am 24. Mai 2004 ist die Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Brandenburgischen Behindertengleichstellungsgesetz erlassen worden. Sie gilt unter anderem für die Internetauftritte der Landesbehörden und verpflichtet diese, bestimmte, in der Verordnung definierte Anforderungen zu erfüllen, um behinderten Menschen den Zugang zu diesen Seiten zu erleichtern.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht misst der Umsetzung dieser Verordnung hohe Priorität bei. Sie ist der Auffassung, dass Verwaltungen dem allgemeinen Informationszugangsrecht nur dann vollständig nachkommen, wenn sie öffentliche Informationen im Internet publizieren und einem möglichst breiten Nutzerkreis zugänglich ma-

chen. Die technische Umsetzung eines möglichst barrierefreien Zugangs ist bei umfangreichen Internetangeboten mit hohem Aufwand verbunden. So weit, wie dies möglich war, wurde die Website der Landesbeauftragten bis zum Ende des Jahres 2005 nach den Kriterien der Verordnung gestaltet. Kritik und Anregungen zum Ergebnis sind jederzeit willkommen.

5.4 Aktuelle Publikationen der Landesbeauftragten

Einige Publikationen der Landesbeauftragten waren im Verlauf des zurückliegenden Berichtszeitraums schnell vergriffen. Die Gesetzesbroschüre zum Archivrecht sowie das Brandenburgische Datenschutzgesetz stehen mittlerweile wieder mit den aktualisierten Gesetzestexten zur Verfügung. Das Akteneinsichts- und Informationszugangsgesetz, das Informationsfreiheitsgesetz des Bundes sowie eine Broschüre zum Umweltinformationsrecht werden in den kommenden Monaten herausgegeben.

Ein neues Faltblatt zum Thema „Datenschutz und Akteneinsicht in Brandenburg“ wurde in größerer Auflage herausgegeben und an alle öffentlichen Stellen in Brandenburg mit Publikumsverkehr versandt. Wir haben diese Einrichtungen darum gebeten, das Faltblatt auszulegen, damit interessierte Bürgerinnen und Bürger bereits vor Ort erste Hinweise zu ihren Rechten auf Datenschutz und Informationszugang erhalten. Gerne stellen wir das Faltblatt auf Anfrage auch in höherer Stückzahl zur Verfügung.

Darüber hinaus haben wir zwei weitere Faltblätter veröffentlicht: „Schon GEZahlt? Acht Antworten zum Datenschutz bei der GEZ“ sowie „Meine Datenschutzrechte als Telefonkunde“. Das gemeinsam mit anderen Landesbeauftragten herausgegebene Merkblatt „Tipps und Informationen zu Adresshandel und unerwünschter Werbung“ wurde in einer aktualisierten Version neu aufgelegt.

Die Vorträge, die auf dem Internationalen Symposium „Informationsfreiheit in Deutschland und Europa“ am 28./29. September 2005 gehalten wurden, haben Eingang in eine gedruckte Dokumentation der Veranstaltung gefunden.

Die „Dokumente zu Datenschutz und Informationsfreiheit“ enthalten Entschließungen verschiedener nationaler, europäischer und internationaler Gremien, die sich mit den Themen Datenschutz und Informationsfreiheit befassen und stellen eine Ergänzung des bislang jährlich erschienenen Tätigkeitsberichts dar. Wir haben diesen Band gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit herausgegeben.

Nachdem der Berichtszeitraum des Tätigkeitsberichts der Landesbeauftragten von einem auf zwei Jahre geändert wurde, fällt er mit dem des Berliner

Beauftragten für Datenschutz und Informationsfreiheit, der bei seinem jährlichen Rhythmus bleibt, auseinander. Der Tätigkeitsbericht 2004/2005 wird daher in diesem Jahr ausnahmsweise zusammen mit zwei einzelnen Jahresbänden dieser Dokumentation ausgeliefert. Allerdings beteiligen wir uns künftig nicht mehr an der Herausgabe. Nach wie vor veröffentlichen wir aktuelle Dokumente aber ebenso wie alle anderen erwähnten Publikationen auf unserer Website.

