Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2003

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung jährlich einen Bericht über seine Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz; § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 12. März 2003 vorgelegten Tätigkeitsbericht 2002 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2003 ab.

Die „Dokumente zu Datenschutz und Informationsfreiheit 2003“, auf die in diesem Bericht verwiesen wird, hat der Landesbeauftragte gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit als gesonderten Anlagenband veröffentlicht. Tätigkeitsbericht und Anlagenband sind aus unserem Internetangebot unter http://www.lda.brandenburg.de abrufbar.

Impressum

Herausgeber: Der 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: Brandenburgische Universitätsdruckerei und
Verlagsgesellschaft Potsdam mbH

Inhaltsverzeichnis Seite

Teil C
Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Anlagen

Verzeichnis der öffentlichen Stellen **Gliederungspunkt**

Einleitung

Die Bilanz des Jahres 2003 für Datenschutz und Akteneinsicht in Brandenburg ist alles andere als ausgeglichen. Als wichtigster Posten auf der passiven Seite der Bilanz muss die wachsende Tendenz zur präventiven, anlassunabhängigen Sammlung und Speicherung von Bürgerdaten genannt werden.

Diese Tendenz beschränkt sich allerdings nicht auf Brandenburg. So hat sich der Bundesrat mit den Stimmen Brandenburgs dafür ausgesprochen, die Anbieter von Telekommunikationsdiensten zur routinemäßigen Speicherung aller anfallenden Verkehrsdaten in den Telefonnetzen und im Internet für ein halbes Jahr zu verpflichten, um mögliche Strafverfolgungsmaßnahmen in der Zukunft zu erleichtern.

Gegen Ende des Berichtszeitraumes wurde bekannt, dass das Innenministerium bereits eine Technik erprobt hat, mit deren Hilfe Kraftfahrzeug-Kennzeichen automatisiert gelesen und erfasst werden können. Das Ministerium hält den Einsatz dieser Technik zur Bekämpfung des Autodiebstahls für wünschenswert. Auch hier geht es nicht um den Einsatz von Kameras bei konkreten Verdachtsmomenten oder im Rahmen von Kontrollstellen, die das geltende Recht bereits zulässt. Vielmehr sollen generell an Hauptverkehrsstraßen und Autobahnbrücken alle vorbeifahrenden Fahrzeuge erfasst und mit dem Fahndungsbestand des Bundeskriminalamtes abgeglichen werden. Der unbescholtene Bürger habe nichts zu befürchten, weil sein Kennzeichen nicht gespeichert bleibe. Dabei wird übersehen, dass der Staat bereits mit der automatisierten Beobachtung aller seiner Bürger in deren Grundrechte auf Datenschutz und Freizügigkeit eingreift. Die Ergebnisse dieser flächendeckenden Kontrollinfrastruktur würden zudem mit Sicherheit nicht nur zur Aufdeckung und Verhinderung von Autodiebstählen genutzt, eine Kriminalitätsform, die durch Maßnahmen der Autohersteller wie die Wegfahrsperre ohnehin bereits stark rückläufig ist.

Ein anderes Beispiel für die Tendenz zur präventiven Vorratsspeicherung ist die Absicht des amerikanischen Heimatschutzministeriums, die Daten sämtlicher Flugpassagiere, die in die USA reisen, aus den Reservierungssystemen der Fluggesellschaften abzurufen, um auf diese Weise Hinweise auf geplante terroristische Anschläge zu gewinnen, aber auch die organisierte Kriminalität und „andere schwerwiegende Straftaten“ zu bekämpfen. Diese Daten sollen für dreieinhalb Jahre bei den amerikanischen Behörden selbst dann gespeichert bleiben, wenn der Passagier die USA verlassen hat, ohne Straftaten zu begehen. Fluggesellschaften, die den amerikanischen Behörden den Zugriff auf ihre Reservierungssysteme untersagen wollten, wurden mit Landeverboten bedroht. Die europäischen Datenschutzbeauftragten, die die Datenverar-

beitung bei den Fluggesellschaften zu kontrollieren haben, halten diese weit reichende Datenspeicherung auch vor dem Hintergrund des unzureichenden Datenschutzniveaus in den Vereinigten Staaten für nicht akzeptabel. Es kann zwar keinem Staat verwehrt werden, von einreisenden Personen ein Visum zu verlangen und hierfür die wenigen notwendigen Daten offen zu erheben, um sie kurze Zeit nach der Ausreise wieder zu löschen. Das jetzt vorgesehene Verfahren geht jedoch weit darüber hinaus; es ist deshalb sowohl von der Internationalen Konferenz der Datenschutzbeauftragten[1] als auch vom Europäischen Parlament[2] abgelehnt worden.

Allen diesen Forderungen und konkreten Planungen liegt die Vorstellung zu Grunde, dass moderne Formen der Datenerfassung und -verarbeitung für eine präventive Vorratsdatenhaltung genutzt werden sollen, auch wenn dies die Grenzen der Verhältnismäßigkeit sprengt. Doch nicht alles, was technisch möglich ist und der Arbeit von Polizei und Strafverfolgungsbehörden nützt, ist auch notwendig und in einem Rechtsstaat hinnehmbar.

Nach den Vorstellungen des brandenburgischen Justizministeriums sollen überdies DNA-Analysen nicht mehr von einer Prognoseentscheidung des Richters abhängen, sondern von jedem Polizisten auch gegen den Willen des Betroffenen angeordnet werden können. Der Richtervorbehalt, den das Bundesverfassungsgericht als grundrechtssicherenden Verfahrensschritt bezeichnet hat, wird vom Justizministerium lediglich als bürokratisches Hemmnis für die Strafverfolgung gesehen und soll deshalb entfallen. Auch hier muss sich noch die Erkenntnis durchsetzen, dass es in einem Rechtsstaat keine Strafverfolgung um jeden Preis geben kann. Die modernen Methoden der DNA-Analyse liefern zwangsläufig mehr Informationen als jeder herkömmliche Fingerabdruck und diese Informationsfülle nimmt auf Grund der schnell voranschreitenden Erforschung des menschlichen Genoms weiter zu. Genau aus diesem Grund sind die bestehenden rechtsstaatlichen Verfahrenssicherungen, zu denen der Richtervorbehalt zählt, unverzichtbar.

Negativ schlägt außerdem zu Buche, dass die dringend notwendige Modernisierung des Datenschutzrechts auf Bundesebene und damit auch in Brandenburg nicht vorankommt. Zudem wurden beim mehrfach angekündigten Bundesinformationszugangsgesetz keine erkennbaren Fortschritte gemacht. Die Bundesregierung hat zwar Anfang September 2003 ein Aktionsprogramm „Informationsgesellschaft Deutschland 2006“ beschlossen, das einen Überblick über sämtliche vorhandenen und geplanten elektronischen Dienstleistungsangebote in Verwaltung, Wirtschaft und Gesundheitswesen enthält[3].

---

1 vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A III 1

2 s. Entschließung vom 9. Oktober 2003, BR-Drs. 857/03

3 s. Aktionsprogramm „Informationsgesellschaft Deutschland 2006“ – ein Masterplan für Deutschlands Weg in die Informationsgesellschaft, BR-Drs. 976/03

Nach Auffassung der Bundesregierung zeigen wichtige Indikatoren für den „Reifegrad“ der globalen Informationsgesellschaft, das Deutschland in den letzten Jahren deutlich vorangekommen ist. Die Vielzahl der Projekte und bereits realisierten Angebote erscheint auf den ersten Blick beeindruckend. Die geplante Einführung von 40 Millionen Job-Karten und 80 Millionen Gesundheitskarten im Laufe der kommenden zwei Jahre macht die Bundesrepublik aber nicht schon zu einer modernen Informationsgesellschaft. Ein wesentlicher Pfeiler fehlt, solange es keinen bundesweiten Rechtsanspruch der Bürgerinnen und Bürger zum Zugang zu Verwaltungsinformationen gibt. Es muss befremden, dass die Bundesregierung das notwendige Informationszugangsgesetz in den Aktionsprogramm „Informationsgesellschaft Deutschland 2006“ nicht einmal erwähnt.

Auch die Landesregierung hat die Aufstellung eines Masterplanes zu E-Government beschlossen, an der sich der Landesbeauftragte im Rahmen seiner Möglichkeiten beteiligt. Wichtig ist in diesem Zusammenhang, dass alle angebotenen und geplanten elektronischen Behördendienste die Vorgaben des Datenschutzrechts und der Datensicherheit bereits im Entwurfsstadium berücksichtigen. Der amerikanische Kongress hat in einem speziellen Gesetz zur Regelung elektronischer Behördendienste sogar eine Datenschutz-Folgenabschätzung (Privacy Impact Assessment) vorgeschrieben[4]. Das vom Brandenburgischen Landtag beschlossene Gesetz über Ziele und Vorgaben zur Modernisierung der Landesverwaltung[5] sieht immerhin vor, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht über die Modernisierungsvorhaben der Landesregierung zu informieren ist. Der Landesbeauftragte wird diese Beteiligung dazu nutzen, die Landesregierung auf die Folgen der einzelnen Vorhaben für den Datenschutz und Möglichkeiten der datenschutzgerechten Gestaltung hinzuweisen.

Positiv zu bewerten ist zudem, dass der Landtag gegen den Widerstand der Landesregierung eine einmonatige Bescheidungsfrist in das Akteneinsichts- und Informationszugangsgesetz aufgenommen und die Information für Bürger, deren Antrag auf Akteneinsicht abgelehnt worden ist, verbessert hat. Damit ist ein kleiner Teil der Vorschläge des Landesbeauftragten aus dem Jahr 2000 umgesetzt worden. Weitere Schritte zur verfassungskonformen Stärkung des Akteneinsichtsrechts sind notwendig.

In der Diskussion über die Modernisierung der Verwaltung und die Einführung von elektronischen Behördendiensten (E-Government) wird häufig davon gesprochen, die Verwaltung müsse stärker „kundenorientiert“ arbeiten und den Bürger wie ein Unternehmen als Kunden verstehen. Bürger sind aber mehr als Kunden oder Leistungsempfänger, sie sind letztlich der Arbeitgeber oder

4 E-Government Act 2002, H.R. 2458, Sec. 208

5 Artikel 2 des Haushaltssicherungsgesetzes 2003, § 13, GVBl. I S. 194

„Dienstherr“ der Verwaltung, sie sind der Souverän. Ein bekanntes Mitglied des brandenburgischen Landesverfassungsgerichts hat es so formuliert: „.....erst Partizipation, die Teilnahme und Anteilnahme an den öffentlichen Angelegenheiten, macht aus Untertanen Bürger“[6]. Dazu sind der Datenschutz und das Recht auf Akteneinsicht wesentliche Voraussetzungen.

[6] vgl. Richard Schröder, Der Stempel der Freiheit, Der Tagesspiegel vom 9. November 2003

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Entwicklung des Datenschutzrechts – kaum Fortschritte in Sicht

Die Entwicklung der allgemeinen Datenschutzgesetzgebung stagnierte im Berichtszeitraum auf Bundes- wie auf Landesebene. Die Bundesregierung hat weder einen Entwurf für ein Datenschutzaudit-Gesetz vorgelegt, noch hat sie erkennbar die notwendige zweite Stufe der Modernisierung des Bundesdatenschutzgesetzes weiter betrieben. Das ist allerdings dringend erforderlich, weil das gegenwärtige Datenschutzrecht der Vereinfachung und Anpassung an die Rahmenbedingungen der entstehenden Informationsgesellschaft bedarf. Das Datenschutzrecht muss sowohl im Bereich der öffentlichen Verwaltung als auch in der Privatwirtschaft die Möglichkeiten der Bürgerinnen und Bürger zum Selbstschutz deutlich verbessern, zugleich aber auch ein Mindestniveau für den Schutz der informationellen Selbstbestimmung desjenigen vorsehen, der keine eigene Entscheidung über den Umgang mit seinen Daten treffen will oder kann.

In einem Punkt zeichnet sich allerdings ein Fortschritt bei der Bundesgesetzgebung ab, für den sich der Landesbeauftragte seit längerem eingesetzt hat: Nach den Bundestagsfraktionen der FDP und CDU/CSU hat jetzt auch der Bundesrat einen Gesetzentwurf zur Änderung des Strafrechts – Schutz der Intimsphäre – beschlossen[7] und in den Deutschen Bundestag eingebracht. Ziel dieses Gesetzentwurfes ist es, eine eklatante Strafbarkeitslücke bei der Missachtung des Rechts am eigenen Bild zu schließen. Bisher ist lediglich die Verbreitung von Fotografien, die verdeckt oder gegen den Willen der abgebildeten Person gemacht worden sind, nach dem Kunsturhebergesetz von 1907 mit Strafe bedroht. Die atemberaubende technische Entwicklung ermöglicht es heute bereits, mit Hilfe von Fotohandys geschossene Bilder mit einem Tastendruck Freunden oder beliebigen anderen Personen über das Mobilfunknetz zu schicken oder mit Digitalkameras gemachte Fotos in sekundenschnelle im Internet zum weltweiten Abruf bereitzustellen. Damit ist es nicht länger hinnehmbar, die unbefugte und die Intimsphäre verletzende Herstellung von Fotografien solange von der Strafandrohung auszunehmen, wie keine Weiterverbreitung oder Veröffentlichung erfolgt. Bereits das heimliche Fotografieren von Personen (z. B. in Toiletten oder Umkleidekabinen) ist eine so

[7] s. BT-Drs. 15/1891

eklatante Verletzung der Privatsphäre des betroffenen Menschen, dass der Staat dies nicht dulden darf. Das gilt erst recht, wenn die Veröffentlichung einer Fotografie sich unmittelbar an ihre Herstellung anschließt. Der Gesetzentwurf des Bundesrates sieht vor, dass jeder, der eine andere Person in einer Wohnung oder einem gegen Einblick besonders geschützten Raum unbefugt fotografiert oder derartige Fotografien überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft wird. Das Gleiche gilt für den, der eine so hergestellte Aufnahme gebraucht oder Dritten zugänglich macht. Die Bundesregierung hat in ihrer Stellungnahme dem Anliegen des Gesetzentwurfes grundsätzlich zugestimmt[8]. Auch sie sieht die Notwendigkeit, die beschriebene Strafbarkeitslücke zu schließen und betrachtet den Gesetzentwurf als gute Diskussionsgrundlage. Es ist zu hoffen, dass der Deutsche Bundestag den Gesetzentwurf unter Berücksichtigung der von der Bundesregierung genannten Gesichtspunkte alsbald verabschiedet.

Das Strafrecht als schärfstes Mittel staatlicher Reaktion reicht sicherlich nicht aus, um den Einsatz einer das Recht am eigenen Bild verletzenden Technik wirksam zu unterbinden. Vielmehr sollten auch die Hersteller von vornherein auf eine datenschutzfreundliche Gestaltung ihrer Produkte achten. So ist in der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation, an der sich auch der Landesbeauftragte beteiligt, der Vorschlag gemacht worden, Fotohandys sollten ein optisches oder akustisches Signal aussenden, wenn mit ihnen auch oder ausschließlich fotografiert wird. Dieser Vorschlag ist mittlerweile zumindest von einem Hersteller aufgegriffen worden. Damit wird zumindest die Wahrscheinlichkeit erhöht, dass Unbeteiligte nicht ohne ihr Wissen oder gegen ihren Willen mit einem Fotohandy fotografiert werden. Sowohl Digitalkameras als auch Fotohandys sind heutzutage so stark miniaturisiert, dass ihr Einsatz häufig nicht bemerkt wird. Hinzu kommt bei Fotohandys, dass Menschen in unmittelbarer Nähe eines Nutzers nicht erkennen können, ob dieser nur telefoniert oder auch Bildaufnahmen mit dem Handy macht.

Auf Landesebene ist das Problem einer einheitlichen unabhängigen Datenschutzkontrolle im öffentlichen und nicht-öffentlichen Bereich noch immer ungelöst. Nachdem der Landesbeauftragte sich im Tätigkeitsbericht 2002 für eine Konzentration der Kontroll- und Beratungsaufgaben in seiner Dienststelle ausgesprochen hatte, beschränkte sich die Landesregierung auf die Feststellung, ihre Stellungnahme zum Tätigkeitsbericht sei „nicht der geeignete Ort“, um die Frage einer solchen Aufgabenbündelung zu klären und zu entscheiden. Ob die Landesregierung die Klärung und Entscheidung dieser offenen Frage an einem anderen, nach ihrer Auffassung geeigneteren Ort vorangetrieben hat, ist nicht bekannt. Soweit die Landesregierung darauf verweist,

[8] s. BT-Drs. 15/1891, 9

sie äußere sich in ihrer Stellungnahme nur zu Fragen, die sich aus den gesetzlichen Zuständigkeiten des Landesbeauftragten ergeben[9], ist daran zu erinnern, dass der Landesbeauftragte nach dem Brandenburgischen Datenschutzgesetz Empfehlungen zur Verbesserung des Datenschutzes geben kann (§ 23 Abs. 2). Dass eine Bündelung der Zuständigkeit für den Datenschutz im öffentlichen und privatwirtschaftlichen Bereich bei der nach der Landesverfassung dafür vorgesehenen unabhängigen Instanz mit ihrem technischen und rechtlichen Sachverstand den Datenschutz verbessern würde, ist offensichtlich.

Zudem liegt inzwischen der Europäischen Kommission eine Beschwerde aus der Bundesrepublik Deutschland vor, in der auf die mangelnde Unabhängigkeit der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hingewiesen wird. Zum einen ist zweifelhaft, ob die Befugnis des Landesbeauftragten, Beanstandungen auszusprechen, dem gemeinschaftsrechtlichen Erfordernis einer „wirksamen Einwirkungsbefugnis“ genügt. Zum anderen hat der Landesbeauftragte seine Auffassung bekräftigt, dass die Einbindung der Aufsichtsbehörde für den Datenschutz in der Privatwirtschaft in das Ministerium des Innern nicht der ausdrücklichen Vorgabe der Richtlinie genügt, dass die Kontrollstellen die ihnen zugewiesenen Aufgaben in „völliger Unabhängigkeit“ wahrzunehmen haben[10]. Auch der Konventsentwurf vom Juni 2003 für eine Europäische Verfassung sieht die Überwachung der Einhaltung des Datenschutzrechts durch eine unabhängige Behörde vor[11].

Die Landesregierung sollte den Ausgang dieses Beschwerdeverfahrens allerdings nicht abwarten. Denn selbst wenn die Europäische Kommission den deutschen Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft, soweit sie in ministerielle Weisungsstränge eingebunden sind, eine „völlige Unabhängigkeit“ bescheinigen sollte, ist eine Bündelung der Beratungs- und Kontrollaufgaben an einer Stelle sinnvoll.

1.2 Outsourcing der Datenverarbeitung – „verdunstet“ die Verantwortung?

Auch im Land Brandenburg sollen künftig verstärkt IT-Bereiche der öffentlichen Verwaltung ausgelagert und Dienstleistern zur Auftragsdatenverarbeitung übergeben werden. Im Zuge der Polizeistrukturreform ist dies bereits geschehen[12]. Landkreise und Gemeinden erhoffen sich von einer solchen Fremdvergabe erhebliche Kosteneinsparungen. Die Aus-

9 s. Drs. 3/6134, S. 10

10 Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG

11 Artikel 50 Abs. 2

12 vgl. dazu näher A 4.1.3

gliederung der Datenverarbeitung (Outsourcing) beinhaltet neben den erhofften Vorteilen aber auch eine große Anzahl von Risiken, die es zu beherrschen gilt.

Outsourcing erfreut sich in Zeiten knapper Kassen und Umstrukturierungen immer größerer Beliebtheit. Im Rahmen einer Umfrage[13] gaben 73 Prozent der befragten Institutionen an, Outsourcing in irgendeiner Form zu betreiben.

Der Begriff des Outsourcing ist allerdings datenschutzrechtlich nicht aussagekräftig. Hinter ihm können sich eine Datenverarbeitung im Auftrag oder eine Funktionsübertragung verbergen, die unterschiedlichen rechtlichen Anforderungen genügen müssen. Die Regelungen zur Datenverarbeitung im Auftrag und zur Funktionsübertragung sollen sicherstellen, dass die datenschutzrechtliche Verantwortung stets eindeutig zugeordnet werden kann und nicht „verdunstet". Gerade bei der Einschaltung Dritter drohen sonst die gebotene Transparenz für die Betroffenen und deren Rechtsschutz verloren zu gehen.

1.2.1 Datenverarbeitung im Auftrag

Werden personenbezogene Daten im Auftrag verarbeitet, ist die Auftrag gebende Stelle für die Einhaltung der Bestimmungen des Brandenburgischen Datenschutzgesetzes verantwortlich, gleich ob der Auftragnehmer eine öffentliche oder nicht-öffentliche Stelle ist. Der Auftraggeber bleibt „Herr" seiner Daten, mit deren Verarbeitung er den Auftragnehmer beauftragt hat. Erfolgt die Datenverarbeitung im Geltungsbereich des Brandenburgischen Datenschutzgesetzes, so unterliegt sie der Kontrolle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht. Bei einer Auftragsdurchführung außerhalb Brandenburgs sind dieser und die für den Ort der Auftragsdurchführung zuständige Datenschutzkontrollbehörde zu unterrichten.

Der Auftraggeber schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Auftragnehmer wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter der Verantwortung des Auftraggebers, gewissermaßen als sein Werkzeug, übertragen. Der Auftragnehmer hat keinen eigenen Handlungs- oder Entscheidungsspielraum. Deutliche Erkennungsmerkmale bei Auftragsdatenverarbeitung sind die fehlende Entscheidungsbefugnis des Auftragnehmers, die weisungsgebundene Unterstützungstätigkeit und seine fehlende Beziehung zu den von der Datenverarbeitung betroffenen Personen. Auftraggeber und Auftragnehmer gelten rechtlich als eine Daten verarbeitende Stelle, die Weitergabe von Daten an den Auftragnehmer ist keine Übermittlung im Sinne des Gesetzes und wird damit

[13] KES/KPMG-Sicherheitsstudie 2002 – Lagebericht zur IT-Sicherheit

stark erleichtert. Gerade die Voraussetzungen und Konsequenzen der Auftragsdatenverarbeitung werden von öffentlichen Stellen in Brandenburg immer wieder unterschätzt oder verkannt. Häufig wird in der Auftragsdatenverarbeitung zu Unrecht eine Möglichkeit gesehen, sich der datenschutzrechtlichen Verantwortung zu entledigen.

Die Verantwortlichkeit des Auftraggebers geht über die gelegentliche Überwachung der Datenverarbeitung hinaus. Die Verantwortlichkeit für eine Datenverarbeitung zwingt die öffentliche Stelle dazu, die Datenverarbeitung in der Gesamtheit mitzugestalten und dabei das Verfahren im wesentlichen zu beherrschen. Hinzu kommt, dass der Auftraggeber grundsätzlich in der Lage sein muss, die Datenverarbeitung vom Auftragnehmer wieder zu übernehmen (z. B. – bei privaten Dienstleistern – im Fall der Insolvenz). Wird die gesamte Datenverarbeitung ausgegliedert, sind kompetente verantwortliche Ansprechpartner zu benennen oder IT-Kopfstellen beim Auftraggeber zu bilden, welche die Auftragsdatenverarbeitung des Outsourcing-Anbieters überblicken und bewerten können. Ihnen obliegt die Erteilung der Weisungen und ihre Aktualisierung, die fortdauernde Kontrolle der Einhaltung der Datenschutzgrundsätze und die Wahrung der Betroffenenrechte (z. B. auf Auskunft oder Löschung).

Alle wesentlichen Komponenten der Auftragsdatenverarbeitung müssen detailliert in einem Vertrag geregelt werden. Dazu zählen mindestens die Rechte und Pflichten der Daten verarbeitenden Stelle, Gegenstand und der Umfang der übertragenen Tätigkeiten, die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Datenschutzmaßnahmen sowie etwaige Unterauftragsverhältnisse. Der Auftragnehmer darf die Datenverarbeitung ganz oder teilweise nur auf Unterauftragnehmer übertragen, soweit der Auftraggeber dem zugestimmt hat. Ferner muss vereinbart werden, dass der Auftraggeber dem Auftragnehmer Weisungen hinsichtlich der Verarbeitung personenbezogener Daten erteilen darf. Das Personal des beauftragten Unternehmens ist auf das Datengeheimnis zu verpflichten. Die Vertragsparteien sollten sich auf gemeinsame Sicherheitsstandards einigen und vertraglich eine für beide Seiten verbindliche Sicherheits-Policy festlegen. Dazu zählt auch die Erstellung eines Sicherheitskonzeptes, wobei die Verantwortung beim Auftraggeber bleibt, der einen entsprechenden Entwurf des Auftragnehmers überprüft, gegebenenfalls erweitert und genehmigt. Zur Sicherheits-Policy gehört auch eine geeignete Katastrophen-Vorsorge beim Auftragnehmer, der unter anderem durch Alarm-Konzepte und Hardware-Backups sicherstellen muss, die vereinbarte Leistung kontinuierlich liefern zu können. Hinzu kommen detaillierte Vereinbarungen zum Datenschutz. Um objektiv überprüfen zu können, ob vertraglich vereinbarte Leistungs-, Qualitäts- und Sicherheitsstandards eingehalten werden, ist vertraglich die Möglichkeit einer IT-Revision beim Auftragnehmer festzuschreiben.

1.2.2 Funktionsübertragung

Werden dagegen auch die der Verarbeitung zu Grunde liegenden Aufgaben ganz oder teilweise übertragen und bestehen Handlungs- und Entscheidungsspielräume bei der Erledigung der Aufgabe, liegt eine Funktionsübertragung vor. In diesem Fall wird der Dienstleister selbst zur Daten verarbeitenden Stelle und hat in eigener Verantwortung für die zur Datensicherung und zur Gewährleistung von Vertraulichkeit erforderlichen technischen und organisatorischen Maßnahmen zu sorgen. Merkmale der Funktionsübertragung sind die Überlassung von Nutzungsrechten an den Daten sowie das Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch). Die Datenweitergabe an den Dienstleister ist eine Datenübermittlung und damit nur unter eingeschränkten Voraussetzungen, nämlich auf Grund einer gesetzlichen Übermittlungsbefugnis oder mit Einwilligung der Betroffenen, zulässig.

Besondere Probleme ergeben sich bei sensitiven Daten, für die spezielle Schutzvorschriften bestehen. Diese schränken jede Offenbarung gegenüber Dritten stark ein. Dazu gehören insbesondere Berufsgeheimnisse (z. B. Arztgeheimnis) und besondere Amtsgeheimnisse (z. B. Sozial- und Steuergeheimnis). In diesen Fällen ist eine Weitergabe der Daten an Dritte nur zulässig, wenn die betreffenden Schutzvorschriften die Offenbarung dieser Daten erlauben.

Vor diesem Hintergrund müssen öffentliche Stellen vor einer Outsourcing-Entscheidung kritisch überprüfen, ob die Fremdvergabe wesentlich kostengünstiger wäre als bei der weiteren Erledigung im eigenen Haus. Diese Frage hat zumindest beim Umgang mit Sozialdaten auch datenschutzrechtliche Bedeutung[14]. In der Privatwirtschaft setzt teilweise bereits ein Umdenken ein, das bei einigen Kernbereichen der Geschäftstätigkeit, die ausgelagert waren, zu einem „Insourcing“ geführt hat. Auch öffentliche Stellen müssen die Entscheidung zur auftragsweisen Vergabe der Verarbeitung von Bürgerdaten regelmäßig überprüfen und bei Bedarf, insbesondere bei datenschutzrechtlichen Mängeln, revidieren.

Öffentliche Stellen dürfen die Verarbeitung personenbezogener Daten ganz oder teilweise nur dann auf private oder öffentliche Dienstleister übertragen, wenn sie ihrer fortbestehenden Verantwortung jederzeit genügen können und die dafür erforderlichen Maßnahmen treffen.

[14] vgl. dazu A 8.2.2

1.3 Gelten Gütesiegel anderer Bundesländer auch in Brandenburg?

Während in Schleswig-Holstein das Datenschutz-Audit erfolgreich eingeführt wurde, fehlen entsprechende Gesetzentwürfe in Brandenburg und im Bund noch immer. Inzwischen sind in Schleswig-Holstein mehrere Produkte und Verfahren von unabhängigen Gutachtern geprüft worden und haben vom dortigen Unabhängigen Landeszentrum für Datenschutz ein Gütesiegel erhalten. Der Anbieter eines so ausgezeichneten elektronischen medizinischen Archivierungssystems wollte von uns wissen, ob dieses Gütesiegel auch von öffentlichen Stellen in Brandenburg berücksichtigt werden muss. Außerdem bat uns das Unabhängige Landeszentrum um die Beurteilung eines Verfahrens in kommunalen Gewerbeämtern, bei dem eine Software eingesetzt wird, deren Hersteller in Schleswig-Holstein ein Gütesiegel beantragt hatte.

Das Brandenburgische Datenschutzgesetz (BbgDSG) schreibt in § 11b vor, dass nach einem förmlichen Verfahren geprüfte und positiv bewertete Produkte und Verfahren von öffentlichen Stellen des Landes Brandenburg vorrangig berücksichtigt werden sollen.

Das Gesetz verlangt dabei lediglich, dass es sich um ein förmliches Verfahren handeln muss. Es beschränkt sich nicht auf das Datenschutz-Audit, das nach § 11c BbgDSG durchgeführt werden kann. Es kommt nach dem Wortlaut nicht darauf an, in welchem Bundesland das Produkt oder Verfahren zertifiziert wurde.

Vielmehr ist festzuhalten, dass öffentliche Stellen des Landes Brandenburg auch solche Produkte und Verfahren vorrangig einsetzen sollen, deren Vereinbarkeit mit dem Datenschutzrecht nach förmlichen Verfahren außerhalb Brandenburgs geprüft und positiv bewertet worden ist.

Wichtig ist, dass die Audit-Verfahren gesetzlich geregelt sein müssen. Nur in diesem Falle ist eine objektive und vergleichbare Bewertung gewährleistet. Diesem Anspruch genügt das schleswig-holsteinische Verfahren ohne Zweifel. Dies gilt aber auch für zukünftige Verfahren in anderen Bundesländern oder auf Bundesebene.

Selbstverständlich ist dabei zu berücksichtigen, dass die jeweiligen Zertifizierungen anhand der Rechtslage im jeweiligen Bundesland durchgeführt werden. Angesichts des weit gehend einheitlichen Datenschutzniveaus wird eine Anpassung an brandenburgische Verhältnisse in der Regel jedoch unproblematisch möglich sein. Im Übrigen ist auch vor dem Einsatz solcher Verfahren

eine Risikoanalyse durchzuführen, ein Sicherheitskonzept zu erstellen und eine förmliche Freigabe zu erteilen.

Wir haben den Landesbetrieb für Datenverarbeitung und Statistik, einzelne Ressorts der Landesregierung und die kommunalen Spitzenverbände auf diese Zusammenhänge hingewiesen und um eine Berücksichtigung rechtlich bedeutsamer Gütesiegel bei Vergabeentscheidungen gebeten. Das Ministerium des Innern hat inzwischen die Ressorts gebeten, die von uns vertretene Rechtsauffassung zu beachten.

Dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein haben wir unsere Bewertung eines EDV-Verfahrens in kommunalen Gewerbeämtern mitgeteilt, damit sie bei der Entscheidung über das beantragte Gütesiegel berücksichtigt werden kann.

Beide Sachverhalte machen deutlich, dass die Vergabe von Gütesiegeln, die im Datenschutzrecht ein positives Wettbewerbselement einführt, zweckmäßigerweise bundeseinheitlich geregelt werden sollte. Wenn dies nicht in absehbarer Zeit geschieht, sollte die Landesregierung auch in Brandenburg einen Entwurf für ein Datenschutz-Audit-Gesetz vorlegen.

Produkte und Verfahren, deren Vereinbarkeit mit den Bestimmungen des Datenschutzes in einem gesetzlichen Verfahren auch außerhalb Brandenburgs geprüft wurde, sollen durch die öffentlichen Stellen des Landes bei Vergabeentscheidungen vorrangig berücksichtigt werden. Wir fordern die Landesregierung auf, den vom Brandenburgischen Datenschutzgesetz vorgesehenen Gesetzentwurf für ein Datenschutz-Audit in Brandenburg vorzulegen, wenn der Bundesgesetzgeber in dieser Frage so passiv bleibt wie bisher.

1.4 Videoüberwachung betrifft alle

Der zunehmende Einsatz von Überwachungskameras durch öffentliche Stellen warf im Berichtszeitraum teils neue Fragestellungen auf, teils gab er Veranlassung, auf die rechtlichen Rahmenbedingungen für diese Form der Verarbeitung von Bürgerdaten hinzuweisen. Der Preisverfall im Bereich der digitalen Kameras trägt dazu bei, dass auch Private sich zunehmend dieser handlichen Beobachtungstechnik bedienen und staatliche Stellen mitunter vor der Frage stehen, ob sie privat erstellte Videoaufnahmen nutzen dürfen.

1.4.1 Nutzung privater Videos durch öffentliche Stellen

An einem markanten Punkt in einer Gemeinde kam es in den Abendstunden immer wieder zu Vandalismus, lauter Musik, Auto-Wettfahrten. Niemand traute sich so recht Anzeige zu erstatten, dafür machten aber

Anwohner und Passanten Videoaufnahmen, die sie der Gemeinde mit der Bitte um Einschreiten zur Verfügung stellten.

Bei den infrage stehenden Belästigungen handelt es sich möglicherweise um Straftaten und Ordnungswidrigkeiten, deren Verfolgung ausschließlich Aufgabe bestimmter staatlicher Stellen – i. d. R. der Polizei – ist. Aufnahmen dürfen zu diesem Zweck nur auf Grund gesetzlicher Bestimmungen gemacht werden. So regelt die Strafprozessordnung diesen Bereich für die Verfolgung bereits begangener Taten, während das Polizeirecht den Rahmen für die Verwendung von Bildmaterial von Personen zwecks Gefahrenabwehr vorgibt. Darüber hinaus enthalten sowohl das Bundesdatenschutzgesetz als auch das Brandenburgische Datenschutzgesetz Bestimmungen zur Videoaufzeichnung durch öffentliche Stellen. Nutzen staatliche Stellen z. B. verdeckt erstellte Aufnahmen Privater, würde dies eine Erweiterung bzw. Umgehung dieser klaren und eindeutigen rechtlichen Bindungen bedeuten und wäre daher unzulässig.

Anders als bei fest installierten und gegen unbefugte Zugriffe gesicherten Überwachungsanlagen, die zusätzliche Angaben über Ort und Zeit der Aufnahme bereitstellen, kommt „freihändigem“, durch beliebige Passanten beschafftem Bildmaterial selbst nur ein begrenzter Aussagewert zu. Aus ihm gehen im Regelfall nicht selbsterklärend die näheren Umstände seiner Entstehung oder seines zeitlichen Kontextes hervor. Hinzu kommen die vielfältigen Möglichkeiten der nachträglichen Bildmanipulation, die moderne Digitaltechnik und Bildbearbeitungssoftware eröffnen. Zur strafrechtlichen Verwertung des Bildmaterials bedarf es stets der zusätzlichen Zeugenaussage der aufnehmenden Person.

Die Verwertbarkeit derartiger Aufnahmen vor Gericht hängt zudem davon ab, ob es nur um die Verfolgung einer schweren Straftat oder einer Ordnungswidrigkeit geht. Bei den beschriebenen Fällen von ruhestörendem Lärm oder Vandalismus scheidet die Verwertung solcher Aufnahmen aus.

Private Bildaufnahmen dürfen durch öffentliche Stellen nicht genutzt werden, wenn es ihnen selbst untersagt ist, sie zu erstellen. Ihre Nutzung als Beweismittel im Strafprozess ist nur im Zusammenhang mit einer zeugenschaftlichen Vernehmung zulässig.

1.4.2 Videoüberwachung von Mitarbeitern einer Haftanstalt

In einer Justizvollzugsanstalt wird eine Kameraüberwachungsanlage installiert, die es ermöglicht, Personen zu beobachten und die Bilder bei Bedarf auch aufzuzeichnen. Inwieweit müssen die Mitarbeiterinnen und Mitarbeiter das hinnehmen ?

Naturgemäß müssen die auf Grund eines Strafurteils Einsitzenden in vielerlei Hinsicht Einschränkungen ihrer persönlichen Freiheiten hinnehmen. Ihre Rechte und Pflichten regeln sich nach dem Strafvollzugsgesetz, auf Grund dessen auch ihre Beobachtung mittels Kameraüberwachungsanlagen möglich ist, soweit die Sicherheit im Strafvollzug es im Einzelfall erfordert.

Aber auch die Bediensteten einer solchen Einrichtung müssen den aus den besonderen Gegebenheiten resultierenden Sicherheitsanforderungen Rechnung tragen. Prinzipiell müssen sie es hinnehmen, dass sie während ihrer Tätigkeit von Überwachungsanlagen erfasst und aufgezeichnet werden. Häufig wird damit auch der Schutz der Bediensteten verfolgt. Aufzeichnungen können bei Zwischenfällen im Einzelfall auch der Entlastung von Bediensteten bei unberechtigten Vorwürfen von Insassen dienen. Andererseits kann mit Bildaufzeichnungen auch Fehlverhalten von Bediensteten beweiskräftig festgehalten werden.

Anders als Strafgefangene befinden sich die Bediensteten auf Grund ihres Dienstverhältnisses in der Haftanstalt und haben daher die gleichen Rechte wie alle anderen Beschäftigten im öffentlichen Dienst. Ungeachtet des besonderen Arbeitsplatzes ist das Brandenburgische Personalvertretungsgesetz anwendbar. Nach dessen § 65 Nr. 2 fällt die Einführung und Anwendung aller technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung von Beschäftigten zu überwachen, unter das Mitbestimmungsrecht des Personalrats.

Unter den Begriff der technischen Einrichtung fällt dabei jede Installation, die das normale Blickfeld eines Menschen unter Zwischenschaltung eines technischen Hilfsmittels erweitert. Auch eine Überwachungskamera ohne Möglichkeit der Bildaufzeichnung erfüllt diese Bedingung. Sie erlaubt es, Dinge an Orten wahrzunehmen, ohne selbst in deren Nähe sein zu müssen. Hierin unterscheidet sie sich von der Verwendung bloßer physikalischer Hilfsmittel wie etwa der eines Spiegels oder eines „Türspions“. Dass es in erster Linie beabsichtigt ist, Strafgefangene oder besondere Sicherheitsbereiche zu überwachen, mindert nicht die objektive Eignung der technischen Anlage zur Überwachung der Beschäftigten. Die Technik arbeitet unabhängig von der konkreten Person, die in ihr Aufnahmefeld gerät und unterscheidet nicht zwischen dem Status, den sie jeweils innehat. Sie ist prinzipiell geeignet, in die Rechte der Beschäftigten einzugreifen, sodass allein diese abstrakte Gefährdung die Mitbestimmungsrechte des Personalrats bei ihrer Einführung auslöst. Unterbleibt die Beteiligung des Personalrats, wird unzulässig in die Rechte der Beschäftigten eingegriffen.

Die Beteiligung des Personalrats soll einen vernünftigen Ausgleich zwischen Beschäftigten und den (Sicherheits-) Interessen der Einrichtung ermöglichen. Möglichst im Rahmen einer Dienstvereinbarung müssen Festlegungen getroffen werden, wie mit Beobachtungen und Bildaufzeichnungen von Beschäftigten umgegangen werden soll. Für Aufzeichnungen sind Aufbewahrungszeiten festzulegen und Regelungen zu treffen, durch wen sie ausgewertet werden, sowie welche Bereiche von den Überwachungseinrichtungen betroffen werden.

Beschäftigte einer Justizvollzugsanstalt müssen es grundsätzlich hinnehmen, dass auch sie ins Blickfeld technischer Sicherheitsanlagen wie z. B. der Videoüberwachung gelangen. Besteht aber die Gefahr, dass sie in ihrem Verhalten oder in ihrer Leistung überwacht werden, ist der Personalrat einzubeziehen.

1.4.3 Videoüberwachung historischer Denkmäler

An vielen Orten bedient sich die Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg der Videoüberwachungstechnik, um ihre zum Weltkulturerbe der UNESCO zählenden Denkmäler, Schlösser und Gärten zu schützen. Auch hier geraten Bedienstete und auf dem Gelände der Stiftung wohnende Menschen ins Blickfeld der Kamera.

Die Schlösser, Denkmäler und Gärten, die von der Stiftung Preußische Schlösser und Gärten betreut werden, sind vielerlei Gefahren ausgesetzt. Ihnen drohen Vandalismus und Einbrüche. Deshalb ist die Stiftung bestrebt, ihre Sicherheitssysteme zu verbessern und installiert Videoüberwachungsanlagen. Auch wenn das angestrebte Ziel der Stärkung des Schutzes der historischen Güter zu unterstützen ist, müssen dabei auch die Rechte von Unbeteiligten ausreichend gewahrt bleiben. Da die eingesetzte Technik nicht zwischen „gefährlichen“ und harmlosen Personen unterscheiden kann, bedarf es flankierender Regelungen.

Prinzipiell ist es nach § 33c Brandenburgisches Datenschutzgesetz zulässig, dass sich die Stiftung moderner technischer Anlagen bedient, um ihre wertvollen Kulturschätze zu sichern. Dennoch müssen alle Personen auf die Überwachungseinrichtungen hingewiesen werden, die in ihren Beobachtungsbereich geraten. Die Stiftung hat uns zugesichert, dass dies durch eine ergänzende Anbringung eines Piktogramms auf den Hinweisschildern, welche die allgemeinen Verhaltensregeln an den Eingängen zu den Schlössern und Parkanlagen der Stiftung enthalten, geschehen soll.

Im Hinblick auf die Beschäftigten der Stiftung bedarf die Installation einer derartigen technischen Einrichtung, die – zumindest auch – geeignet ist, das

Verhalten und die Leistung von Beschäftigten zu kontrollieren, der Mitbestimmung der Personalvertretung. Die Modalitäten zur Auswertung von Aufzeichnungen sowie die Aufbewahrungsdauer müssen mindestens durch eine förmliche Dienstanweisung, besser mit einer Dienstvereinbarung, festgelegt werden.

Hinzu kam in einem konkreten Fall, dass auch der Wohnbereich von Mietern durch die Überwachungsanlagen betroffen sein konnte. Es bestand die Gefahr, dass Umstände der Lebensführung der betroffenen Personen festgehalten wurden. Die Überwachung der Zugänge zu Schlössern und Parkanlagen umfasste zugleich die Möglichkeit, Besucher- und Mieterverhalten zu beobachten. Hier waren die legitimen Interessen der Stiftung und der Öffentlichkeit am Schutz der Kulturdenkmäler und die Rechte der Betroffenen an ihrer Privatsphäre zum Ausgleich zu bringen. Einerseits müssen die Mieter es hinnehmen, dass die Zufahrtswege zu ihrer Wohnung in einem überwachten Bereich liegen, wenn dessen Herausnahme aus der Überwachung eine nicht hinnehmbare Sicherheitslücke bedeuten würde. Andererseits haben die Mieter einen Anspruch auf Wahrung ihrer Privatsphäre, d. h. es geht niemanden etwas an, was in ihren Räumen vorgeht, da die Kenntnis darüber nicht sicherheitsrelevant ist. Die Mieter müssen sicher sein, dass keine unzulässigen Aufnahmen von ihnen oder ihren Besuchern gespeichert oder ausgewertet werden. Soweit möglich, sind der Wohnbereich – insbesondere die Fenster der Wohnungen – von der direkten Überwachung auszuschließen, was sich ohne Weiteres durch entsprechendes Einstellen der Aufnahmewinkel der verwendeten Kameras sowie das Aufstellen von Sichthindernissen bewerkstelligen lässt. Auch sollten die Mieter von Anfang an mit einbezogen werden. Sie sind über die Installation der Überwachungseinrichtungen zu informieren; ihnen sollte dargelegt werden, inwieweit ihre Sphäre hiervon berührt wird, um Misstrauen und Missverständnisse zu vermeiden.