Anlagen

Anlage 1

Auszug aus dem Geschäftsverteilungsplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Stand: 15. Februar 2006

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht	Dagmar Hartge
Stellvertreter	Herr Urban
Sekretariat	Frau Objartel App. 10

Bereich Recht und Verwaltung

Bereichsleiter	Herr Dr. Jendro App. 34
Arbeitsgebiete: - Rechtliche Grundsatzfragen - Wissenschaft, Forschung und Kultur - Justiz und Europaangelegenheiten (außer Staatsanwaltschaften) - Landesrechnungshof - Landtag, Staatskanzlei - Beauftragter des Haushalts	
Arbeitsgebiete: - Telekommunikation und Medien - Kommunalrecht - Rechtsfragen der elektronischen Verwaltung (E-Government) - Internationaler und europäischer Datenschutz	Herr Hermerschmidt App. 40
Arbeitsgebiete: - Polizei, Verfassungsschutz - Verkehrsordnungswidrigkeiten - Ausländer, Asylverfahren - Staatsanwaltschaften - Presse- und Öffentlichkeitsarbeit	Frau Schraut App. 41

Arbeitsgebiete: App. 45
- Landwirtschaft, Umweltschutz und Raumordnung
- Stadtentwicklung, Wohnen und Verkehr
- Personaldaten allgemein

Arbeitsgebiete: Herr S. Müller
- Akteneinsicht und Informationszugang App. 20
- Verwaltungsmodernisierung
- Redaktion von Veröffentlichungen
- Koordination des Internetangebots
- Internationaler und europäischer Informationszugang

Arbeitsgebiete: App. 22
- Bildung, Jugend und Sport

Arbeitsgebiete: App. 44
- Gesundheit
- Gesundheitsdaten allgemein

Arbeitsgebiete: Frau Oehme
- Arbeit, Soziales und Familie App. 66
- Sozialdaten allgemein
- Finanzen

Arbeitsgebiete: Herr Hoff
- Inneres App. 36
- Wirtschaft

Arbeitsgebiete: App. 12
- Personal- und Verwaltungsangelegenheiten
- Büroleitungsaufgaben
- Haushaltsangelegenheiten
- Beschaffungen

Arbeitsgebiete: App. 43
- Bibliothek
- Schreibdienst
- Informationsmaterialien

Bereich Technik und Organisation

Bereichsleiter	Herr Urban App. 30
Arbeitsgebiete: - Technisch/organisatorische Grundsatzfragen - komplexe IT-Verfahren - Videoüberwachung - Dokumentenmanagementsysteme - interne TK-Anlagen	
Arbeitsgebiete: - kryptographische Verfahren und elektronische Signaturen - Kartentechnologien - Kommunikationsnetze - Verzeichnisdienste	App. 32
Arbeitsgebiete: - Personalinformationssysteme - elektronische Akteneinsicht - Datenbanksysteme - Wartung und Fernwartung	Herr Dr. Reinke App. 31
Arbeitsgebiete: - Statistik - Umgang mit Datenträgern - Datenschutzaudit - Isolierte und vernetzte PC	App. 33
Arbeitsgebiete - Einsatz von IT-Sicherheitsprodukten - Risikoanalysen und Sicherheitskonzepte - Organisations- und Dienstanweisungen - Gebäudesicherung - Computerviren	Herr Budszus App. 35
Arbeitsgebiete: - Schreibdienst - Mitarbeit bei der Öffentlichkeitsarbeit	App. 42

Gleichstellungsbeauftragte	App. 12
Personalrat	App. 45
Behördlicher Datenschutzbeauftragter	Herr Hermerschmidt App. 40