Die Wahl von Maßnahmen zur Gewährleistung des Schutzes vor Einbrüchen und Beschädigungen obliegt prinzipiell den Eigentümern eines Objektes, sie können dazu auch eine Überwachungsanlage installieren. Allerdings darf dabei nicht unzulässig in die Rechte Unbeteiligter eingegriffen werden. Die Privatsphäre von Wohnbereichen muss gewahrt bleiben.

1.5 RFIDs – Elektronische Etikettierung von Waren und Menschen

Auf Radio-Frequenzen gestützte Identifizierungsetiketten (RFID tags) werden gegenwärtig getestet und zunehmend eingesetzt als eine weiterentwickelte Form und möglicher Ersatz für Strichcodes („Smart-Labels“, schlaue Etiketten). Ein großer deutscher Handelskonzern hat angekündigt, diese Etiketten im Herbst 2004 schrittweise einführen zu wollen.

Auch die Aufnahme solcher funkender Kleinst-Etiketten in Ausweispapiere wird erwogen.

Die Größe dieser Mikrochips ist ungefähr ein Drittel eines Millimeters. Die meisten von ihnen funktionieren als so genannte passive Transponder (ohne Batterien), indem sie Radiosignale empfangen, die von RFID-Lesern über kurze Distanzen gesendet werden. Sie nutzen die Energie des Radiosignals, um es zu beantworten. Da die Preise für RFID-Mikrochips und Lesegeräte gegenwärtig fallen, wird ihr flächendeckender Einsatz zunehmend wirtschaftlich. RFID-Etiketten werden voraussichtlich eine allgegenwärtige Datenverarbeitung bewirken. Auf Grund ihrer Speicherkapazität und Eignung für interaktive Kommunikation sind sie erheblich mächtiger als die bisher genutzten Strichcodes. Außerdem ermöglichen sie die individuelle Identifikation jeder gekennzeichneten Einheit, während Strichcodes für jede Einheit desselben Produktes identisch sind.

RFID-Etiketten können zu Einrichtungen von „intelligenten Regalen“ in Geschäften genutzt werden, um besser für rechtzeitige Nachlieferungen zu sorgen und das Auffüllen von Waren und Nachschub zu erleichtern. Sie können auch für die berührungslose Bezahlung an Kassen genutzt werden, insbesondere wenn sie mit Kreditkarten verknüpft sind. Zudem kann ein Arbeitgeber die Technik einsetzen, um sein Eigentum zu kennzeichnen und auf diese Weise die Diebstähle durch eigene Beschäftigte zu reduzieren. Die Etiketten könnten mit Videoüberwachungskameras verbunden werden, um sowohl das Verhalten der Beschäftigten als auch das der Kunden zu kontrollieren. Dokumente können gekennzeichnet werden, um sie in einem Büro leichter aufzufinden. Sowohl Identitätspapiere als auch Pässe und Visa können mit RFID-Etiketten ausgestattet werden. In jüngerer Zeit hat die Europäische Zentralbank angekündigt, dass Euro-Banknoten mit RFID-Etiketten versehen werden, um Fälschungen und Geldwäsche zu bekämpfen und den Geldkreislauf zu kontrollieren. Die Tickets für die Fußball-Weltmeisterschaft 2006 in Deutschland sollen mit dieser Technologie ausgestattet werden. Waschbare RFID-Etiketten können in Kleidungsstücke integriert werden („tragbare Datenverarbeitung“), um Produktpiraterie zu verhindern oder festzustellen und um die Authentizität eines Warenzeichens zu beweisen. Andere mögliche Einsatzbereiche reichen von Autoschlüsseln (Wegfahrsperre) bis hin zum Management von Containern.

Die RFID-Technologie hat zahlreiche Auswirkungen auf die Privatsphäre. Dies ist offenkundig im Fall von Mikrochips, die bei Menschen implantiert werden. Aber auch im weiter verbreiteten Fall von etikettierten Gegenständen und Gütern bezieht sich die übermittelte Information ebenso auf die Person, die den etikettierten Gegenstand mit sich führt oder auf eine ganze Konstellation von ihr bevorzugter Markenzeichen, sodass auf diese Weise der Ge-

schmack oder Stil der betroffenen Person offenkundig wird. Deshalb können personenbezogene Daten mit Hilfe von RFID-Etiketten verarbeitet, übermittelt oder gelesen werden oder zumindest können derartige objektbezogene Informationen leicht mit personenbezogenen Informationen verknüpft werden (z. B. wenn eine Kreditkarte zum Kauf eines etikettierten Gegenstandes genutzt wird). RFID-Etiketten bergen das Potenzial, die Bewegungen der Person zu registrieren, die etikettierte Gegenstände besitzt oder mit ihnen umgeht. Das gilt insbesondere dann, wenn sie noch ausgelesen werden können, nachdem der Kunde die Ware bezahlt und das Geschäft verlassen hat.

Auf Vorschlag des brandenburgischen Landesbeauftragten hat sich zunächst die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation mit diesem Fragenkreis beschäftigt und eine Entschließung der Internationalen Konferenz der Datenschutzbeauftragten befürwortet, die am 20. November 2003 beschlossen worden ist.[15]

Funkende Mikrochips werden voraussichtlich in Kürze zu unserer täglichen Umgebung gehören. Ihre möglichen Auswirkungen auf die Privatsphäre sind weit reichend. Soweit sie zur Etikettierung von Waren eingesetzt werden, müssen die Käufer darauf hingewiesen werden und die Möglichkeit haben, diese Etiketten mit dem Kauf zu entfernen oder zu deaktivieren. Anderenfalls können ohne großen Aufwand umfassende Konsum- und Bewegungsprofile über einzelne Menschen erstellt werden. Auch der Einsatz der RFID-Technik durch öffentliche Stellen, z. B. die geplante Integration von Funkchips in Geldscheine und Ausweispapiere, muss von Maßnahmen zur Sicherung des Datenschutzes begleitet werden.

2 Technisch-organisatorische Entwicklungen

2.1 Trusted Computing - ein sicherer PC auf Kosten des Datenschutzes?

Die seit 1999 in der „Trusted Computing Platform Alliance“ (TCPA) – seit 2003 umbenannt in „Trusted Computing Group“ – zusammengeschlossenen Hersteller von Hard- und Software beabsichtigen, den PC im Internet durch ein spezielles integriertes Hardware-Modul vor Softwareangriffen zu schützen und seine Integrität nachweisbar gegenüber anderen Systemen zu sichern. Durch Schutz vor Manipulationen soll der Computer vertrauenswürdiger werden. Dabei ist jedoch kritisch zu prüfen, inwieweit gerade die als Sicherheitsfunktionen angebotenen Lösungen

[15] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A III 2

dem Nutzer den Einfluss auf seinen Computer entziehen und seine Privatsphäre gefährden.

Die folgenden fünf wesentlichen Funktionen zur Verbesserung der PC-Sicherheit sollen bereitgestellt werden:

- Durch technische Versiegelung werden zu schützende Daten an die aktuelle Systemkonfiguration gebunden, d. h. diese sind nach Manipulationen an Hard- oder Software nicht mehr lesbar.

- Mit einem manipulationssicheren Speicherbereich erhält der Anwender die Möglichkeit, seine kryptografischen Schlüssel die i. d. R. aus seiner Hardwarekonfiguration abgeleitet werden, auf seinem System selbst sicher zu speichern.

- Es besteht die Möglichkeit zur sicheren Authentifizierung der Systemkonfiguration eines Anwenders gegenüber externen Systemen, dazu gehört u. a. auch eine sichere Überprüfung der digitalen Signatur.

- Ein spezieller Zufallsgenerator dient zur Erzeugung sicherer kryptografischer Schlüssel durch den Anwender selbst.

- Eine zusätzliche manipulationssichere Echtzeituhr ermöglicht die Überprüfung von Zertifikaten und Zeitstempeln anderer Kommunikationspartner.

Diese Komponenten könnten dazu beitragen, dass Hard- und Software die Entscheidungen eines PC-Nutzers zuverlässig und manipulationssicher umsetzen und möglicherweise einen entscheidenden Beitrag zum Einsatz sicherer datenschutzgerechter Technik erzielen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in ihrer Entschließung „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“ vom März 2003[16] allerdings darauf hin, dass diese Technologie auch zahlreiche negative Nebenwirkungen haben kann und formulieren eine Reihe von Anforderungen und Fragen, die vor ihrem Einsatz erfüllt bzw. beantwortet werden müssen. Sie zielen insgesamt auf die Sicherung der informationellen Selbstbestimmung und damit der Autonomie des Anwenders von Hard- und Software ab, wie sie das Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 formuliert hat. Zum einen muss der Einzelne wissen können, wer, was, wann und bei welcher Gelegenheit über ihn weiß (Transparenzerfordernis). Darüber hinaus muss der Einzelne zum anderen aber grundsätzlich selbst darüber entscheiden können, ob und wenn ja welche personenbezogenen Informationen er über sich und wem gegenüber

[16] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A I 1

preisgibt. Dem würde das Erstellen von Nutzungsprofilen und das Auslesen von Informationen und Dokumenten durch eine externe Instanz ohne Einwilligung der Betroffenen diametral zuwider laufen.

So wäre auch ein faktischer „Anschluss- und Benutzungszwang“ des Internet bei der Nutzung von TCPA-Plattformen mit der Selbstbestimmung des PC-Nutzers nicht zu vereinbaren. Dies wäre etwa dann gegeben, wenn bei jedem Hochfahren des Rechners automatisch ohne Einflussmöglichkeit des Nutzers eine Internetverbindung aufgebaut würde, um die Konfiguration des Rechners und ihre Übereinstimmung mit bestimmten Vorgaben des oder der Hersteller zu überprüfen (Attestierung). Einen damit verbundenen „Anschluss- und Benutzungszwang“ darf es auch aus Gründen der informationellen Selbstbestimmung nicht geben, denn er würde dem Nutzer die eigenständige Verfügungsbefugnis über die Informationen auf der Festplatte seines Rechners entziehen oder zumindest infrage stellen. Selbst wenn dem Nutzer, der auf die Herstellung einer Netzverbindung durch die TCPA-Plattform verzichtet, sein Rechner nur mit eingeschränkten Funktionalitäten zur Verfügung steht, wird er im Ergebnis einem problematischen „Anschluss- und Benutzungszwang“ unterworfen. Das Gleiche gilt für die automatische Aktualisierung der Systemkonfiguration durch bestimmte Internetdienste. Trusted Computing birgt zudem die Gefahr, dass der Anwender durch die Attestierung und anschließende Bereinigung der Abweichungen vom gewünschten Systemzustand von der Nutzung von Alternativprogrammen wie Open-Source-Lösungen ausgeschlossen wird und dass Monopolstellungen ausgeweitet werden.

Das TCPA-Konzept kann auch dazu führen, dass eine eindeutige Identifikation des jeweiligen PC und damit des Nutzers möglich wird. Statt ihm jedoch ein möglicherweise globales Personenkennzeichen anzuheften, sollte ein vertauenswürdiger Computer seinen Nutzer in die Lage versetzen, nach seiner Wahl mit unterschiedlichen Identitäten (Pseudonymen) im Cyberspace Transaktionen durchzuführen. Die gegenwärtigen TCPA-Spezifikationen lassen es damit zu, dass auch Transaktionen die unter verschiedenen Pseudonymen durchgeführt werden dem Computer zugeordnet werden können. Damit lässt sich i. d. R. auch die Person, die an ihm arbeitet, identifizieren. Erst durch die Verwendung kryptografischer Protokolle, mit deren Hilfe unterschiedliche Identitäten gebildet werden können, die nicht mehr miteinander verknüpfbar sind, kann die TCPA ihr erklärtes Ziel erreichen, die Privatsphäre des Anwenders zu schützen. Denn die Verwendung von Pseudonymen soll gerade nicht zu einer regelmäßigen Identifikation, sondern zu einer Authentifikation ohne Personenbezug im Netz führen, was zum Abschluss bestimmter Rechtsgeschäfte vollkommen ausreicht.

Eine weitere zentrale Frage ist die Wahlfreiheit des Anwenders bei der Auswahl der vertrauenswürdigen Attestierungsinstanz. Wenn der Hersteller der jeweiligen PC-Plattform oder der Hersteller der Systemsoftware ihm eine Instanz zur Überprüfung der Systemkonfiguration vorschreibt, dem Nutzer mithin faktisch verordnet wird, wem er zu vertrauen hat, dann ist ein weiterer Aspekt der informationellen Selbstbestimmung tangiert.

Das TCPA-Konzept erhebt den Anspruch, die Vertrauenswürdigkeit rechnergestützter Kommunikation entscheidend steigern und damit auch Datenschutz und Datensicherheit fördern zu wollen. Dass solche Ansprüche erhoben werden, um Marktanteile zu gewinnen, Datenschutz also zunehmend zum Verkaufsargument wird, ist durchaus positiv zu bewerten. Allerdings müssen alle, die solche Ansprüche erheben, sich auch im Detail daran messen lassen, wie diese Ansprüche umgesetzt werden.

2.2 Schutzprofile für Informationssysteme

Die Komplexität von Informations- und Kommunikationssystemen (IuK-Systeme) steigt stetig. Der Anwender ist in den meisten Fällen kaum noch in der Lage, die IuK-Systeme in ihrer Gesamtheit zu durchschauen. Ob Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, ist in vielen Fällen nicht nachvollziehbar. Diverse Studien belegen, dass ausbleibende Erfolge beim E-Commerce und E-Government auf mangelnde Akzeptanz bei den Anwendern zurückzuführen sind. Nur Informationssysteme, bei denen die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten nachvollziehbar gewährleistet werden, können die Anwender überzeugen. Es ist deshalb wichtig, dass bereits vor der Entwicklung von IuK-Systemen bestimmte Sicherheitsanforderungen von den Anwendern definiert werden können. Dieses Ziel kann mit so genannten Schutzprofilen (Protection Profiles) erreicht werden, die unter anderem auch vom Bundesbeauftragten für den Datenschutz zur Verfügung gestellt[17] werden. Die Schutzprofile wurden auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt. Der Anwender erhält dadurch die Möglichkeit, bereits vor Produktentwicklung seine Anforderungen bezüglich der Sicherheit zu definieren, und die Hersteller solcher Systeme können datenschutzfreundliche Produkte nach prüffähigen Vorgaben entwickeln.

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen in einer Entschließung[18] die Anwendung von Schutzprofilen, damit die Anwender besser beurteilen können, ob IuK-Systeme vertrauenswürdig und datenschutzfreundlich sind.

[17] http://www.bfd.bund.de/technik/protection_profile.html

[18] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A I 1

Durch die Anwendung von Schutzprofilen kann das Vertrauen der Anwender in datenschutzfreundliche und transparente IuK-Systeme erheblich erhöht werden.

2.3 Risikoanalyse und IT-Sicherheitskonzept

Nach § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, einer Untersuchung, ob von diesen Verfahren spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können. Die Freigabe darf nur erklärt werden, wenn sichergestellt ist, dass diese Risiken nicht bestehen oder durch technische und organisatorische Maßnahmen beherrscht werden können.

Grundlage für die Risikoanalyse und das IT-Sicherheitskonzept ist § 7 Abs. 3 BbgDSG. Beide Komponenten sind inhaltlich so eng miteinander verbunden und voneinander abhängig, dass eine getrennte Betrachtung kaum Sinn ergeben würde. Ihre wichtigste Aufgabe besteht darin, den Umgang mit drohenden Gefahren zu regeln.

Zwingende Voraussetzung für ein IT-Sicherheitskonzept ist die Identifizierung von Sicherheitslücken anhand einer Risikoanalyse. Daraus leiten sich dann die Sicherheitsanforderungen ab, die durch das IT-Sicherheitskonzept umgesetzt werden müssen. Man verhindert so, dass Bedrohungen unterschätzt oder übersehen werden, Gefahren überbewertet werden und ein aus ökonomischer Sicht nicht akzeptabler Aufwand geleistet wird. Die Herausforderung an das IT-Sicherheitskonzept liegt nicht nur in der optimalen Auswahl angemessener Schutzmechanismen, sondern auch in der Gewährleistung einer beständigen, über die Lebensdauer der Systeme hinausgehenden Sicherheitsstrategie. Sicherheit kann nur erreicht werden, wenn die Schutzmaßnahmen in regelmäßigen Abständen überprüft und den aktuellen Bedingungen angepasst werden.

Für die Erstellung von Risikoanalysen und IT-Sicherheitskonzepten empfehlen wir, nach dem BSI Grundschutzhandbuch vorzugehen. Das damit erreichbare Sicherheitsniveau ist für den normalen Schutzbedarf ausreichend und angemessen. Sollte aus der Schutzbedarfsfeststellung (Teil der Risikoanalyse) ein erhöhter Schutzbedarf für bestimmte Verfahren festgestellt werden, muss für diese Anwendung eine ergänzende IT-Sicherheitsanalyse durchgeführt werden. Der Vorteil des Grundschutzhandbuchs liegt auch in der Pauschalierung bestimmter ähnlich gelagerter Gefährdungen und deren Lösungen. Es fasst Bündel von Standard-Sicherheitsmaßnahmen für die Be-

reiche Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge zusammen.

Mit Hilfe der Software BSI Tool IT-Grundschutz (GSTOOL)[19] wird eine gut handhabbare Software bereit gestellt, die den Anwender bei der Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten effizient unterstützt (für unmittelbare Bundes-, Landes- und Kommunalverwaltung kostenfrei).

Sobald neue Verfahren zum automatisierten Verarbeiten personenbezogener Daten eingesetzt werden, müssen eine Risikoanalyse und ein IT-Sicherheitskonzept erstellt werden. Mit Hilfe des IT-Grundschutzhandbuchs lassen sich IT-Sicherheitskonzepte einfach und arbeitsökonomisch realisieren.

2.4 Computer-Viren: Der Lovesan-Angriff

Im August 2003 kam es weltweit zu panikartigen Reaktionen. Der Grund lag in der explosionsartigen Verbreitung des Wurms Lovesan, alias Blaster, der in kürzester Zeit Hunderttausende Rechner infizierte, obwohl das hierfür verantwortliche Sicherheitsproblem schon lange bekannt war.

Wieder einmal demonstrierte ein Virus eindrucksvoll, wie bedenklich der Einsatz sicherheitstechnisch unausgereifter Software sein kann. Die verfehlte Sicherheitspolitik von Herstellern und die fehlende Sensibilität vieler Institutionen und privater Nutzer für IT-Sicherheit garantierten eine schnelle Verbreitung. Wären einfachste Sicherheitsregeln eingehalten worden, hätte der Virus kaum eine Chance gehabt. Dazu zählt in erster Linie das Einspielen aktueller Sicherheits-Patches, die nach dem Veröffentlichen von aufgedeckten Sicherheitslücken auf einschlägigen Internetseiten zur Verfügung gestellt werden. In diesem Fall existierte bereits seit mehreren Wochen ein entsprechendes Patch, welches die Schwachstelle, die den Angriffspunkt für den Wurm bildet, behoben hätte. Neben der Aktualisierung der Software konnte auch der Einsatz einer Firewall mit entsprechend restriktiven Filterregeln eine Infektion verhindern. Ohne diese Vorsichtsmaßnahmen riskierte jeder Internet-Nutzer einen unkontrollierten Rechnerabsturz sowie die Zwangsrekrutierung zum Virenverteiler.

Infolge der raschen Verbreitung von Lovesan, kamen immer mehr neue Varianten des Virus in Umlauf, deren Gefährdungspotential das der Urversion übertraf. Es zeichnete sich ab, dass der eigentliche Virus nur als Transportmittel für „Trojaner“ genutzt wurde, um Tür und Tor zu anderen Computern zu

[19] http://www.bsi.de

öffnen. Die bloße Anbindung an das Netzwerk reichte aus, um sich zu infizieren.

Trotz der vielen Warnungen vor Gefährdungen aus dem Internet war die Mehrzahl der Nutzer nicht auf den Virus vorbereitet. Erst nach dessen Verbreitung verzeichneten die Webseiten der Antiviren-Hersteller einen Ansturm von Anfragen zu den schnell bereitgestellten Removal-Tools, Sicherheits-Updates und Anleitungen zum Schutz vor Lovesan.

Das Netz der brandenburgischen Landesverwaltung konnte den Lovesan-Angriff erfolgreich abwehren. Besondere Maßnahmen waren nur im Intranetzwerk der Polizei notwendig, deren System weit gehend unabhängig vom Netz der Landesverwaltung arbeitet. Einzelne Server die der Kommunikation nach außen dienten, wurden vorsorglich für eine gewisse Zeit abgeschaltet.

In letzter Zeit mehren sich jedoch die Meldungen, dass im Landesverwaltungsnetz Lovesan-Virenfälle aufgetreten sind. Externe Laptops dürften hierfür in erster Linie verantwortlich sein; auf ihren Anschluss an das Landesverwaltungsnetz sollte daher weitest gehend verzichtet werden.

Der Einsatz von Firewalls und das Einspielen von aktuellen Sicherheits-Updates für bekannt gewordene Sicherheitslücken können die Ausbreitung von und Infektion mit Viren wesentlich erschweren oder sogar verhindern. Keine öffentliche Stelle in Brandenburg kann sich einen Verzicht auf solche Maßnahmen leisten.

2.5 Gefahren beim automatischen Software-Update

Um die immer häufiger auftretenden Funktionsmängel und Sicherheitslücken in Softwareprodukten, insbesondere in Betriebssystemen zu beheben, werden Updates der Software in immer kürzeren Zeitabständen erforderlich. Während in der Vergangenheit solche Maßnahmen lediglich im Zeitraum von Monaten oder Jahren erfolgten, werden sie heutzutage bereits nach Wochen oder gar Tagen notwendig. Weltweit agierende Softwareanbieter versuchen nun, ihren damit verbundenen Aufwand durch automatische Software-Updates über das Internet zu reduzieren. In ihren Lizenzbedingungen werden sie die Nutzer dazu veranlassen, ihnen über das Netz uneingeschränkte und praktisch nicht kontrollierbare Zugriffsmöglichkeiten auf ihre Informationstechnik einzuräumen, um die verwendete Version der Software automatisch zu prüfen und bei Bedarf zu aktualisieren. Dies kann bei Verarbeitung personenbezogener Daten dazu führen, dass Anwender die datenschutzrechtlichen Forderungen nach Zugriffskontrolle und Vertraulichkeit nicht in angemessener Weise realisieren.

Automatische Updatefunktionen wirken häufig wie eine Fernwartung von Datenverarbeitungsanlagen. Diese erfordert schriftliche Verträge mit detaillierten Festlegungen zur Datensicherheit und zu Kontrollmöglichkeiten des Auftraggebers (§ 11a Brandenburgisches Datenschutzgesetz), eine einfache Zustimmung zu den Lizenzbedingungen reicht nicht aus. Die datenschutzrechtliche Verantwortung verbleibt dabei bei der Daten verarbeitenden Stelle, insbesondere sind Zugriffe auf Betriebssystemebene ausreichend zu sichern und revisionssicher zu protokollieren. Sie dürfen nur besonders autorisiertem Personal ermöglicht werden. Vollautomatische Updatefunktionen entsprechen diesen Forderungen nicht. Der Softwarelieferant wird zum Herr über das Betriebssystem, indem er neue Betriebssystemkomponenten bereitstellt, die automatisch zum Auftraggeber übertragen und dort installiert werden. Derartige Verfahren bergen auch die Gefahr, dass im Falle eines nicht ausreichend getesteten und noch fehlerhaften Updates weitere Systeme des Nutzers gestört werden, ohne dass dieser die auslösende Ursache erkennen kann. Dagegen bestehen keine Einwände gegen die automatische Aktualisierung von Virendefinitionen, die teilweise täglich erfolgen muss.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in ihrer Entschließung vom August 2003[20] mit dieser Thematik befasst und datenschutzrechtliche Anforderungen an automatische Software-Updates formuliert. Vor dem Hintergrund der marktbeherrschenden Stellung großer ausländischer Software-Hersteller, die solche Update-Funktionen durchsetzen wollen, erfordert dieses Problem auch eine weltweite Reaktion.

Der brandenburgische Landesbeauftragte hat sich deshalb erfolgreich dafür eingesetzt, dass die 25. Internationale Datenschutzkonferenz in Sydney im September 2003 eine entsprechende Entschließung gefasst hat.[21]

Automatische Updatefunktionen sind nach dem Brandenburgischen Datenschutzgesetz nicht zulässig und deshalb zu deaktivieren. Updates von Betriebssystemen und Anwendungsprogrammen dürfen nur offline nach entsprechenden Test- und Freigabeverfahren erfolgen. Die automatische netzgestützte Aktualisierung von Virendefinitionen ist demgegenüber zulässig und sinnvoll.

[20] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A I 2

[21] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A III 1

2.6 Sicherheit in Funknetzen

Eine öffentliche Stelle fragte bei uns an, welche technischen und organisatorischen Maßnahmen bei der Installation und dem Betrieb von Funknetzen zu realisieren sind.

In den letzten Monaten zeigte sich, dass eine ganze Reihe von Behörden darüber nachdenkt, ein Funknetz an ihr bestehendes lokales Netz anzuschließen. Da die Ausbreitung von Funkwellen nicht auf einen Raum bzw. auf ein Gebäude beschränkt werden kann, müssen technische und organisatorische Maßnahmen realisiert werden, die ein unbefugtes Abhören von Datenpaketen sowie ein Eindringen in das Funknetz verhindern. Das Aufspüren von unsicheren Funknetzen ist bereits ein „Volkssport“ unter Hackern geworden. Bereits mit einem Notebook, das mit einem Funknetz-Adapter ausgestattet ist, sowie mit aus dem Internet kostenlos beschaffter Software ist es selbst für Laien möglich, ungesicherte Funknetze zu orten, abzuhören bzw. in diese einzudringen.

Wenn sich eine öffentliche Stelle dazu entschließt, ein Funknetz aufzubauen, so ist die Erstellung einer Risikoanalyse und eines IT-Sicherheitskonzepts unabdingbar. Werden personenbezogene Daten in einem Funknetz übertragen, so müssen zusätzliche technische und organisatorische Maßnahmen getroffen werden. Dasselbe gilt auch, wenn ein Funknetz an ein lokales Netz angeschlossen wird, in dem personenbezogene Daten verarbeitet werden. Folgende Maßnahmen sollten bei der Verarbeitung personenbezogener Daten realisiert werden:

- Änderung der Standardpasswörter der Access-Points,

- Filterung der Funknetz-Clients auf Basis der zugelassenen MAC-Adressen,

- SSID Broadcast am Access-Point deaktivieren,

- die SSID sollte so gewählt werden, dass sie keine Rückschlüsse auf die öffentliche Stelle zulässt,

- Deaktivierung des DHCP-Servers im Access-Point
  (nur statische IP-Adressen verwenden),

- Abschottung des Funknetzes vom lokalen Netz durch eine Firewall,

- Einsatz von Intrusion Detection Systemen zur Angriffserkennung,

- Installation von Personal Firewalls auf mobilen Clients,

- Beschränkung der Reichweite des Funknetzes durch Reduzierung der Sendeleistung,

- Die Konfiguration der Access-Points sollte nur von bestimmten Clients aus über sichere Verbindungen möglich sein,

- Access-Points sollten an arbeitsfreien Tagen bzw. außerhalb der Dienstzeit abgeschaltet werden,

- Regelmäßige Überprüfung der Protokolldateien der Access-Points.

Weiterhin ist darauf hinzuweisen, dass die bei WLANs notwendige Verschlüsselung von personenbezogenen Daten mit sicheren kryptografischen Verfahren derzeitig nur durch zusätzliche Sicherheitsmaßnahmen (VPN, IPSec) erreicht werden kann. Die Verwendung der WEP-Verschlüsselung mit 128 Bit kann allenfalls als Minimalschutz angesehen werden, da WEP vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als unsicher eingeschätzt wird und daher nicht geeignet ist, die Vertraulichkeit bei der Übertragung personenbezogener Daten sicherzustellen.

Schon bei der Beschaffung von Funknetz-Komponenten sollte darauf geachtet werden, dass die aufgeführten technisch-organisatorischen Maßnahmen auch realisierbar sind.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat eine Arbeitsgruppe unter unserer Leitung ins Leben gerufen, die eine Orientierungshilfe zur „Datensicherheit in drahtlosen Netzen“ erarbeiten wird.

Zudem haben der Arbeitskreis „Medien“ unter dem Vorsitz Brandenburgs und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation die durch Funknetze neu aufgeworfenen rechtlichen und technischen Fragen eingehend erörtert. Sie werden die schnelle technische Entwicklung in diesem Bereich weiter beobachten.

Auf Grund der zusätzlichen Gefährdungen beim Einsatz von Funknetzen ist die Erstellung einer Risikoanalyse und eines IT-Sicherheitskonzepts von besonderer Bedeutung. Nur durch zusätzliche technisch-organisatorische Maßnahmen kann der Schutz von personenbezogenen Daten sichergestellt werden.

2.7 Datensicherheit bei USB-Geräten

Öffentliche Stellen fragten bei uns an, welche technisch-organisatorischen Maßnahmen realisiert werden müssen, um einen Missbrauch der USB (Universal Serial Bus)-Schnittstelle zu verhindern.

Fast alle neuen Arbeitsplatzcomputer werden standardmäßig mit einer USB-Schnittstelle ausgerüstet. An diese Schnittstelle können verschiedene Hardwarekomponenten wie z. B. Disketten-, DVD- oder CD-ROM-Laufwerke, Festspeichermedien (z. B. USB-Sticks von der Größe eines Autoschlüssels), Netzwerkkarten oder WLAN-Adapter angeschlossen werden. Ein Vorteil der USB-Schnittstelle ist, dass neu angeschlossene Geräte sofort vom Betriebssystem erkannt und installiert werden. Aufwändige Installationsprozeduren für Hard- und Software entfallen dadurch. Dieser Komfort birgt jedoch auch Risiken. Der unkontrollierte Betrieb von USB-Komponenten bedroht die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten. USB-Schnittstellen sollten daher grundsätzlich deaktiviert werden.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat in der Orientierungshilfe „Datensicherheit bei USB-Geräten“ konkrete technische Maßnahmen beschrieben, um einen Missbrauch von USB-Geräten weitest gehend auszuschließen[22].

USB-Geräte können relativ leicht und unbemerkt an Arbeitsplatzcomputer angeschlossen und genutzt werden. Um einen Missbrauch personenbezogener Daten zu verhindern, müssen Maßnahmen ergriffen werden, die eine unberechtigte Nutzung dieser Geräte ausschließen.

2.8 Einsatz kryptografischer Verfahren

Kryptografische Verfahren sind besonders geeignet, um die Vertraulichkeit und Integrität bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Der Einsatz kryptografischer Verfahren entspricht heute dem Stand der Technik. Personenbezogene Daten dürfen in Weitverkehrsnetzen (z. B. Internet, Landesverwaltungsnetz) nur verschlüsselt übertragen werden. Es müssen dabei sichere kryptografische Verfahren zum Einsatz kommen. Werden sensitive personenbezogene Daten der Schutzstufe C unseres Schutzstufenkonzeptes bzw. besondere Kategorien personenbezogener Daten gem. § 4a Brandenburgisches Datenschutzgesetz (BbgDSG) verarbeitet, so sind diese

[22] vgl. Anlage 1

verschlüsselt zu speichern. Bereits bei der Auswahl von Produkten sollten diese Forderungen berücksichtigt werden. Es zeigt sich immer wieder, dass Verfahren implementiert werden, und im nachhinein dann festgestellt wird, dass eine Integration von Verschlüsselungsverfahren „zu aufwändig“ bzw. technisch nicht realisierbar ist. Auch sollten die neuen Möglichkeiten der Verschlüsselung und der Bildung von sog. virtuellen privaten Netzen (VPNs), die das Landesverwaltungsnetz 3 bietet, von vornherein genutzt werden.

Schließlich ist zu berücksichtigen, dass kryptografische Verfahren stets nur nach dem gegenwärtigen Stand der Technik als sicher angesehen werden und der technischen Entwicklung laufend angepasst werden müssen.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe zum Einsatz kryptografischer Verfahren erstellt, in der u. a. Grundlagen der Kryptografie erörtert und konkrete Anwendungsszenarien beschrieben werden. Diese kann auf unserer Website (www.lda.brandenburg.de) abgerufen werden.

2.9 IT-Strategie jetzt – Sicherheitskonzept später?

Die von der Landesregierung im Zuge der Umsetzung des Gesetzes über die Ziele und Vorgaben zur Modernisierung der Landesverwaltung[23] erarbeitete IT-Strategie 2004 - 2008 zielt darauf ab, die Informations- und Kommunikationsinfrastruktur nach wirtschaftlichen Gesichtspunkten zu optimieren, indem einheitliche Standards für die Beschaffung von Hard- und Software sowie auch für die Organisation des Einsatzes der Informationstechnik in der Landesverwaltung festgelegt werden sollen.

Der Entwurf der IT-Strategie[24] sah vor, dass „zu einem späteren Zeitpunkt ... allgemeinverbindliche Festlegungen zur IT-Sicherheit in einer gesonderten „IT-Sicherheitsrichtlinie“ getroffen (werden)“. Es ist demgegenüber unabdingbar, dass strategische Betrachtungen in der Informationstechnik mit IT-Sicherheitsbetrachtungen einher gehen müssen. Wir haben uns daher dafür eingesetzt, die IT-Strategie und die IT-Sicherheitsrichtlinie zeitgleich zu verabschieden. Grundlage hierfür kann das IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik sein.

Nach dem Entwurf ist beabsichtigt, zentrale Serverstrukturen im verstärktem Maße einzusetzen. Dabei ist zu berücksichtigen, dass solche Strukturen einerseits höhere Sicherheitsanforderungen zu erfüllen haben (z. B. die Über-

[23] vom 10. Juli 2003, GVBl. 2003 I S. 193

[24] Stand: 11. November 2003

tragung personenbezogener Daten im Landesverwaltungsnetz), andererseits aber auch geprüft werden muss, unter welchen Bedingungen eine Zentralisierung nach geltendem Datenschutzrecht überhaupt möglich ist. So ist z. B. die Abschottung von personenbezogenen Datenbeständen verschiedener Daten verarbeitender Stellen eine der Grundforderungen des Datenschutzes.

Auch sieht die IT-Strategie vor, einen zentralen IT-Dienstleister zu etablieren und den IT-Betrieb stärker zu zentralisieren. Dabei ist zu berücksichtigen, dass die Daten verarbeitenden Stellen „Herr ihrer Daten“ bleiben müssen. Werden personenbezogene Daten durch einen Dienstleistungsbetrieb verarbeitet, so handelt es sich um eine Datenverarbeitung im Auftrag gem. § 11 Brandenburgisches Datenschutzgesetz (BbgDSG). Dabei bleibt die Auftrag gebende Stelle für die Einhaltung der Bestimmungen des BbgDSG und anderer Vorschriften über den Datenschutz verantwortlich. Der Dienstleister unterliegt den Weisungen des Auftraggebers[25].

Bei der Optimierung von Informations- und Kommunikationsinfrastrukturen müssen neben wirtschaftlichen Gesichtspunkten auch die Belange der IT-Sicherheit von vornherein berücksichtigt werden.

2.10 Externe Zugänge zum Landesverwaltungsnetz

Die in unserem Tätigkeitsbericht 2001[26] beschriebene Umfrage des Landesbetriebes für Datenverarbeitung und Statistik (LDS) zu „Externe Zugänge zum Landesverwaltungsnetz (LVN)“ erbrachte aus Sicht des Datenschutzes ein durchaus positives Ergebnis.

Nur 3 der ca. 250 befragten Stellen konnten in den Fragebögen keinen hinreichenden Nachweis erbringen, dass die betriebenen externen Zugänge den Sicherheitsforderungen des LVN entsprechen. Nach Abschluss der Befragung haben wir die externen Zugänge dieser Stellen gemeinsam mit dem LDS überprüft. Es stellte sich heraus, dass konkrete technische und organisatorische Maßnahmen zur Absicherung der externen Zugänge bei den Stellen bereits realisiert waren bzw. auf Grund unserer Hinweise umgehend realisiert wurden. Die Sicherheit der am Landesverwaltungsnetz angeschlossenen Einrichtungen war deshalb aus dieser Sicht nicht gefährdet.

Auf Grund der Vielzahl der an das Landesverwaltungsnetz angeschlossenen öffentlichen Stellen kann nie ausgeschlossen werden, dass unzulässige externe Zugänge, wenn auch nur kurzzeitig, existieren. Wir bekräftigen daher

[25] vgl. dazu oben A 1.2
[26] vgl. A 2.3

unsere Forderung[27], dass auch lokale Netze von am LVN angeschlossenen öffentlichen Stellen, in denen personenbezogene Daten verarbeitet werden, durch Firewallsysteme abzusichern sind. Nur so kann das LVN als Ganzes wirksam vor Angriffen von außen geschützt werden.

Beim Anschluss einer öffentlichen Stelle, in der personenbezogene Daten verarbeitet werden, an das Landesverwaltungsnetz, ist die Abschottung des lokalen Netzes durch ein entsprechendes Firewallsystem sicherzustellen.

2.11 Wann sind gelöschte Daten wirklich weg?

Das vollständige Löschen von Daten ist nicht einfach. So führte eine in den USA erstellte Studie, in der 158 gebraucht erworbene Festplatten von Computern untersucht wurden, zu einem alarmierenden Ergebnis. Auf 146 Speichermedien konnten noch z. T. sehr sensitive personenbezogene Daten rekonstruiert werden. Der weit verbreitete Irrtum, wonach digitale Daten bei ihrer Löschung keine Restbestände hinterlassen, kann zu schwerwiegenden Folgen für die Datensicherheit führen.

Nach einem einfachen logischen Datenlöschbefehl löschen die meisten Computerbetriebssysteme lediglich die Verweise auf die Fundorte der Dateien. Die Daten selbst aber bleiben unverändert erhalten, bis der betreffende Speicherplatz mehr oder weniger zufällig und wenn, dann oft auch nur teilweise durch das Überschreiben mit neuen Daten physisch gelöscht wird. So können Dateien auf leistungsfähigen Festplatten mit mehreren Gigabyte Speicherkapazität, abhängig von der weiteren Verwendung des Computers, noch Monate oder Jahre nach dem beabsichtigten Löschvorgang mit teils allgemein zugänglicher Software wiederhergestellt werden. Doch auch bereits überschriebene Daten lassen sich unter bestimmten Umständen mit technischen Hilfsmitteln noch lesen.

Eine Lösung besteht in der Nutzung spezieller Löschtools. Diese Softwarewerkzeuge versuchen die Daten vor dem eigentlichen logischen Löschvorgang physisch mit bis zu 35 verschiedenen speziellen Bitmustern so zu überschreiben, dass alle Kodierungen ausgenutzt werden und aus dem verbliebenen Restmagnetismus keine brauchbaren Daten mehr zu rekonstruieren sind. Für die zu nutzenden Datenüberschreibungsverfahren existieren keine aktuellen Standards und selbst in Expertenkreisen herrscht Uneinigkeit darüber, wann sich vermeintlich überschriebene Daten wiederherstellen lassen. Dies hängt u. a. vom Festplattentyp, von den verfügbaren technischen Hilfsmitteln und dem betriebenen Personalaufwand zur Datenwiederherstellung ab. Ähnlich wie bei kryptografischen Verfahren führt die technische Entwick-

[27] vgl. 6. Tätigkeitsbericht (1997), 1.4.1.1

lung auch hier dazu, dass früher als datenschutzgerecht angesehene Verfahren heute oder in naher Zukunft keine sichere Löschung von Daten mehr gewährleisten. Auf alle Fälle sollte bei der Wahl des Löschvorganges der Schutzbedarf der zu entfernenden Daten eine angemessene Berücksichtigung finden.

Zudem reicht es nicht aus, nur die betreffenden sensitiven Dateien im Dateisystem durch vorheriges zielgerichtetes Überschreiben sicher zu löschen, denn die meisten Betriebssysteme oder Softwareprodukte legen für unterschiedliche Zwecke Kopien von den Dateien im Speicher ab. Dabei ist ihre Existenz und Lage auf der Festplatte dem Nutzer meist gar nicht bekannt. Im Laufe der Zeit sammeln sich so auf einer Festplatte immer mehr Kopien von Dateien an, die auch das Betriebssystem nicht mehr kennt. Um wirklich sicher zu gehen, dass sich keine sensitiven Daten mehr auf dem Speichermedium befinden, muss die gesamte Festplatte in geeigneter Weise physisch überschrieben werden. Bei geringem Schutzbedarf der gespeicherten Daten reicht eine Formatierung der Festplatte aus. Dies ist insbesondere dann unerlässlich, wenn Computer, mit denen personenbezogene Daten verarbeitet wurden, in andere Bereiche umgesetzt oder nach der Ausmusterung einer anderen Nutzung zugeführt werden sollen.

Daten verarbeitende Stellen haben bei der Löschung personenbezogener Daten durch zusätzliche Maßnahmen eine vollständige Löschung zu sichern. Dabei ist der Stand der (Lösch- und Wiederherstellungs-) Technik zu berücksichtigen.

3 Telekommunikation und Medien

3.1 Datenschutz in Telekommunikation und Internet – das Ende anonymer Kommunikation?

3.1.1 Neuordnung des Datenschutzes in der Telekommunikation

Das Jahr 2003 war geprägt von zwei Gesetzgebungsvorhaben zur Änderung des Telekommunikationsgesetzes (TKG), die sich in unterschiedlicher Weise auch auf die in diesem Bereich geltenden datenschutzrechtlichen Bestimmungen auswirken.

Das Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er Mehrwertdiensterufnummern soll vor unlauteren Angeboten schützen[28]. Damit wurde auch die Telekommunikations-Datenschutzverordnung dahingehend

[28] Gesetz vom 9. August 2003, BGBl. I S. 1590

geändert, dass die Zielrufnummern mit den Vorwahlen 0190 und 0900 generell vollständig gespeichert werden dürfen. Dadurch sollen die Verbraucher in die Lage versetzt werden, bei Einwendungen gegen die Rechnung mit Hilfe der vollständigen Rufnummer den Anbieter ermitteln zu können.

Es ist zwar anzuerkennen, dass der Kunde mit der vollständigen Rufnummer eine stärkere Rechtsposition zur Verfolgung seiner rechtlichen Interessen hat. Jedoch ist es unverhältnismäßig, die Speicherung der vollständigen Rufnummern zwangsweise auch den Kunden zu verordnen, die dies nicht wünschen. Dabei ist zu berücksichtigen, dass die Informationen über Anrufe bei bestimmten Mehrwertdiensten unter Umständen aus Sicht der Betroffenen einen sehr sensiblen Datenbestand darstellen können. Das ebenfalls zwingend vorgeschriebene Erscheinen dieser Rufnummern in einem Einzelverbindungsnachweis und die damit verbundene Kenntnisnahme möglicher Mitbenutzer des Anschlusses ist für eine Reihe von Betroffenen nicht wünschenswert. Zum anderen gibt es eine Reihe von Mehrwertdiensten, die kaum eine Missbrauchsgefahr aufweisen, wie z. B. Wettervorhersagen, andere Informationsdienste oder Faxabrufdienste. Wir haben daher vorgeschlagen, die Speicherung der vollständigen 0190er- und 0900er-Rufnummern von einer Einwilligung der Kunden abhängig zu machen oder zumindest eine Widerspruchsmöglichkeit vorzusehen. Das Ministerium für Wirtschaft hat unseren Vorschlag im Rahmen der Bundesratsabstimmung ebenso wenig unterstützt, wie die übrigen am Gesetzgebungsverfahren beteiligten Stellen.

Parallel dazu wird auf Initiative der Bundesregierung das Telekommunikationsgesetz insgesamt derzeit einer umfassenden Novellierung unterzogen. Damit sollen eine Reihe von europäischen Richtlinien – darunter die Richtlinie 2002/58/EG zum Datenschutz in der elektronischen Kommunikation – umgesetzt werden. Die entsprechende Anpassungsfrist wurde im Oktober 2003 bereits überschritten, sodass die Europäische Kommission inzwischen gegen die Bundesrepublik ein Vertragsverletzungsverfahren eingeleitet hat.

Der Schwerpunkt des Gesetzgebungsvorhabens liegt zwar bei der Neuordnung der Marktregulierung. Auch die datenschutzrechtlichen Bestimmungen sind jedoch von den geplanten Änderungen betroffen.