Anlage 2

Aktenplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Problemkreis	Bezeichnung
002	Akteneinsichts- und Informationszugangsgesetz
003	Arbeit
008	Ausländer
009	Bau-/Wohnungswesen
010	Landesregierung
024	Landtag/Parteien
027	Bildung/Kultur/Wissenschaft
028	BRD/Bund/Bundesländer
034	Allgemeines Datenschutzrecht
046	Zusammenarbeit Bundesbeauftragter für den Datenschutz/ Landesbeauftragte für den Datenschutz
054	Dateienregister LDA
056	Internationale Datenschutzangelegenheiten
061	Finanzen
062	Ernährung/Landwirtschaft/Forsten
066	Gesundheitswesen
078	Familie/Frauen/Jugend
082	Justiz
086	Kommunalrecht
089	Interne Verwaltung LDA
100	Öffentlichkeitsarbeit LDA
104	Inneres
108	Personaldatenverarbeitung
110	Polizei
128	Sozialwesen
132	Statistik
135	Technik
136	Medien/Telekommunikation/Post
138	Umwelt/Raumordnung/Stadtentwicklung
146	Verfassungsschutz
147	Verkehr
154	Wirtschaft/Technologie
163	Nicht öffentlicher Datenschutz
180	Personalräte
999	Sonstiges

Abkürzungsverzeichnis

Abs.	=	Absatz
AN.ON	=	Anonymität Online
AO	=	Abgabenordnung
APSIS	=	Automatisierte Personalverwaltung und Stellenbewirtschaftung im Schulamt
AufenthG	=	Aufenthaltsgesetz
BAföG	=	(Förderung nach dem) Bundesausbildungsförderungsgesetz
BALVI iP	=	Bundeseinheitliche Anwendung zur Lebensmittel- und Veterinär-Information, integriertes Programm
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgMeldG	=	Brandenburgisches Meldegesetz
BGBl.	=	Bundesgesetzblatt
BIOS	=	Basic Input Output System
BKA	=	Bundeskriminalamt
BOA	=	Brandenburger Online Amt
BOS	=	Behörden und Organisationen mit Sicherheitsaufgaben
BRAVORS	=	Brandenburgische Vorschriftensammlung
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
bzw.	=	beziehungsweise
CDU	=	Christlich Demokratische Union
CERT	=	Computer Emergency Response Team
DAV	=	Dienstanschlussvorschrift
DNA	=	Desoxyribonuclein Acid (Desoxyribonukleinsäure)
d. h.	=	das heißt
EPA	=	elektronische Patientenakte
e. V.	=	eingetragener Verein
FIFA	=	Fédération Internationale de Football Association (Internationaler Fußballverband)
ff.	=	fortfolgende
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GVBl.	=	Gesetz- und Verordnungsblatt
ICAO	=	International Civil Aviation Organisation (Internationale Organisation für zivile Luftfahrt)
i. d. R.	=	in der Regel
IMA-IT	=	Interministerieller Ausschuss für Informationstechnik
IP	=	Internet Protocol
IPSec	=	Internet Protocol Security

i. S. v.	=	im Sinne von
IT	=	Informationstechnik
KAN	=	Kriminalaktennachweis Land/Bund
KLR	=	Kosten- und Leistungsrechnung
LDG	=	Landesdisziplinargesetz
LDS	=	Landesbetrieb für Datenverarbeitung und Statistik
MDStV	=	Mediendienste-Staatsvertrag
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
Nr.	=	Nummer
OSCI	=	Online Services Computer Interface
PASS	=	Polizeiliches Auskunftssystem Straftaten
PayTV	=	Bezahlfernsehen
PDA	=	Personal Digital Assistant
PGP	=	Pretty Good Privacy
PIN	=	persönliche Identifikationsnummer
Pkt.	=	Punkt
RBB	=	Rundfunk Berlin-Brandenburg
RFID	=	Radio Frequency Identification
SMS	=	Short Message Service
SPD	=	Sozialdemokratische Partei Deutschlands
SSL	=	Secure Socket Layer
StPO	=	Strafprozessordnung
sog.	=	so genannte
TDDSG	=	Teledienstedatenschutzgesetz
TKG	=	Telekommunikationsgesetz
u. a.	=	unter anderem
USB	=	Universal Serial Bus
usw.	=	und so weiter
u. U.	=	unter Umständen
vgl.	=	vergleiche
Viper	=	Verfassungsschutz-Informationsportal für Ermittlung und Recherche
VNC	=	Virtual Network Computing
VoIP	=	Voice over IP
WLAN	=	Wireless Local Area Network
WM 2006	=	Weltmeisterschaft 2006
WSUS	=	Windows Server Update Service
z. B.	=	zum Beispiel

Stichwortverzeichnis