Geplant ist, die datenschutzrechtlichen Bestimmungen nunmehr in das Telekommunikationsgesetz selbst aufzunehmen, um Doppelregelungen zu vermeiden und die Telekommunikations-Datenschutzverordnung ersatzlos aufzuheben. Die Datenschutzbeauftragten hätten es begrüßt, wenn diese insgesamt positive Aufwertung des Datenschutzes in einem gesonderten Gesetz erfolgt wäre, um eine spätere Zusammenfassung mit den Datenschutzvor-

schriften für andere Bereiche der elektronischen Kommunikation und die Einbindung in das Bundesdatenschutzgesetz zu erleichtern.[29]

Das Vorhaben der Bundesregierung, die von den Telekommunikationsunternehmen zu erstellende Statistik über die Telefonüberwachung abzuschaffen, konnte schon im Gesetzgebungsverfahren verhindert werden. Zum anderen hat die Bundesregierung in ihrem Kabinettsbeschluss vom 15. Oktober 2003 davon Abstand genommen, die Zweckentfremdung von Bestandsdaten (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Hier soll – wie bisher – die informierte Einwilligung des Betroffenen erforderlich sein. Der Bundesrat fordert allerdings nach wie vor, die im Bundesdatenschutzgesetz für die Privatwirtschaft allgemein geltende Widerspruchsregelung einzuführen. Die auch aus unserer Sicht gebotene Vereinheitlichung des Datenschutzniveaus sollte stattdessen dazu führen, dass in allen Bereichen für eine Zweckentfremdung gespeicherter Daten zu Werbezwecken eine Einwilligung vorausgesetzt wird.

Der Entwurf sieht eine Reihe von zusätzlichen Verschlechterungen des Datenschutzes in der Telekommunikation vor, die die Datenschutzbeauftragten in einer Entschließung öffentlich kritisiert haben.[30] Der Bundesrat hat zudem noch gravierendere Einschnitte in den Datenschutz verlangt.

Es sollen nach dem Willen der Bundesregierung die Anbieter in Zukunft berechtigt sein, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne überzeugende Begründung eine Regelung aufgegeben, die als Regelfall bisher die Speicherung von verkürzten Zielrufnummern vorsieht. Mit der in der Praxis bewährten bisherigen Regelung werden sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen berücksichtigt. Dem Bundesrat geht auch der Vorschlag der Bundesregierung nicht weit genug. Er fordert, allein im Interesse der Sicherheitsbehörden, die Anbieter zu einer sechsmonatigen Speicherung aller Verkehrsdaten zu verpflichten.

Die Vorschläge der Bundesregierung und mehr noch die des Bundesrates würden dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert blieben und damit dem Zugriff anderer Stellen ausgesetzt wären, wenn die Diensteanbieter sie für ihre Abrechnungszwecke

[29] vgl. Tätigkeitsbericht 2001, A 3.1.1

[30] vgl. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21. November 2003 „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“, Dokumente zu Datenschutz und Informationsfreiheit, A 1.4

nicht mehr benötigten. Unberücksichtigt blieben zudem die Rechte der angerufenen Teilnehmer, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird. Die Umsetzung der Forderungen des Bundesrates würden dazu führen, dass auf Vorrat gespeicherte unvorstellbare Datenmengen dem Zugriff von Strafverfolgern, Polizisten und Geheimdiensten ausgesetzt wären, ohne dass dem ein nennenswerter Sicherheitsgewinn gegenübersteht, da nur ein verschwindend geringer Teil dieser Daten jemals erforderlich sein wird. Mit einer solchen Vorratsdatenspeicherung wäre die Grenze des verfassungsrechtlich Zulässigen überschritten.

Die Datenschutzbeauftragten werden sich zudem unverändert gegen die von der Bundesregierung geplante Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys einsetzen und sehen sich jetzt in dieser Auffassung durch ein Urteil des Bundesverwaltungsgerichts bestätigt[31]. Auch diese Pläne würden auf der Ebene der Bestandsdaten zu einer verdachtslosen Datenspeicherung auf Vorrat führen. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Die Datenschutzbeauftragten von Bund und Ländern wenden sich entschieden gegen die fortwährende Aushöhlung des grundrechtlich geschützten Fernmeldegeheimnisses und appellieren an Bundesregierung und Bundestag, das bisher vorbildhafte Datenschutzniveau in der elektronischen Kommunikation nicht leichtfertig infrage zu stellen.

3.1.2 Unzulässige Speicherung von IP-Adressen durch Access-Provider

Bei der Vermittlung des Zugangs zum Internet ist es eine weit verbreitete Praxis der Anbieter (Access-Provider), die IP-Adressen der Nutzerinnen und Nutzer für einen bestimmten Zeitraum nach Ende der Nutzung zu speichern. Diese Tatsache war Gegenstand der datenschutzrechtlichen Prüfung eines bedeutenden Anbieters durch das Regierungspräsidium Darmstadt als zuständige Aufsichtsbehörde.[32]

Das Regierungspräsidium hält die Speicherung von IP-Adressen für Zwecke der Abrechnung und aus Gründen der Datensicherheit für zulässig.

---

[31] vgl. Urteil des BVerwG vom 22. Oktober 2003 (Az.: 6 C 23.02)

[32] Die Stellungnahme des Regierungspräsidiums Darmstadt ist im Internet veröffentlicht unter http://www.jurpc.de/rechtspr/20030043.htm

Da auch öffentliche Stellen des Landes als Access-Provider in Erscheinung treten können (z. B. wenn sie ihren Bediensteten die private Nutzung des Internets erlauben), weisen wir demgegenüber auf Folgendes hin:

Es dürfen nur solche Daten gespeichert werden, die für die Inanspruchnahme und Abrechnung des Dienstes erforderlich sind. Soweit die Nutzung des Internets nicht abgerechnet wird, besteht nach Ende der Nutzung ohnehin keine Rechtfertigung, die IP-Adressen zu speichern. Aber auch für die Abrechnung eines kostenpflichtigen Zugangs werden die IP-Adressen nicht benötigt. Die so genannten Radius-Server (Remote Authentication Dial-in User Service) authentifizieren anhand der Nutzerkennung und des Passwortes den Nutzer. Zudem können Zeitpunkt der An- und Abmeldung protokolliert werden. Die IP-Adresse ist dagegen zum Nachweis der Leistungserbringung nicht nötig.

Auch Gründe der Datensicherheit können die Speicherung von IP-Adressen nicht rechtfertigen. Zwar sind die Anbieter gesetzlich verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen. Zum Schutz der eigenen Datensicherheit des Anbieters ist die IP-Adresse jedoch nicht erforderlich. Sie könnte allenfalls dazu dienen, die Identität eines Nutzers zu bestimmen, der sich möglicherweise missbräuchlich verhalten hat. Dies erhöht die Datensicherheit allerdings in keiner Weise. Die Anbieter sind vielmehr verpflichtet, die geeigneten technischen Maßnahmen zur Abwehr von Angriffen zu ergreifen. Konkrete Maßnahmen können u. a. der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“[33] entnommen werden.

Die Vorschriften über die technischen und organisatorischen Maßnahmen dienen dem Schutz der Persönlichkeitsrechte und würden ins Gegenteil verkehrt, wenn sie als Rechtsgrundlage für eine umfassende Protokollierung der Internetnutzung herangezogen würden.

Bei der Vermittlung des Zugangs zum Internet ist eine regelmäßige Speicherung der den Nutzern zugewiesenen IP-Adressen weder für Abrechnungszwecke noch aus Gründen der Datensicherheit erforderlich und damit unzulässig.

[33] im Internet abrufbar unter http://www.lda.brandenburg.de

3.1.3 Es geht auch anders – Vorbildliches Internet-Angebot einer Gemeinde

Auf Grund der Beschwerde eines Bürgers haben wir uns mit dem Internet-Angebot der Gemeinde Petershagen/Eggersdorf[34] beschäftigt. Gegenstand der Prüfung war u. a. die Tatsache, dass der von der Gemeinde mit der Bereitstellung und Administration des Angebotes beauftragte Anbieter automatisch die IP-Adressen aller Zugriffe protokollierte.

Mit der Bereitstellung eines eigenen Internet-Angebotes betreibt die Gemeinde einen Mediendienst nach dem Mediendienste-Staatsvertrag (MDStV). Sie ist auch dann verantwortlicher Anbieter dieses Mediendienstes, wenn sie einen Dritten mit der technischen Abwicklung des Angebotes beauftragt hat (Web-Hosting). Neben den eigenen datenschutzrechtlichen Pflichten des Auftragnehmers muss auch die Gemeinde als Auftraggeber dafür Sorge tragen, dass die datenschutzrechtlichen Bestimmungen der §§ 16 bis 21 MDStV eingehalten werden.

Danach dürfen u. a. personenbezogene Daten über Beginn, Ende, Umfang oder Dauer der Nutzung eines Internet-Angebots (Nutzungsdaten) ohne Einwilligung des Nutzers nur dann erhoben, verarbeitet und genutzt werden, wenn sie für die Inanspruchnahme des Dienstes oder dessen Abrechnung erforderlich sind. Dabei ist zu berücksichtigen, dass auch dynamisch vergebende IP-Adressen als personenbezogene Daten zu behandeln sind, da mithilfe des Access-Providers ein Personenbezug hergestellt werden kann.

Handelt es sich – wie in den weitaus meisten Fällen – um ein kostenloses Angebot, ist eine Speicherung von IP-Adressen nach Ende des Nutzungsvorgangs für Abrechnungszwecke nicht erforderlich.

Der von der Gemeinde beauftragte Provider rechtfertigte die Protokollierung mit dem Argument, die Daten würden für die Erkennung und Abwehr von Hacker-Angriffen aus Gründen der Datensicherheit benötigt. Auch diese Begründung hat uns nicht überzeugt.

Selbstverständlich muss es dem Anbieter möglich sein, Hacker-Angriffe zu erkennen und abzuwehren. Der Zugang zum Webserver kann für diesen Zweck zum einen so konfiguriert werden, dass er nur die Protokollierung problematischer Zugriffe bzw. Zugriffsversuche mit vollständigen IP-Adressen vornimmt. Für eine Protokollierung erfolgreicher Zugriffe besteht allerdings auch aus Gründen der Datensicherheit kein Erfordernis. Zudem werden die Hacker-Angriffe nicht dadurch erkannt und abgewehrt, dass der Provider die IP-Adresse des zugreifenden Rechners kennt. Für die Analyse und Abwehr

[34] http://www.doppeldorf.de

solcher Angriffe ist deren Herkunft letztlich nicht unmittelbar relevant, sodass die geeigneten Maßnahmen (z. B. die Abschottung durch Firewalls) auch ohne die Kenntnis der IP-Adressen getroffen werden können.[35] Im Ergebnis gibt es keine Rechtsgrundlage für die automatische Speicherung vollständiger IP-Adressen in Protokolldateien. Allerdings bestehen keine datenschutzrechtlichen Einwände, wenn die Protokolldateien ohne oder mit verkürzter IP-Adresse, z. B. zu statistischen Zwecken, gespeichert werden.

Die Gemeinde hat unsere Hinweise sehr ernst genommen. Da der von ihr beauftragte Anbieter nicht bereit war, auf die Protokollierung der IP-Adressen zu verzichten, hat die Gemeinde den entsprechenden Vertrag gekündigt und einen regionalen Anbieter beauftragt, der bereit war, die datenschutzrechtlichen Forderungen umzusetzen.

Auch im Übrigen kann das Internet-Angebot der Gemeinde aus datenschutzrechtlicher Sicht nunmehr als vorbildlich bezeichnet werden: Es enthält eine ausreichende Datenschutzerklärung, auf das Setzen von Cookies wird verzichtet und das Online-Forum bietet die Möglichkeit einer pseudonymen Teilnahme.

Beauftragt eine öffentliche Stelle einen Provider mit der technischen Abwicklung ihres Internet-Angebots, bleibt sie für die Einhaltung der datenschutzrechtlichen Pflichten nach dem Mediendienste-Staatsvertrag verantwortlich. Es ist unzulässig, die vollständigen IP-Adressen aller Zugriffe automatisch in Protokolldateien zu speichern.

3.1.4 Online-Prüfungen von Websites

Um verschiedene Websites öffentlicher Stellen im Rahmen unserer gesetzlichen Aufgabe auf die Einhaltung datenschutzrechtlicher Vorgaben zu prüfen, bedienten wir uns eines Software-Werkzeugs, das es ermöglicht, auch komplexe Internet-Angebote online vollständig zu analysieren.

Im Verlauf der Prüfung werden zur Analyse der Websites die entsprechenden Seiten des Angebots auf einen Prüfserver geladen und dort einer automatischen Überprüfung auf eine Vielzahl von datenschutzrelevanten Aspekten unterzogen. Das Ergebnis der Untersuchung bewerten wir und ergänzen es gegebenenfalls durch weitere Feststellungen.

Die Prüfung hilft uns, zu kontrollieren, ob der Anbieter seinen gesetzlichen Informationspflichten (Anbieterkennzeichnung, Datenschutz-Unterrichtung) nachkommt, ob personenbezogene Daten veröffentlicht oder erhoben werden

[35] zur Speicherung von IP-Adressen durch Access-Provider s. o. A 3.1.2

und ob eine Weitervermittlung zu Angeboten anderer Anbieter integriert ist. Ferner wird das Angebot auf die Verwendung von Cookies, Verschlüsselungsmechanismen und interaktiver Formulare untersucht. Der Prüfbericht endet mit einem Katalog von Fragen, die nicht automatisch beantwortet werden können und einer Bearbeitung durch uns bedürfen.

Die von uns stichprobenartig geprüften Internetangebote, die sich auf die Bereiche Bildung, Polizei und Kommune beschränkt haben, erfüllen im wesentlichen die Anforderungen des Datenschutzes. Einige Anbieter hatten Defizite bei der Anbieterkennzeichnung. Andere informierten nur mangelhaft über die von ihnen getroffenen Maßnahmen zum Datenschutz oder wiesen nicht darauf hin, dass Formulardaten ungesichert übertragen werden. Die meisten Mängel werden von den Anbietern auf Grund unseres Prüfberichts behoben.

Anbieter von Internetseiten sind Anbieter nach dem Teledienstegesetz (TDG) bzw. dem Mediendienste-Staatsvertrag (MDStV). Sie müssen sich an die datenschutzrechtlichen Bestimmungen des Teledienstedatenschutzgesetzes (TDDSG) bzw. des MDStV halten. Dazu gehört im wesentlichen die Anbieterkennzeichnung, die Datenschutzerklärung, Informationen zu einer möglichen Weiterleitung und die Verschlüsselung der zu übertragenen Formulardaten bzw. der Hinweis auf fehlende Verschlüsselung. Der Nutzer ist auch zu Beginn des Nutzungsvorgangs umfassend über die Verarbeitung seiner personenbezogenen Daten zu unterrichten.

3.2 Rundfunk

3.2.1 Neuordnung der Datenschutzaufsicht beim öffentlich-rechtlichen Rundfunk

Auf Grund des zwischen den Ländern Berlin und Brandenburg geschlossenen Staatsvertrages über die Errichtung einer gemeinsamen Rundfunkanstalt entstand an Stelle des Ostdeutschen Rundfunks Brandenburg (ORB) und des Senders Freies Berlin (SFB) die Zwei-Länder-Anstalt Rundfunk Berlin-Brandenburg (RBB).

Mit dem In-Kraft-Treten des Staatsvertrages am 1. Mai 2003 wurde u. a. auch die Kontrolle des Datenschutzes beim RBB neu geordnet. Sofern der RBB, vor allem durch die für ihn tätigen Journalisten, personenbezogene Daten zu journalistischen und redaktionellen Zwecken verarbeitet, wird wegen der verfassungsrechtlich garantierten Rundfunkfreiheit die Datenschutzaufsicht ausschließlich durch die Datenschutzbeauftragte des RBB ausgeübt. Ist ein Betroffener zum Beispiel der Ansicht, der RBB habe in der Berichterstattung durch die Veröffentlichung personenbezogener Informationen seine Persön-

lichkeitsrechte beeinträchtigt, kann er sich unmittelbar an die Datenschutzbeauftragte des RBB unter folgender Anschrift wenden:

Rundfunk Berlin-Brandenburg
Datenschutzbeauftragte
Masurenallee 8-14
14046 Berlin

Soweit der RBB außerhalb des journalistischen Bereichs personenbezogene Daten zu wirtschaftlichen oder administrativen Zwecken verarbeitet, ist wie bisher bei ORB und SFB eine unabhängige Datenschutzkontrolle gewährleistet. Sie wird durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit im Benehmen mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg wahrgenommen. Dies betrifft in der Praxis fast ausschließlich die Verarbeitung personenbezogener Daten durch die vom RBB beauftragte Gebühreneinzugszentrale (GEZ) zum Zwecke der Erhebung der Rundfunkgebühren. Dieses Thema ist bereits häufiger Gegenstand unserer Tätigkeitsberichte gewesen.[36]

Die Verarbeitung personenbezogener Daten durch die GEZ wird hinsichtlich der Gebührenzahlerinnen und Gebührenzahler aus Berlin und Brandenburg einvernehmlich durch die unabhängigen Datenschutzbeauftragten beider Länder kontrolliert. In der Praxis kann sich jedermann an uns oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden.

3.2.2 Datenhunger der GEZ kaum zu stillen

Auf Grund eines Beschlusses der Ministerpräsidenten der Länder vom Oktober 2002 soll die Finanzierung des öffentlich-rechtlichen Rundfunks weiterentwickelt werden. Dabei soll vor allem berücksichtigt werden, dass die technische Entwicklung einen qualitativ zunehmend besseren Rundfunkempfang auch über das Internet ermöglicht. Für diese – zurzeit auf Grund eines von den Ländern vereinbarten Moratoriums – gebührenfreie Empfangsmöglichkeit soll in Zukunft auch bezahlt werden. Die im zurückliegenden Jahr gemachten Vorschläge für einen neuen Rundfunkgebührenstaatsvertrag sahen jedoch aus Sicht des Datenschutzes zum Teil gravierende Verschlechterungen vor.

Geplant war, alle Meldebehörden zu verpflichten, der GEZ die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch wäre bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-

[36] vgl. Tätigkeitsbericht 1999, A 3.4.2; Tätigkeitsbericht 2000, A 3.6; Tätigkeitsbericht 2001, A 3.2; Tätigkeitsbericht 2002, A 3.2.2 sowie unten, A 3.2.2

jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen) entstanden, obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

Zudem sollte die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Melderegistern um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten wollte die GEZ künftig auch online zugreifen.

Schließlich sollte die von uns als unzulässig festgestellte Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben[37], ausdrücklich erlaubt werden.

Die Datenschutzbeauftragten des Bundes und der Länder waren sich einig, dass die auf Vorstellungen der Rundfunkanstalten basierenden Vorschläge unverhältnismäßig waren und daher nicht akzeptiert werden konnten. Sie haben sich in einer Entschließung vom 30. April 2003 entschieden dagegen ausgesprochen.[38]

Nicht zuletzt wegen der massiven Kritik der Datenschutzbeauftragten wurden die Pläne fallen gelassen und das Moratorium zum gebührenfreien Rundfunkempfang über das Internet bis zum 31. Dezember 2006 verlängert.

Die Landesregierung sollte auch in Zukunft eine weitere Verschlechterung des ohnehin schon häufig kritisierten Datenschutzniveaus beim Einzug der Rundfunkgebühren[39] nicht zulassen. Bei der seit Jahren diskutierten Neuordnung der Finanzierung des öffentlich-rechtlichen Rundfunks sollten alternative und gleichzeitig datenschutzfreundliche Modelle ernsthaft geprüft und unterstützt werden.

[37] vgl. Tätigkeitsbericht 2002, A 3.2.2

[38] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A I 2

[39] vgl. Tätigkeitsbericht 1999, A 3.4.2; Tätigkeitsbericht 2000, A 3.6; Tätigkeitsbericht 2001, A 3.2.2; Tätigkeitsbericht 2002, A 3.2.2

4 Inneres

4.1 Polizei- und Ordnungsbehörden

4.1.1 „INPOL-neu“ und „INPOL-Land“

Im Berichtszeitraum ist die Modernisierung des länderübergreifenden Informationssystems der Polizei (INPOL) beim Bundeskriminalamt durch die Einführung des Verfahrens „INPOL-neu“ vorangetrieben worden. Neben einer Überarbeitung der INPOL-Errichtungsanordnungen bedurfte es daher einer Anbindung der bei den Länderpolizeien betriebenen Datenbanken, aus denen der weitaus größte Teil der insgesamt in INPOL verarbeiteten Daten fließt.

Das Bundeskriminalamt betreibt als Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern das Polizeiliche Informationssystem „INPOL-neu“ als Verbunddatei (§ 11 Bundeskriminalamtgesetz - BKAG). Das System ist in zwei Bereiche gegliedert: in „INPOL-zentral“ beim Bundeskriminalamt und „INPOL-Land“ bei den Länderpolizeien. Die Länderverfahren dienen der Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten sowie der Strafverfolgung, soweit die Delikte von bundesweiter Bedeutung sind. Zu jeder Datei müssen die Modalitäten der einzelnen Verarbeitungsschritte verbindlich festgelegt werden.

Entsprechend der BKA-Errichtungsanordnung ist auch in Brandenburg festgelegt worden, dass nicht nur bestimmte, überregional bedeutsame Straftaten, sondern auch alle Staatsschutzdelikte bundesweit gespeichert werden sollen. Eine Straftat ist aber erst dann der länderübergreifenden oder internationalen Kriminalität zuzurechnen, wenn dadurch die Belange eines anderen Bundeslandes oder eines anderen Staates berührt sind. Ausschlaggebend für die Einstufung einer Tat als eine Straftat von erheblicher Bedeutung ist nicht der Straftatbestand als solcher, sondern die Art und Schwere der konkreten Tat. Erst wenn beide Aspekte berücksichtigt wurden und beide Merkmale vorliegen, ist die Einstufung als „überregional bedeutsam“ gerechtfertigt. Vor diesem Hintergrund ist insbesondere die Festlegung nicht sachgerecht, dass politisch motivierte Kriminalität stets überregional bedeutsam sei und die dazu geführte Kriminalakte eines Täters oder Tatverdächtigen daher im bundesweit abrufbaren Kriminalaktennachweis-Bund registriert werden muss. Wir haben angeregt, festzulegen, dass Kriminalakten erst dann in die Verbunddatei eingestellt werden dürfen, wenn der Ausgang des staatsanwaltschaftlichen Ermittlungsverfahrens gegen den Täter oder Tatverdächtigen bekannt ist.

Weiterhin haben wir gefordert, im Entwurf den die Rasterfahndung regelnden § 46 BbgPolG als Rechtsgrundlage für die Verarbeitung von personenbezo-

genen Daten in „INPOL-Land“ zu streichen. Die Erhebung und Verarbeitung von Rasterfahndungsdaten in der dem allgemeinen Zugriff der Polizei offenstehenden Datei „INPOL-Land“ ist unzulässig. Sie ist mit der strikten Zweckbindung der Rasterfahndungsdaten nicht zu vereinbaren, die in allen Phasen der Durchführung eine Verarbeitung in einer der Maßnahme gewidmeten Datei erfordert. Erst nach Abschluss der Rasterfahndung können die Daten von als Tatverdächtige ermittelten Personen ggf. in „INPOL-Land“ verarbeitet werden.

Die Verbunddatei „INPOL-neu“ besteht aus den zwei Komponenten: „INPOL-zentral“ beim Bundeskriminalamt und das bei der jeweiligen Landespolizei betriebene Verfahren „INPOL-Land“. Das brandenburgische Verfahrens- und Anlagenverzeichnis hat das Ministerium des Innern unseren Hinweisen entsprechend modifiziert.

4.1.2 ASS – eine landesweite Datenbank für den Staatsschutz

Im Berichtszeitraum ist mit dem „Auswerte-System Staatsschutz Brandenburg“ (ASS) eine landesweite Datei für alle Dienststellen des polizeilichen Staatsschutzes in Betrieb genommen worden.

ASS wird auf der Basis eines strategischen Informationssystems betrieben, das Informationen beliebiger Komplexität grafisch darstellen kann. Seine besondere Stärke liegt in der Auswertung: Ausgehend von einem oder mehreren Objekten werden sämtliche anderen Objekte gezeigt, die direkt oder indirekt mit dem Ausgangsobjekt verbunden sind. Die Auswertung ist damit nicht mehr abhängig von einer bestimmten Fragestellung, sondern es werden zuverlässig sämtliche überhaupt in der Datenbank vorhandenen Informationen präsentiert. Damit lassen sich die klassischen W-Fragen der Kriminalistik (wer, was, wann, wo, wie, warum und womit) soweit beantworten, als sie als Objekt und Beziehungen zu anderen Objekten darstellbar sind. Mit diesem flexiblen Recherche-Werkzeug können zahlreiche bisher unbekannte Zusammenhänge sichtbar gemacht werden.

Bislang wurde das strategische Informationssystem nur im Rahmen bestimmter Ermittlungsverfahren eingesetzt. Solange eine Datei zu dem Zweck betrieben wird, Aufklärung und Verfolgung bereits begangener Straftaten in einem bestimmten Ermittlungsverfahren zu unterstützen, ergibt sich keine besondere datenschutzrechtliche Problematik. Das Ermittlungsverfahren bildet einen abgeschlossenen Rahmen, der durch die Eröffnung bzw. Nichteröffnung eines Gerichtsverfahrens zeitlich begrenzt ist und somit eine klar definierte Abgrenzung von personenbezogenen Daten ermöglicht.

ASS hat jedoch eine andere datenschutzrechtliche Qualität. Es ist ein Verdachtsgewinnungs- bzw. Verdachtsverdichtungsinstrument. Das System enthält neben Daten, deren Tatbezug zu Straftaten auf Grund von Ermittlungen schon bestätigt worden ist, auch solche Daten, die lediglich auf Grund bestimmter Merkmale eingestellt werden, ohne dass ihre Relevanz bereits nachweisbar ist. Durch die vorbeugende Bekämpfung von Straftaten wird der zeitliche und sachliche Rahmen der zulässigen Datenverarbeitung erheblich ausgeweitet. Ausschlaggebend für die weitere Speicherung in ASS ist die von der Polizei erstellte Prognose, dass eine Person auch künftig wieder als Täter im Bereich des politischen Strafrechts auftreten wird. Maßstab, ob die Daten von Kontakt- und Begleitpersonen eines Tatverdächtigen – also selbst nicht tatverdächtigen Personen – gespeichert werden, richtet sich nach der Auslegung des unbestimmten Rechtsbegriffs der „Straftat von erheblicher Bedeutung“. Auch wenn die Daten aus strafrechtlichen Ermittlungsverfahren übernommen wurden und sich damit noch ein Bezug zu einem bestimmten Ermittlungsverfahren herstellen lässt, greift die verfahrensübergreifende Datenverarbeitung tiefer in die Persönlichkeitsrechte der Betroffenen ein als bisherige Dateien.

Um die von ASS ausgehenden datenschutzrechtlichen Risiken zu minimieren, insbesondere aber um die Datenqualität und damit die Aussagefähigkeit der Datenbank zu sichern, wurde ein zweistufiger Systemaufbau gewählt. Betrieben wird das Verbundsystem über ein „Rootsystem“, an welches alle Nutzer – neben den Staatsschutzdienststellen in den Polizeipräsidien und im Landeskriminalamt auch die Kommissariate „Jugend“, „Täterorientierte Maßnahmen“, MEGA und TOMEG in den Schutzbereichen gleichberechtigt angeschlossen sind. Auf dieser Systemebene werden ausschließlich bewertete Daten der Staatsschutzkriminalität geführt. Vorgeschaltet sind „Vorsysteme“, die einzelne Nutzer einrichten zur Unterstützung laufender Ermittlungsverfahren und Gefahrenabwehrvorgänge sowie zur Speicherung besonders schutzwürdiger oder sensibler personenbezogener Daten. Unbewertete Daten dürfen nur auf dieser Systemebene verarbeitet werden. In das zentrale Rootsystem kommen Daten aus den Vorsystemen erst, wenn der Vorgang abgeschlossen ist und die Prüfung der durch die Vorgangsbearbeitung erlangten personenbezogenen Daten ergeben hat, dass sie für die weitere Aufgabenerfüllung erforderlich sind. Die anderen Daten werden gelöscht. Darüber hinaus müssen auch personenbezogene Daten von Tatverdächtigen, die durch die Ermittlungen nicht Beschuldigteneigenschaft erlangt haben, nach Abschluss des strafrechtlichen Ermittlungsverfahrens gelöscht werden. Schließlich dürfen die Daten von Kontakt- und Begleitpersonen nicht länger als insgesamt drei Jahre gespeichert werden.

Mit dem Verbundsystem ASS steht der Brandenburgischen Polizei nach dem Polizeilichen Auskunftssystem Straftaten (PASS) ein weiterer Datenbestand

landesübergreifend, wenn auch beschränkt auf den Staatsschutz zur Verfügung. Die davon eventuell ausgehenden Risiken für die Rechte der Betroffenen müssen vor der Freigabe des Verbundsystems gem. § 7 Abs. 3 BbgDSG analysiert und auf der Basis eines Sicherheitskonzepts durch entsprechende technisch organisatorische Maßnahmen aufgefangen werden. Dessen ungeachtet enthielt das uns im Entwurf zugegangene Verfahrensverzeichnis zunächst keine Risikoanalyse. Nach mehreren Entwürfen ist schließlich zusammen mit dem endgültigen überarbeiteten Verfahrensverzeichnis auch eine den datenschutzrechtlichen Anforderungen genügende Risikoanalyse vor der Inbetriebnahme der Datei erstellt worden.

Mit dem Verbundsystem ASS hat die Datenverarbeitung der brandenburgischen Polizei eine neue Qualität erreicht. Die davon ausgehenden Risiken für die Persönlichkeitsrechte sind vor der Einrichtung der Datenbank analysiert und bei dem Systemaufbau und bei der Festlegung von Prüffristen sowie der technisch organisatorischen Maßnahmen berücksichtigt worden.

4.1.3 Globalvertrag zur Datenverarbeitung bei der Polizei

Seit Abschluss der Polizeistrukturreform lässt die Brandenburgische Polizei ihre Daten beim Zentraldienst der Polizei (ZD Pol) verarbeiten. Die mit dieser Umstellung in den Polizeibehörden ausgelöste Unsicherheit darüber, welche Stelle wofür zuständig und damit verantwortlich ist, sind noch nicht behoben.

Rechtlich ist der Zentraldienst keine Polizeibehörde wie die Polizeipräsidien und das Landeskriminalamt, sondern eine Einrichtung (§ 1 Abs. 2 Polizeiorganisationsgesetz – POG). Welche Aufgaben ihm zugewiesen sind, ist gesetzlich nicht geregelt. Dass er die gesamte Datenverarbeitung der brandenburgischen Polizei betreiben soll, ergibt sich nur indirekt aus Art. 15 Polizeistrukturreformgesetz, wonach dem Zentraldienst alle Bediensteten der Sachgebiete für Informations- und Kommunikationstechnik der gegenwärtigen sowie der ehemaligen Polizeipräsidien und des Landeskriminalamts zugeordnet werden. Damit hat jedoch keine Übertragung der rechtlichen Entscheidungsbefugnis stattgefunden, sodass er die Datenverarbeitung auch nicht als eigenständige hoheitliche Aufgabe wahrnehmen kann. Es handelt sich vielmehr um eine Datenverarbeitung im Auftrag, bei der die zur Ausübung hoheitlicher Aufgaben befugten Polizeibehörden als Daten verarbeitende Stellen den Auftragnehmer ZD Pol mit der Verarbeitung ihrer Daten beauftragen und insoweit weisungsbefugt sind. Dazu bedarf es gem. § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) eines Vertrages[40].

[40] vgl. dazu schon oben A 1.2

Ungeachtet der insoweit klaren Rechtslage herrschen in den Polizeibehörden immer noch Zweifel darüber, inwieweit sie gegenüber ZD Pol und insbesondere gegenüber seinen bei ihnen tätigen Mitarbeitern weisungsberechtigt sind. Dabei wird zu Unrecht aus dem in § 10 Abs. 3 POG ausdrücklich geregelten Weisungsrecht des Landeskriminalamts als zentrale Nachrichten- und Auswertestelle gegenüber den Polizeipräsidien geschlossen, dass auch ein Weisungsrecht der Polizeibehörden als Daten verarbeitende Stellen gegenüber ihrem Auftragnehmer ZD Pol einer ausdrücklichen gesetzlichen Regelung bedürfe. Dies ist jedoch nicht erforderlich. Der Vertrag muss das Weisungsrecht der auftraggebenden Polizeibehörden klar ausgestalten und eine Kündigungsmöglichkeit der Vertragspartner für den Fall vorsehen, dass die vertraglichen Pflichten nicht eingehalten werden.

Der uns zur Stellungnahme übersandte Vertragsentwurf ist in zwei Teile gegliedert. Der erste Teil enthält die allgemeinen Vertragsbestimmungen, wie die Festlegung der Rechte und Pflichten der Vertragspartner, während in dem zweiten Teil die Verfahren aufgeführt sind, die die jeweilige Polizeibehörde beim Zentraldienst verarbeiten lässt. Diese Anlage lässt sich fortlaufend um neu hinzukommende Verfahren ergänzen, ohne dass jeweils ein neuer Vertrag abgeschlossen werden muss.

Wir haben angeregt, im Vertrag festzulegen, dass die Polizeibehörde die Risikoanalyse hinsichtlich der Verarbeitung personenbezogener Daten vornimmt, da nur sie beurteilen kann, ob davon spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen. Der Zentraldienst sollte das Sicherheitskonzept anhand der örtlichen und personellen Gegebenheiten sowie des Ergebnisses der Risikoanalyse entwickeln. Damit der Auftraggeber seiner Verantwortung als Daten verarbeitende Stelle auch im Zusammenhang mit den technisch-organisatorischen Maßnahmen beim Auftragnehmer gerecht werden kann, muss er das Sicherheitskonzept genehmigen. Es sollte daher ebenso wie die Risikoanalyse Bestandteil des Vertrages werden. Dazu wird der Auftraggeber verpflichtet, dem Zentraldienst bei Vertragsabschluss ein jeweils gültiges Verfahrensverzeichnis und die Risikoanalyse für jedes in Auftrag gegebene Verfahren zu übergeben.

Zudem ist es notwendig, dass die Polizeibehörden als Auftraggeber entsprechend qualifizierte Bedienstete benennen oder IT-Kopfstellen bilden, die die weiter bestehende datenschutzrechtliche Verantwortung der Präsidien und des Landeskriminalamtes gegenüber dem Zentraldienst der Polizei wahrnehmen und gegebenenfalls entsprechende Weisungen an dessen Bedienstete erteilen. Es geht nicht darum, die in der Polizeistrukturreform getroffene Entscheidung zur Bündelung von EDV-Fachleuten beim Zentraldienst zu revidieren. Die Auftraggeber müssen aber personell und organisatorisch in die Lage versetzt werden, die Verarbeitung der Daten in ihrem Auftrag beim

Zentraldienst zu kontrollieren. Ihre datenschutzrechtliche Verantwortung darf nicht „verdunsten“.

Die Polizeibehörden erheben und nutzen die Daten für die ihnen im Polizeigesetz zugewiesenen Vollzugsaufgaben. Sie sind als Daten verarbeitende Stellen i. S. d. Datenschutzgesetzes für die gesamte Datenverarbeitung auch nach der Polizeistrukturreform verantwortlich. Der Zentraldienst der Polizei kann nur in ihrem Auftrag Daten verarbeiten. Dazu ist ein Vertrag erforderlich, in dem die Rechte und Pflichten einschließlich der Erstellung von Risikoanalysen und Sicherheitskonzepten eindeutig festgelegt sind. Die auftraggebenden Polizeibehörden sind gegenüber dem Zentraldienst der Polizei und seinen Mitarbeitern weisungsberechtigt. Sie sollten hiermit entsprechend qualifizierte Bedienstete betrauen oder IT-Kopfstellen bilden.

4.1.4 Ein Datenlöschverfahren in PASS ohne Löschwirkung

Ein Petent wies uns auf das Löschungsverfahren im Polizeilichen Auskunftssystem Straftaten (PASS) in Fällen von Kleinstkriminalität hin, das dem rechtlichen Anspruch der Betroffenen, in polizeilichen Datenbanken nicht mehr registriert zu sein, wenn der Verdacht einer Straftat gegen sie entfallen ist, nicht ausreichend Rechnung trägt.

Die in Akten und Datenbanken gespeicherten personenbezogenen Daten sind zu löschen, wenn bei der Polizei der Verdacht einer Straftat gegen den Betroffenen entfallen ist (§ 39 Abs. 2 Brandenburgisches Polizeigesetz - BbgPolG). Dagegen ist im Verfahrensverzeichnis zu PASS festgelegt, dass in allen Fällen von Kleinstkriminalität ohne Kriminalakte zu dem Tatverdächtigen der vollständige Datensatz nicht sofort nach Wegfall des Tatverdachts, sondern erst 13 Monate nach der Abgabe des Verfahrens an die Staatsanwaltschaft gelöscht werden muss. Somit müssen vor allem bei Verfahren, die die Staatsanwaltschaft mangels ausreichenden Anfangsverdachts bald einstellt, die Betroffenen eine verlängerte Speicherung ihrer Daten hinnehmen. Um dem Rechtsanspruch auf unverzügliche Datenlöschung wenigstens teilweise Rechnung zu tragen, werden Name und Vorname in der Identdatengruppe durch „ANONYM“ ersetzt.

Festgelegt wurde eine 13-monatige Aufbewahrungsfrist, die wir schon bei der Inbetriebnahme von PASS als zu lang kritisiert haben, weil die Fälle in die jährlich zu erstellende Kriminalstatistik einfließen müssen und dazu neben dem Delikt auch Daten wie Geburtsjahr und Adresse benötigt werden. Während der 13 Monate werden die Datensätze jedoch nicht nur zur Statistiknutzung aufbewahrt, sondern auch in Datenbank-Recherchen einbezogen.

Grundsätzlich ist die weitere Nutzung zu löschender Daten nur in Ausnahmefällen zulässig. Dazu zählt die in § 39 Abs. 5 BbgPolG geregelte Nutzungsbefugnis rechtmäßig aufbewahrter Daten für Statistikzwecke, geknüpft an die Voraussetzung, dass personenbezogene Daten zum frühest möglichen Zeitpunkt anonymisiert werden. Diese Voraussetzung ist durch das oben beschriebene Verfahren aber nicht erfüllt. Als „anonymisiert“ gilt ein Datum erst dann, wenn der Personenbezug nicht oder nur mit unverhältnismäßig hohem Aufwand wiederhergestellt werden kann. Die noch belegten Datenfelder „Geburtsdatum“ und „Wohnanschrift“ der Identdatengruppe verlangen keinen unverhältnismäßig hohen Aufwand zur Deanonymisierung, sondern machen es leicht, den durch „Anonym“ ersetzten Namen wiederherzustellen. Andere Nutzungsmöglichkeiten zu löschender Datensätze – wie ihre Einbeziehung in Datenbank-Recherchen – sind im Polizeigesetz nicht vorgesehen, sodass es dazu an einer Rechtsgrundlage fehlt. Sie sind daher rechtswidrig.

Ein „Löschverfahren“, bei dem lediglich Name und Vorname durch „ANONYM“ ersetzt werden, ist gänzlich unzulänglich und stellt einen unzulässigen Eingriff in die Persönlichkeitsrechte des Betroffenen dar. Obwohl er nicht mehr „polizeipflichtig“ ist und daher einen Anspruch darauf hat, von der Polizei „in Ruhe gelassen zu werden“, stehen Daten über ihn ca. 8000 zugriffsberechtigten Polizeibediensteten zur Verfügung.

Als Ergebnis der datenschutzrechtlichen Prüfung halten wir eine Änderung des Verfahrens für unabdingbar. Zur Lösung des Problems haben wir vorgeschlagen, übergangsweise eine zusätzliche, nicht allgemein zugängliche Datenbank für Statistikzwecke in PASS zu schaffen, in der die nach § 39 Abs. 2 BbgPolG zu löschenden Datensätze abgelegt werden, sodass die gesamte Datengruppe – und nicht nur Name und Vorname – in dem im allgemeinen Zugriff stehenden Datenbankbereich „ANONYM“ gesetzt werden kann.

Die Praxis, ein Datum durch Umbenennung eines Feldes als Statistikdatum zu markieren, ist wegen der einfachen Wiederherstellung des Personenbezugs unzulässig. Zum Schutz der Persönlichkeitsrechte der Betroffenen müssen Daten, die nur noch zu Statistikzwecken aufbewahrt werden dürfen, entweder ausreichend anonymisiert oder – wenn das wie in PASS nicht möglich ist – durch geeignete Datenverarbeitungsmaßnahmen dem allgemeinen Datenzugriff für Vollzugszwecke entzogen werden.

4.1.5 Anforderungen an das Datenschutzkonzept der Deutsch-Polnischen Verbindungsstelle der Polizei, des BGS und des Zolls in Frankfurt (Oder)

Seit April 2003 wird im Polizeipräsidium Frankfurt (Oder) die gemeinsame Deutsch-Polnische Verbindungsstelle (DPV) der Polizei, des Bundesgrenzschutzes (BGS) und des Zolls aufgebaut. Sie soll anfragenden Behörden beider Länder unter Beachtung der einschlägigen Rechtsvorschriften die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zur Verfügung stellen.

Rechtsgrundlage für den vorgesehenen Informationsaustausch ist das noch nicht ratifizierte Abkommen vom 18. Februar 2002 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Polen über die Zusammenarbeit der Polizeibehörden und der Grenzschutzbehörden in den Grenzgebieten sowie die für die Vertragsparteien jeweils geltenden innerstaatlichen Rechtsvorschriften. Für die Datenübermittlungen brandenburgischer an polnische Polizeidienststellen sind dies § 42 i. V. m. § 41 Brandenburgisches Polizeigesetz (BbgPolG), für den Informationsaustausch zwischen sonstigen für die Gefahrenabwehr zuständigen brandenburgischen und polnischen öffentlichen Stellen § 43 i. V. m. § 41 BbgPolG. Letzteres gilt vor allem für den gem. Art. 5 des Abkommens vorgesehenen Informationsaustausch im Rahmen der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten. Auch bedarf es spätestens mit Aufnahme des Dienstbetriebes der Verbindungsstelle einer Rechtsverordnung über die Zulässigkeit der Datenübermittlungen an die polnischen Polizeibehörden, die bisher fehlt.

Wir haben vorgeschlagen, das Datenschutzkonzept grundsätzlich an Art. 19 des Abkommens zu orientieren. Es sollte enthalten:

- datenschutzrechtliche Vorkehrungen vor der Datenübermittlung

- Umfang der Übermittlungen

- Festlegung technisch-organisatorischer Maßnahmen

- Schulung der Mitarbeiter der Verbindungsstelle

Des Weiteren sollte das Konzept um die Rechtsgrundlagen für den Informationsaustausch ergänzt werden. Dabei wären neben dem Abkommen nicht nur das Polizeigesetz aufzuführen, sondern auch die einschlägigen Rechtsvorschriften für den Bundesgrenzschutz und den Zoll. Um deutlich zu machen, innerhalb welcher Grenzen sich der Informationsaustausch bewegen darf, sollte das Datenschutzkonzept darüber hinaus klarstellen, dass die übermit-

telten Daten grundsätzlich nur zu den in dem Abkommen aufgeführten Zwecken verwendet werden dürfen. Eine Zweck ändernde Nutzung ist nur zur Verhütung und Bekämpfung von Kriminalität von erheblicher Bedeutung, wie zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit, zulässig.

Es ist vorgesehen, dass Informationen über Datenübermittlungsvorgänge der Deutsch-Polnischen Verbindungsstelle während eines bestimmten, am Einzelfall orientierten Zeitraums aufbewahrt werden sollen. Dies scheint uns nicht sachgerecht. Zur Sicherung des Verwaltungshandelns bei der Verbindungsstelle ist es nur erforderlich, den einzelnen Übermittlungsvorgang jahrgangsbezogen abzulegen und nach Ablauf des dem Informationsaustausch folgenden Kalenderjahres zu vernichten.

Weiterhin muss gewährleistet werden, dass die Daten liefernde sowie die Daten empfangende Stelle den Zweck der Übermittlung und die Herkunft bzw. den Empfänger der Daten nachvollziehen können. Daher sollte das zum Datenaustausch von der Verbindungsstelle genutzte Formular bzw. die EDV-Maske den Anlass, z. B. die Straftat auf Grund derer ermittelt wird, sowie die weiteren zu einer Dokumentation erforderlichen Informationen enthalten. Das Datenschutzkonzept sollte um ein entsprechendes Formular ergänzt werden. Die empfangende Behörde ist verpflichtet, die übermittelnde Behörde auf Ersuchen über die Verwendung der übermittelten Daten und die dadurch erzielten Ergebnisse zu unterrichten. Bei einer zweckändernden Nutzung der Daten muss die Unterrichtung unaufgefordert erfolgen. Da davon auszugehen ist, dass diese Unterrichtungspflichten wiederum über die Verbindungsstelle erfolgen, haben wir angeregt, das Übermittlungsformular um einen abtrennbaren Abschnitt für die in Rede stehenden Unterrichtungspflichten zu ergänzen.

Ferner besteht eine Auskunftspflicht über den Informationsaustausch gegenüber dem Betroffenen, wenn dieser Auskunft über die zu seiner Person gespeicherten Daten verlangt hat. Rechtsgrundlage für die Auskunftserteilung ist das jeweilige Landesrecht nach Maßgabe der Zustimmung des Datenempfängers. Die zuständigen Landesbehörden sind explizit zu benennen.

Das Polizeipräsidium hat sich zu unseren Empfehlungen noch nicht geäußert.

Die im Aufbau befindliche Deutsch-Polnische Verbindungsstelle im Polizeipräsidium Frankfurt (Oder) darf im Rahmen des Deutsch-Polnischen-Abkommens unter Beachtung der dortigen datenschutzrechtlichen Vorgaben und der für Polizei, Bundesgrenzschutz und Zoll geltenden Rechtsvorschriften den Informationsaustausch zwischen deutschen und polnischen Sicherheits- und Ordnungsbehörden koordinieren. In einem Datenschutzkonzept sollten die Rechtsgrundlagen benannt, Hinweise zum Verfahren gegeben, Dokumentationspflichten durch geeignete Formulargestaltung unterstützt, die eigene Vorgangsverwaltung festgelegt und die Auskunft erteilenden Stellen bezeichnet werden.

4.1.6 „Freiwillige“ Teilnahme am DNA-Massenscreening

Die Staatsanwaltschaft Leipzig hat zur Aufklärung eines Mordfalles an zwei Mädchen aus dem Jahre 1994 ein DNA-Massenscreening angesetzt, in das auch eine Region in Brandenburg mit einbezogen wurde. Da sich zunächst nur wenige Personen an dem Massenscreening beteiligten, forderte die Polizei von den Meldebehörden die Daten einschließlich der gegenwärtigen Anschrift derjenigen Einwohner an, die auf Grund von Alter und Geschlecht als Täter infrage kommen könnten. Die Betroffenen wurden schriftlich zur Teilnahme aufgefordert. Ein Betroffener, der dazu an seiner Arbeitsstelle angerufen wurde, hat sich nicht nur darüber, sondern auch über den Umgang mit ihm bei der Abgabe seiner Speichelprobe beschwert. Insbesondere hat ihn beunruhigt, dass die brandenburgische Polizeibehörde ihm auf seine Nachfrage fälschlicherweise mitgeteilt hat, die DNA-Analysedaten seiner Speichelprobe würden nach Abschluss der Ermittlungen nicht gelöscht, sondern dauerhaft aufbewahrt.

Für ein DNA-Massenscreening und die erkennungsdienstliche Behandlung aller Teilnehmer gibt es keine gesetzliche Grundlage. Die Teilnahme ist freiwillig. Gemäß § 4 Abs. 1 Buchst. b Brandenburgisches Datenschutzgesetz (BbgDSG) ist eine Verarbeitung personenbezogener Daten ohne gesetzliche Grundlage nur zulässig, wenn der Betroffene ohne jeden Zweifel aus freien Stücken in die Maßnahme eingewilligt hat. Vorher muss er in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über die Empfänger der Daten sowie den Zweck der Übermittlung aufgeklärt werden (§ 4 Abs. 2 BbgDSG). Die Einwilligung ist schriftlich zu erteilen.

Wer sich nicht an einem DNA-Massenscreening beteiligt, dem dürfen überdies keine Nachteile entstehen. Zwar wird die Polizei ihn zu den Gründen

seines Verhaltens befragen, sie darf ihn nach der Rechtssprechung des Bundesverfassungsgerichts[41] aber auch dann nicht als Verdächtigen behandeln. In einem Rechtsstaat ist niemand verpflichtet, sich selbst zu belasten.

Im vorliegenden Fall waren die Betroffenen nicht nur ungenügend, sondern auch falsch aufgeklärt worden. Der Petent wäre darüber zu informieren gewesen, dass seine Identdaten zusammen mit den Fingerabdrücken und den Fotos aus der erkennungsdienstlichen Behandlung sowie die bei ihm entnommene Speichelprobe an die Staatsanwaltschaft Leipzig übersandt werden. Weiterhin hätte ihm mitgeteilt werden müssen, dass die Speichelprobe in einem wissenschaftlichen Institut analysiert wird, nachdem sie zuerst anonymisiert und mit einem Barcode gekennzeichnet worden ist und dass sie nach der Analyse vernichtet wird. Insbesondere hätte der Petent aber erfahren müssen, dass die DNA-Analysedaten nur für das in Rede stehende Ermittlungsverfahren genutzt und – soweit sich der Betroffene nicht als Täter herausstellt – vernichtet werden, wenn der Doppelmord aufgeklärt worden ist oder wenn sich herausstellt, dass die durch das Massenscreening erhobenen Daten zur Tataufklärung nicht oder nicht mehr erforderlich sind.

Außerdem sollten die Probanden wegen der Komplexität des Verfahrens nicht nur mündlich, sondern schriftlich über den weiteren Umgang mit den in Rede stehenden Daten aufgeklärt werden.

Das zuständige Polizeipräsidium hat sich bisher zu dem Fall noch nicht geäußert.

Die Teilnahme an DNA-Massenscreenings einschließlich erkennungsdienstlicher Behandlung ist mangels einer gesetzlichen Regelung in jedem Fall freiwillig. Auch wenn Anhaltspunkte dafür vorliegen, dass sich der Täter in der Masse der Teilnehmer befindet, ist der einzelne Proband unverdächtig. Daher können die DNA-Analysedaten nur bis zum Abschluss des Vergleichs mit den am Tatort aufgefundenen Spuren aufbewahrt werden. Wegen der Komplexität des Verfahrens sollten die Probanden nicht nur mündlich, sondern durch ein Merkblatt aufgeklärt werden.

Das DNA-Massenscreening auf freiwilliger Basis darf die Unschuldsvermutung nicht unterlaufen.

[41] vgl. NJW 1996, S. 3071 f.

4.1.7 Kooperation zwischen Polizei und Interventionsstellen in Fällen häuslicher Gewalt

Gewalttätigkeiten innerhalb von Partnerschaften oder Familien können von der zu Hilfe gerufenen Polizei häufig nur vorübergehend beendet werden. In einigen Bundesländern haben sich sog. Interventionsstellen auf privater Basis gebildet, die von der Polizei über alle dort bekannt gewordenen Vorfälle häuslicher Gewalt informiert werden, damit sie den Betroffenen ihre Hilfe anbieten können. Auch in Brandenburg gab es Überlegungen, eine solche Kooperation zwischen Polizei und Interventionsstellen einzurichten.

Zwar können nach § 44 Abs. 1 Nr. 2 Brandenburgisches Polizeigesetz personenbezogene Daten auch an nicht öffentliche Stellen übermittelt werden. Die Befugnis ist aber auf den konkreten Einzelfall beschränkt. Eine Übermittlungsbefugnis für alle Fälle von häuslicher Gewalt lässt sich aus der Vorschrift nicht ableiten.

Die Polizei könnte somit eine Interventionsstelle hier nur einschalten, wenn zumindest einer der Betroffenen seine Einwilligung zur Weitergabe seiner personenbezogenen Daten schriftlich erteilen würde. Nach § 4 BbgDSG setzt eine rechtsgültige Einwilligung voraus, dass der Betroffene vorher auf die Freiwilligkeit seiner Zustimmung hingewiesen und umfassend über den Empfänger – also die Interventionsstelle – und den Verwendungszweck der Daten informiert wird.

Wenn die Polizei in den Fällen, in denen sie Gewalttätigkeiten innerhalb von Familien oder Partnerschaften beendet hat, eine private Interventionsstelle über den Vorfall informieren soll, kann die Datenweitergabe nur mit Zustimmung zumindest eines der Betroffenen erfolgen.

4.2 Verfassungsschutz

4.2.1 Worüber der Verfassungsschutz dem Betroffenen Auskunft erteilen muss – was er verschweigen darf

Obwohl die Landesverfassung den Bürgerinnen und Bürgern ein umfassendes Auskunfts- bzw. Einsichtsrecht gegenüber brandenburgischen Behörden über zu ihrer Person gespeicherte Daten garantiert, müssen Betroffene gelegentlich feststellen, dass sie vom Verfassungsschutz keine vollständige Auskunft über alle dort erfassten Erkenntnisse erhalten. Zuweilen wird ihnen auch das Recht abgesprochen, eine Vertrauensperson mit der Einsichtnahme zu beauftragen. In solchen Fällen werden die

Antragsteller – wie im Brandenburgischen Verfassungsschutzgesetz vorgeschrieben – an uns verwiesen.

Das Auskunfts- und Akteneinsichtsrecht der Betroffenen ist in § 12 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG) geregelt. In der Vorschrift wird klargestellt, dass es auch bei der Verfassungsschutzbehörde keine ihrem Wesen nach grundsätzlich geheimhaltungsbedürftigen Informationen gibt, sondern die Auskunfts- bzw. Einsichtsgewährung immer in Abwägung des Einzelfalls gehandhabt werden muss. Die Auskunft oder Einsicht kann nur verweigert werden, wenn ein überwiegendes öffentliches Interesse an der Geheimhaltung der Erkenntnisse oder der nachrichtendienstlichen Arbeitsmethoden und Mittel besteht oder wenn die Verweigerung im überwiegenden Interesse eines Dritten geboten ist.

Vom Informationszugang ausgeschlossen werden können demnach Angaben über nachrichtendienstliche Arbeitsmethoden einschließlich V-Personen, mit denen die Verfassungsschutzbehörde die Informationen über einen Betroffenen gesammelt hat. Sie kann die Auskunft auch über ansonsten nicht geheimhaltungsbedürftige Sachverhalte verweigern, wenn dem Betroffenen damit zugleich auch bekannt würde, dass eine V-Person aus seinem Umfeld berichtet. Abgesehen von den Fällen, in denen das Interesse der Allgemeinheit oder eines Dritten überwiegt, ist aber über alle anderen Erkenntnisse Auskunft zu erteilen. Selbst bei Verdacht, dass die Arbeitsmethoden der Verfassungsschutzbehörde mittels einer koordinierten Aktion zur Auskunftsbeantragung ausgeforscht werden sollen, kann eine Verweigerung nicht allein mit dem Hinweis auf solch eine Aktion begründet werden. Dazu müssten vielmehr weitere Anhaltspunkte für einen entsprechenden Verdacht bei dem einzelnen Antragsteller selbst vorliegen.

Weitere Beschränkungen des Auskunftsrechts ergeben sich aus dem Zuständigkeitsprinzip. Die Verfassungsschutzbehörde kann nur über die von ihr selbst erhobenen und gespeicherten Erkenntnisse verfügen und Auskunft erteilen. Das gilt auch für die im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder (NADIS) gespeicherten Daten. Erkenntnismeldungen und Datenspeicherungen anderer Landesämter bzw. des Bundesamtes für Verfassungsschutz einschließlich der Tatsache, dass sie vorliegen, oder Mitteilungen anderer Stellen unterliegen nicht der Verfügungsbefugnis des brandenburgischen Verfassungsschutzes, sodass er dem Betroffenen darüber nur Auskunft erteilen darf, wenn und soweit diese Stellen zugestimmt haben.

Bei vollständiger oder teilweiser Ablehnung eines Auskunfts- bzw. Einsichtsantrags muss der Betroffene gem. § 12 Abs. 3 BbgVerfSchG darauf hinge-

wiesen werden, dass er sich an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wenden kann.

Das Auskunfts-/Einsichtsrecht ist nicht in der Form „personengebunden“, dass es nur vom Betroffenen selbst ausgeübt werden kann. Eine solche Einschränkung lässt sich aus dem Recht auf informationelle Selbstbestimmung nicht ableiten, das dem Betroffenen schließlich nicht auferlegt, ihn betreffende Informationen vor Dritten geheim zu halten, sondern ihm vielmehr die Verfügungsbefugnis über „seine Daten“ zuspricht. Die Verfassungsschutzbehörde kann ihm seine Entscheidung, einen Rechtsanwalt oder eine andere Person seines Vertrauens zu der ihm gewährten Akteneinsicht hinzuzuziehen und damit ggf. nachteilige Informationen über sich preiszugeben, auch aus Fürsorgegründen nicht abnehmen. Jeder hat das Recht, sich in Rechtsangelegenheiten aller Art durch einen Rechtsanwalt seiner Wahl beraten und vor Behörden vertreten zu lassen. Dies gilt auch bei der Wahrnehmung des Auskunfts- bzw. Akteneinsichtsrechts beim Verfassungsschutz.

Trotz des in Art. 11 der Brandenburgische Verfassung garantierten umfassenden Auskunfts- bzw. Akteneinsichtsrechts kann die brandenburgische Verfassungsschutzbehörde Betroffenen die Auskunft über die zu ihrer Person erfassten Erkenntnisse im Einzelfall ganz oder teilweise verweigern. Auf der anderen Seite gibt es beim Verfassungsschutz keine ihrem Wesen nach grundsätzlich geheimhaltungsbedürftigen Informationen. Der Betroffene kann einen Rechtsanwalt mit der Wahrnehmung seines Auskunfts- bzw. Akteneinsichtsrechts beim Verfassungsschutz beauftragen und sich dort von ihm vertreten lassen. Er kann auch eine Person seines Vertrauens hinzuziehen.

4.2.2 Wer muss dem Verfassungsschutz auf welchem Weg Hinweise geben?

Die brandenburgische Verfassungsschutzbehörde hatte die obersten Landesbehörden entsprechend dem Gesetz zur Umsetzung des Terrorismusbekämpfungsgesetzes und zur Stärkung der parlamentarischen Kontrolle[42] aufgefordert, die nachgeordneten Stellen ihres Zuständigkeitsbereichs darauf hinzuweisen, dass sie nunmehr verpflichtet seien, dem Verfassungsschutz von sich aus verfassungsschutzrelevante Tatsachen personenbezogen mitzuteilen. Offensichtlich ohne zu prüfen, ob alle nachgeordneten Stellen ihres Geschäftsbereichs gleichermaßen der Vorschrift unterliegen, haben mehrere Ministerien das an sie gerichtete Schreiben darauf hin unverändert weitergeleitet. Der Verfassungsschutz hatte in seinem Rundschreiben Mitteilungen von Behörden auf dem Postweg, per Fax oder E-Mail erbeten. Er wies dabei darauf hin, dass

[42] vgl. Tätigkeitsbericht 2002, A 1.2

eine auf dem Postweg gemachte schriftliche Mitteilung in einem verschlossenen Umschlag zu versenden sei. Verschiedene Landesbehörden wie z. B. das Landessozialgericht, einige Landkreise und Kommunen haben bei uns angefragt, ob die Übermittlungsverpflichtung für sie gelte und wie zu verfahren sei, falls solche Sachverhalte bekannt würden.

Seit 2002 sind die „Behörden, Betriebe, Einrichtungen des Landes sowie die der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts in Brandenburg“ verpflichtet, dem Verfassungsschutz unaufgefordert ihnen bekannt gewordene Tatsachen einschließlich personenbezogener Daten mitzuteilen, die sicherheitsgefährdende oder Spionagetätigkeiten oder gewaltgeneigte Bestrebungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG) bezeichneten Schutzgüter der Verfassung erkennen lassen (§ 14 Abs. 1 BbgVerfSchG).

Die ordentlichen Gerichte sowie die Verwaltungsgerichte einschließlich der Sozialgerichte gehören nicht zu den Normadressaten des § 14 Abs. 1 BbgVerfSchG. Dies ergibt sich auch schon aus dem Schreiben der Verfassungsschutzbehörde, das den Empfängerkreis auf die Stellen nach dem Landesorganisationsgesetz beschränkt.

Entscheidend sind die für die Gerichte maßgeblichen Übermittlungsvorschriften. Gemäß §§ 12 bis 18 Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG), dürfen Gerichte der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften von Amts wegen personenbezogene Daten unter bestimmten Voraussetzungen zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben übermitteln. Der Umfang der abschließend aufgezählten Übermittlungstatbestände macht deutlich, dass damit alle beim Gericht vorliegenden Erkenntnisse und Sachverhalte gemeint sind.

Da das Sozialgerichtsgesetz keine Datenverarbeitungsvorschriften enthält und der Anwendungsbereich des § 12 EGGVG bei der Schaffung des Justizmitteilungsgesetzes auch nicht auf die Sozialgerichtsbarkeit erstreckt wurde, ist davon auszugehen, dass der Gesetzgeber den Sozialgerichten, wenn überhaupt, nur sehr eingeschränkt Übermittlungsbefugnisse zugestehen wollte. Als Rechtsgrundlage kommen hier nur die Regelungen des Brandenburgischen Datenschutzgesetzes in § 14 Abs. 1 i. V. m. § 13 Abs. 2 Satz 1 Buchst. d BbgDSG in Betracht.

Eine uneingeschränkte Befugnis – oder gar Verpflichtung – der ordentlichen Gerichte oder der Sozialgerichtsbarkeit zu Initiativübermittlungen für Zwecke des Verfassungsschutzes kann weder dem Brandenburgischen Verfassungsschutzgesetz noch dem Datenschutzgesetz entnommen werden.

Beschränkungen der Übermittlungsbefugnis bestehen auch bei den Kommunen und Landkreisen. Hier ist zu beachten, dass durch die Vorschrift nicht nur keine Verpflichtung der Kommunen zu Initiativübermittlungen besteht, sondern die Ämter, die dem Sozialgeheimnis unterliegen, dazu auch keine Befugnis haben. Zur Wahrung des Sozialgeheimnisses sind die Übermittlungsbefugnisse der Sozialbehörden einschließlich der Jugendämter in Sozialgesetzbuch Zehntes Buch (SGB X) abschließend geregelt. § 72 enthält lediglich eine Übermittlungsbefugnis bei Ersuchen der Verfassungsschutzbehörde im Einzelfall sowie die abschließende Aufzählung der zu übermittelnden Daten. Für die Jugendämter besteht auch diese Übermittlungsbefugnis nicht.

Aber auch das Rundschreiben des Verfassungsschutzes selbst weist gravierende datenschutzrechtliche Mängel auf. Es zeugt zudem von einem erheblichen Mangel an Professionalität, wenn ein Nachrichtendienst zur Mitteilung von Hinweisen per Post, Fax oder E-Mail auffordert und nur bei Mitteilungen auf dem Postweg auf die Notwendigkeit eines „verschlossenen Umschlags“ hinweist. Personenbezogene Hinweise, die unverschlüsselt per E-Mail gegeben werden, können nicht nur von beliebigen Dritten mitgelesen, sondern auch unbemerkt verändert werden. Eine Verschlüsselungsmöglichkeit bietet die Verfassungsschutzbehörde nicht an. Auch Telefaxe können von Unbefugten eingesehen werden oder durch Fehlbedienung des Absendegeräts leicht irrtümlich beim falschen Empfänger landen. Um die Rechte der Betroffenen (einschließlich der Hinweisgeber) angemessen zu wahren, kann die Übermittlung nur in einem verschlossenen Umschlag mittels Behörden- oder regulärer Post erfolgen.

Die um Stellungnahme gebetenen Ministerien haben bisher auf unsere Hinweise ebenso wenig reagiert wie die zur Abänderung und Ergänzung ihres Schreibens aufgeforderte Verfassungsschutzbehörde.

Gerichte sind nicht zu Initiativübermittlungen an die Verfassungsschutzbehörde verpflichtet. Ämter, die wie Sozial- und Jugendämter dem Sozialgeheimnis unterliegen, haben keine Befugnis zu solchen Übermittlungen. Sie dürfen der Verfassungsschutzbehörde nicht von sich aus verfassungsschutzrelevante Erkenntnisse mitteilen.

Wenn ein Nachrichtendienst andere Behörden zur Übermittlung personenbezogener Hinweise per unverschlüsselter E-Mail oder Fax auffordert, lässt er damit nicht nur einen Mangel an Professionalität erkennen, sondern er nimmt damit auch die Verletzung datenschutzrechtlicher Bestimmungen in Kauf.

4.3 Meldewesen

4.3.1 Meldewesen im Internet-Zeitalter

Das Ministerium des Innern plant, das Meldewesen in Brandenburg mit dem E-Government-Projekt „G2x-Communications im Meldewesen“ unter Nutzung moderner Informations- und Kommunikationstechnologien wirtschaftlicher und serviceorientierter zu organisieren. Ziel ist, unter Beibehaltung der dezentralen Organisation des Meldewesens den Datenaustausch der Meldebehörden untereinander und mit anderen Behörden zu beschleunigen und zu vereinfachen, die Melderegister rund um die Uhr verfügbar zu halten und den rechtlich zulässigen Zugang zu den Melderegistern für Private über das Internet zu erleichtern.

Im Einzelnen besteht das Projekt im Wesentlichen aus drei Komponenten.

- Ab 1. Januar 2005 soll auch bei Umzügen aus oder in andere Bundesländer die Pflicht wegfallen, sich bei der Meldebehörde des bisherigen Wohnortes abzumelden. Dafür soll ein bundesweites elektronisches Rückmeldeverfahren eingeführt werden, das bei der Anmeldung am neuen Wohnort die Abmeldung am bisherigen Wohnort sicherstellt.

- Öffentliche Stellen, die – entweder regelmäßig oder im Einzelfall zur Erfüllung ihrer Aufgaben – befugt sind, Daten aus den Melderegistern zu erhalten, sollen die Möglichkeit bekommen, die erforderlichen Daten elektronisch abzurufen.

- Die jedermann zustehende Möglichkeit, ohne Angabe von Gründen eine einfache Melderegisterauskunft (Name, Vorname, derzeitige Anschrift und Doktorgrad) zu bekommen, soll in Zukunft ebenfalls auf elektronischem Wege eröffnet werden.

Die rechtlichen Voraussetzungen für das Vorhaben sind – unabhängig von diesem Projekt – bereits vorhanden oder werden derzeit geschaffen.[43] Angesichts der heterogenen technischen Ausstattung der etwa 200 Meldebehörden im Land ist zunächst vorgesehen, für das gesamte Land Brandenburg beim Landesbetrieb für Datenverarbeitung und Statistik eine Stelle einzurichten, die die genannten Aufgaben übernimmt. Dort soll ein tagesaktueller Auskunfts- und Übermittlungsdatenbestand in dem bundesweit verbindlichen Datenformat XMeld vorgehalten werden, der auf täglichen Zulieferungen aller Meldebehörden des Landes basiert. Dieser Datenbestand enthält die Mehrzahl der bei den Meldebehörden gespeicherten Daten. Im Rahmen der elekt-

[43] vgl. Tätigkeitsbericht 2000, A 4.4.1

ronischen Rückmeldung soll der Landesbetrieb für Datenverarbeitung und Statistik die Daten nach dem Übermittlungsstandard OSCI (Online Services Computer Interface) in die anderen Bundesländer übermitteln und von dort die Daten der aus Brandenburg weggezogenen Personen erhalten. Für die Übermittlung an öffentliche Stellen und die elektronische einfache Melderegisterauskunft soll der Datenbestand rund um die Uhr zum Abruf zur Verfügung stehen. Das Projekt „Zentrales elektronisches Melderegister (MDIS)“ geht vollständig darin auf und wird nicht weiterverfolgt.[44]

Aus datenschutzrechtlicher Sicht wird es darauf ankommen, das bisher gegebene Datenschutzniveau mindestens aufrecht zu erhalten und Potenziale zur Verbesserung der Datensicherheit zu nutzen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist an der vom Ministerium des Innern eingesetzten Arbeitsgruppe beteiligt und kann damit frühzeitig datenschutzrechtliche Belange bei der Umsetzung des Projekts einbringen.

Entscheidend ist, dass trotz der zentralen Einbindung des Landesbetriebs für Datenverarbeitung und Statistik die vom Brandenburgischen Meldegesetz vorgeschriebene Zuständigkeitsordnung erhalten bleibt und technisch abgebildet wird. Meldebehörden sind danach unverändert die Ämter, amtsfreien Gemeinden und kreisfreien Städte. Nach den geplanten Vorschriften soll der Landesbetrieb für Datenverarbeitung und Statistik lediglich Weiterleitungs- und Verteilaufgaben wahrnehmen. Die Speicherung des Auskunfts- und Übermittlungsdatenbestandes wird nur als Datenverarbeitung im Auftrag möglich sein. Die einzelne Meldebehörde muss nach außen für die ordnungsgemäße Datenverarbeitung verantwortlich bleiben. Eine Vermischung der einzelnen Melderegister zu einem zentralen Landesmelderegister darf es nicht geben. Die einzelnen Melderegister sind daher logisch getrennt zu speichern.

Um die Risiken eines elektronischen Abrufs durch Private per Internet bei der einfachen Melderegisterauskunft zu begrenzen, werden die Einwohnerinnen und Einwohner die Möglichkeit haben, dieser Form der Melderegisterauskunft zu widersprechen. Die Meldebehörden werden gesetzlich verpflichtet, regelmäßig über das Widerspruchsrecht zu informieren.

[44] vgl. Tätigkeitsbericht 2002, A 4.4

Das E-Government-Projekt „G2x-Communications im Meldewesen“ bietet gute Voraussetzungen, einen hohen landeseinheitlichen Standard an Datensicherheit zu gewährleisten. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird darauf achten, dass kein zentrales landesweites Melderegister entsteht. Die Bürgerinnen und Bürger haben das Recht, der Melderegisterauskunft über das Internet zu widersprechen.

4.3.2 Die Polizei greift nach dem Meldewesen

Der Minister des Innern hat sein Ministerium zum 1. August 2003 umfassend umstrukturiert. In erster Linie wird damit das Ziel verfolgt, die strategischen Aufgaben des Ministeriums vor allem im Hinblick auf Verwaltungsmodernisierung und E-Government stärker in den Vordergrund zu stellen. Im Zuge dessen wurden unter anderem die Zuständigkeiten für das Melde-, Pass- und Ausweiswesens der in erster Linie für die Polizei zuständigen Abteilung des Ministeriums übertragen.

Aus dieser Organisationsentscheidung des Ministers erwachsen aus unserer Sicht Gefahren für das Recht auf informationelle Selbstbestimmung. Die datenschutzrechtlich gebotene Trennung zwischen den Aufgaben der Polizei einerseits und denen des Meldewesens andererseits wird an dieser Stelle aufgeweicht.

In Brandenburg sind – wie auch in allen anderen Ländern – die Aufgaben des Meldewesens sowohl funktionell als auch organisatorisch von denen der Polizei getrennt. Während Meldebehörden jeweils die örtlichen Ordnungsbehörden (kreisfreie Städte, Ämter und amtsfreie Gemeinden) sind, werden die Aufgaben der Polizei durch spezielle Landesbehörden wahrgenommen. Diese getrennte Aufgabenzuweisung wird durch die Umstrukturierung des Ministeriums des Innern nicht infrage gestellt. Sie ist auch datenschutzrechtlich geboten, weil damit die Zweckbindung der unterschiedlichen Aufgaben dienenden personenbezogenen Daten gewährleistet werden kann.

Das Ministerium des Innern ist jedoch die oberste Aufsichtsbehörde im Meldewesen. Als solche stehen dem Ministerium bestimmte Weisungsbefugnisse zu. Das Ministerium übt seine Weisungsbefugnis in der Praxis insbesondere in Form von Rundschreiben aus. Vor dem Hintergrund der Aufsichtsbefugnisse des Ministeriums des Innern im Bereich des Meldewesens erscheint die organisatorische Einordnung in die Polizeiabteilung aus datenschutzrechtlicher Sicht bedenklich. Grundsätzlich liegt es in der Organisationshoheit des Ministers, welche Organisationseinheit innerhalb des Ministeriums bestimmte Aufgaben wahrnimmt. Auch sind insofern keine unmittelbaren datenschutzrechtlichen Auswirkungen zu besorgen, als das Ministerium als oberste Auf-

sichtsbehörde regelmäßig nicht mit personenbezogenen Daten Einzelner umgeht.

Die Tatsache, dass die Meldebehörden über eine Reihe von personenbezogenen Daten aller Einwohner verfügen und sie diese als Informationsplattform für eine moderne, multifunktionale Verwendung bereithalten, gibt ihnen im Hinblick auf das Recht auf informationelle Selbstbestimmung eine einzigartige Stellung gegenüber allen anderen Behörden. Dieser gewandelten Funktion des modernen Meldewesens widerspricht es, wenn die Aufsicht praktisch von der Polizeiabteilung des Ministeriums des Innern ausgeübt wird.

Es ist daher aus unserer Sicht bedenklich, wenn der Konflikt zwischen den Sicherheitsaufgaben der Polizei und dem Recht auf informationelle Selbstbestimmung innerhalb der gleichen Abteilung einer Behörde gelöst werden muss. Dies gilt auch für die Aufsichtsbehörde, wenn Weisungsbefugnisse von identischen Personen ausgeübt oder ihre Ausübung durch den Minister vorbereitet werden.

Das Ministerium des Innern hat unsere Bedenken geprüft, teilt sie jedoch nicht.

Eine organisatorische Verknüpfung von Aufgaben des Meldewesens mit denen der Polizei ist im Hinblick auf das Recht auf informationelle Selbstbestimmung angesichts der einzigartigen Stellung der Meldebehörden bedenklich. Das Ministerium des Innern sollte diese Bedenken ernst nehmen und auch auf der Ebene der Aufsicht für eine klare organisatorische Trennung sorgen.

4.3.3 Brandenburger Wahlen jetzt mit Internethilfe

Durch Änderungen im Landeswahlrecht[45] war es bei der Kommunalwahl 2003 im Land Brandenburg erstmals möglich, auch bei Wahlen auf der Landesebene den Wahlschein über das Internet zu beantragen.

Bereits bei der Bundestagswahl 2002 wurde diese Möglichkeit angeboten. Im Vorfeld der Änderung der Landeswahlvorschriften setzte sich das Ministerium des Inneren des Landes Brandenburg mit uns in Verbindung, um eine datenschutzgerechte Durchführung der Internetnutzung bei der Wahlscheinbeantragung sicherzustellen. Im Ergebnis dieser Abstimmung erstellte das Ministerium des Inneren ein Rundschreiben an die Kommunen, in dem zum einen

[45] Verordnung über den Wahltag und die Wahlzeit der landesweiten Kommunalwahlen 2003 sowie zur Änderung der Brandenburgischen Kommunalwahlverordnung v. 25. März 2003, GVBl. II, S. 162

auf die Möglichkeit der Bürger hingewiesen wurde, den Wahlscheinantrag auszudrucken, um ihn wie herkömmlich auf dem Postweg zu versenden. Zum anderen sollte sichergestellt werden, dass bei einer unverschlüsselten Onlineübertragung des Antrags – dies stellt die übliche Methode dar – der Bürger auf die „unsichere“ Datenübertragung deutlich aufmerksamgemacht wird und ein Hinweis auf die alternative postalische Übermittlung erfolgt.

Wie die Rückmeldungen aus einer Vielzahl von Kommunen belegt, wurden die datenschutzrechtlichen Hinweise dort aufgenommen und entsprechend in den Internetangeboten umgesetzt. Nicht bekannt ist leider bislang, in welchem Umfang die Bürger von der Möglichkeit der Wahlscheinbeantragung per Internet Gebrauch gemacht haben.

Wahlscheine für brandenburgische Wahlen können in datenschutzgerechter Weise auch per Internet beantragt werden.

4.4 Personaldaten

4.4.1 Was folgt aus „Rosenholz“?

Nachdem die Regierung der Vereinigten Staaten alle sog. „Rosenholz“-Unterlagen des Ministeriums für Staatssicherheit, die in der Wendezeit auf nicht bekanntem Wege in die USA gelangt waren, der Bundesregierung übergeben und die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes mit ihrer Entschlüsselung begonnen hatten, fasste der Bundesrat auf Antrag der Länder Thüringen, Sachsen und Sachsen-Anhalt und mit den Stimmen des Landes Brandenburg eine Entschließung zur weiteren Auswertung dieser jetzt zugänglichen Informationen[46]. Darin forderte er Bund und Länder auf, die mit der Freigabe der „Rosenholz“-Dateien gewonnenen neuen Erkenntnisse zu nutzen, um weiteren Aufschluss über eine mögliche Tätigkeit von öffentlichen Bediensteten für den Staatssicherheitsdienst der ehemaligen DDR zu erhalten. Die Parlamentarier von Bund und Ländern wurden aufgerufen, sich ebenfalls einer solchen Überprüfung zu unterziehen.

Die Landesregierung beschloss gleichzeitig, dass sich alle Landesminister einer erneuten Überprüfung bei der Bundesbeauftragten unterziehen sollten; diese ergab keinerlei Hinweise auf eine Zusammenarbeit mit dem Ministerium für Staatssicherheit.

Im Zusammenhang mit der Entschließung des Bundesrates wurde in der Öffentlichkeit die Forderung erhoben, dass sich auch sämtliche Landesbediens-

[46] s. BR-Drs. 668/03 (Beschluss)

teten einer erneuten Überprüfung durch die Bundesbeauftragte für die Stasi-Unterlagen unterziehen sollten. Der Landesbeauftragte hat daraufhin dem Ministerpräsidenten, dem Minister des Innern und der Ministerin der Justiz und für Europaangelegenheiten mitgeteilt, dass er eine flächendeckende, anlassunabhängige Überprüfung aller Bediensteten des Landes oder auch derjenigen, die aus den alten Bundesländern stammen, für unverhältnismäßig hält. Er hat zugleich auf die Verpflichtung der Bundesbeauftragten für die Stasi-Unterlagen hingewiesen, von sich aus ohne Ersuchen unter bestimmten Voraussetzungen öffentliche Stellen über eine hauptamtliche oder inoffizielle Tätigkeit für den Staatssicherheitsdienst zu informieren, wenn ihr neue Erkenntnisse vorliegen. In jedem Fall sollten die Voraussetzungen einer Überprüfung von Landesbediensteten durch Anfrage bei der Bundesbeauftragten in einheitlichen Richtlinien festgelegt werden, die eine divergierende Praxis der einzelnen Ministerien in diesem schwierigen Bereich ausschließt. Der Landesbeauftragte hat angeboten, die Landesregierung bei der Ausarbeitung entsprechender Richtlinien zu beraten.

Dieses Angebot ist von der Landesregierung positiv aufgenommen wurden, allerdings war ihre Meinungsbildung in der Sache gegen Ende des Berichtszeitraumes noch nicht abgeschlossen.

Eine flächendeckende, anlassunabhängige Überprüfung aller Bediensteten des Landes oder aller aus den alten Bundesländern stammenden Bediensteten auf Grund der jetzt zugänglichen „Rosenholz“-Daten wäre unverhältnismäßig. In jedem Fall sollten die Voraussetzungen einer zukünftigen Überprüfung durch landeseinheitliche Richtlinien festgelegt werden.

4.4.2 Personalauswahlverfahren bei der Polizei

Das Ministerium des Innern hat im Rahmen seiner Polizeistrukturreform Personalauswahlverfahren im höheren Polizeidienst durchgeführt. Dabei kam das psychologische Testverfahren einer in Österreich ansässigen Firma zur Anwendung.

Zur Vorbereitung des Testverfahrens wurden der Firma seitens des Ministeriums des Innern die Namen der betroffenen Beamten, die Amtsbezeichnung und die jeweilige Dienststelle übermittelt. Dabei meinte das Ministerium, dass es genüge, mit der Firma einen Nutzungsvertrag zu schließen, in welchem sie sich verpflichtet, bei den ihr überlassenen Daten die Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) einzuhalten.

Anfangs war unklar, ob die Durchführung rechtlich als Datenverarbeitung im Auftrag i. S. v. § 11 BbgDSG zu qualifizieren war. Das Ministerium war der Ansicht, lediglich einen Teilbereich des weit umfangreicheren Auswahlverfah-

rens und nicht etwa die eigene Entscheidungen auf Dritte delegiert zu haben und betrachtete den Vorgang deshalb nicht schon als Datenverarbeitung im Auftrag. Tatsächlich sind jedoch deren Merkmale vollständig erfüllt. § 11 BbgDSG setzt nämlich voraus, dass die Verantwortung für das gesamte Auswahlverfahren bei der Auftrag gebenden Stelle verbleibt und die Firma lediglich untergeordnete Hilfsaufgaben bei der Verarbeitung personenbezogener Daten durchführt. Würde hingegen die Firma Personalentscheidungen hinsichtlich des Auswahlverfahrens treffen, so hätte es sich um eine Funktionsübertragung gehandelt, die jedenfalls mangels besonderer gesetzlicher Ermächtigungsgrundlage hier unzulässig wäre[47]. Der Dienstherr darf aber im Rahmen seiner eigenen Beurteilung unterstützend einen psychologischen Eignungstest heranziehen.

Der uns vorgelegte Nutzungsvertrag erfüllt nicht die Anforderungen an einen Mindestvertragsinhalt für eine Datenverarbeitung im Auftrag und bedarf daher der Nachbesserung. Das Ministerium des Innern sagte dies bereits seit zwei Jahren zu, ohne dass uns bisher ein geänderter Vertrag zugeleitet worden wäre.

Im Innenministerium haben wir festgestellt, dass die Ergebnisberichte der im März 2002 durchgeführten Tests aufbewahrt werden. Diese Unterlagen befinden sich für jeden Betroffenen in verschlossenen Umschlägen. Diese wiederum wurden alphabetisch geordnet in Ringordnern abgelegt und in einem Stahlschrank verschlossen. Auf jedem der Ringordner ist die Löschungsfrist (2005) vermerkt. Weil die Betroffenen erst nach Ablauf von drei Jahren erneut an einem Auswahlverfahren teilnehmen können, werden diese Ergebnisse bis zum Ablauf der drei Jahre aufbewahrt. Das Ministerium des Innern hat uns zugesagt, aus diesem Grund die Ergebnisberichte i. S. v. § 19 Abs. 2 BbgDSG zu sperren und auf jeden Umschlag einen entsprechenden Sperrvermerk aufzubringen.

Ist eine Personaldatenverarbeitung durch Dritte vorgesehen, kann dies nur auf der Grundlage des § 11 Brandenburgisches Datenschutzgesetz als Datenverarbeitung im Auftrag geschehen. Dem Schutz der Persönlichkeitsrechte von Mitarbeiterinnen und Mitarbeitern ist durch eine Vertragsgestaltung mit entsprechendem Mindestinhalt Rechnung zu tragen.

4.4.3 Auswertung dienstlicher Tätigkeit für Leistungskontrollen bei der Polizei

In verschiedenen Polizeidienststellen des Landes erfolgte eine Erfassung von Tätigkeiten der Beschäftigten auch, um sie zu Leistungsver-

[47] vgl. dazu oben A 1.2

gleichen zu nutzen. Beispielsweise wurde eine beschäftigtenbezogene Sonderauswertung der Effizienz von Geschwindigkeitskontrollen sowie eine Auswertung der eingenommen Verwarngelder der einzelnen Polizeibeamtinnen und Polizeibeamten vorgenommen.

Beschäftigtendaten dürfen nach § 29 Brandenburgisches Datenschutzgesetz (BbgDSG) nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Sowohl die personenbezogene Sonderauswertung der Radareffizienz als auch die der verhängten Verwarngelder kann in vielfacher Hinsicht erlaubt sein.

Zweifel hatten wir zwar, inwieweit die Verarbeitung dieser Daten (Anzahl der Blitzerfotos, Höhe der Verwarngelder) objektiv geeignet ist, einen Leistungsvergleich durchzuführen. Generell schließt der Gesetzgeber Leistungskontrollen aber nur für die Daten der Beschäftigten aus, die im Rahmen der Durchführung der technisch-organisatorischen Maßnahmen nach § 10 Abs. 2 BbgDSG gespeichert werden (vgl. § 29 Abs. 5 BbgDSG). Diese sind nur zur Sicherstellung des technischen Ablaufs, nicht aber für andere Zwecke bestimmt.

Die bei der Polizei praktizierten personenbezogenen Auswertungen können bspw. erforderlich sein, um den Personaleinsatz in einer Dienststelle besser zu organisieren. Unzulässig ist nur eine permanente und lückenlose Überwachung der Beschäftigten. Dies wäre mit dem Schutz der Persönlichkeit der Beschäftigten am Arbeitsplatz unvereinbar. Werden Daten von Arbeitnehmerinnen und Arbeitnehmern erhoben, die zur Leistungskontrolle geeignet sind, ist neben § 29 BbgDSG zusätzlich auch § 65 Brandenburgisches Personalvertretungsgesetz zu berücksichtigen, der ein Mitbestimmungsrecht des Personalrats vorsieht.

Beschäftigtendaten dürfen im Rahmen der Erforderlichkeit auch zu Verhaltens- und Leistungskontrollen verarbeitet werden. Die Mitbestimmungsrechte der Personalvertretung nach dem Brandenburgischen Personalvertretungsgesetz bleiben jedoch unberührt.

4.4.4 Einführung der Kosten- und Leistungsrechnung in der Landesverwaltung

Die von der Landesregierung beschlossene Einführung der Kosten- und Leistungsrechnung (KLR) als neues Steuerungsinstrument in Branden-

burg ist auch unter dem Blickwinkel des Personaldatenschutzes von erheblicher Bedeutung.

Das Ministerium der Finanzen hat uns von sich aus vor Beginn der pilothaften Einführung der KLR in das Projekt einbezogen und um eine datenschutzrechtliche Bewertung gebeten.

Ziel der KLR ist es, die Kosten der von der Verwaltung erbrachten Leistungen sowie die hierbei erwirtschafteten Erträge festzustellen. Damit soll Kostentransparenz für alle Beteiligten, aber auch Kostenverantwortung der Bediensteten erreicht werden. Da Personalkosten in diesem Zusammenhang ein wesentlicher Aspekt sind, geraten die Besoldungs- und Leistungsdaten der Bediensteten ins Blickfeld der KLR.

Folgende allgemeine Kriterien sind von Beginn an zu berücksichtigen, um einen Konflikt zwischen diesen neuen Analysemethoden und dem Personaldatenschutzrecht zu vermeiden.

- Vor der Einführung der KLR, bei der personenbezogene Daten verarbeitet werden, sind die damit verfolgten Zielsetzungen (Zwecke) eindeutig festzulegen.

- Der Personalrat ist zu beteiligen. Dienstvereinbarungen sollten die näheren Modalitäten der KLR regeln.

- Automatisierte Systeme im Rahmen von KLR sind vor ihrem Wirkbetrieb zu dokumentieren, zu testen und freizugeben. Es muss ein Sicherheitskonzept vorliegen.

- Daten, die im Rahmen von KLR verarbeitet werden sollen, sind, wenn möglich, bei den betroffenen Bediensteten zu erheben.

- Die Verarbeitung von Urlaubs- und Krankheitsdaten von Bediensteten in personenbeziehbarer Form ist ebenso unzulässig wie die Nutzung von KLR-Daten für Verhaltens- und Leistungskontrollen der Bediensteten.

- Alle erhobenen personenbezogenen Daten sind zum frühestmöglichen Zeitpunkt zu löschen oder zu anonymisieren.

- Eine Anonymisierung von Daten kann durch folgende Maßnahmen erfolgen: Zusammenfassung von Personalstellen zu größeren organisatorischen Einheiten, Aggregieren von Datensätzen, Löschen von Referenzlisten, Standardisierung arbeitsplatzbezogener Kosten- und Leistungsstellen.

- Die KLR ist in einer von der Personalstelle räumlich und organisatorisch getrennten Organisationseinheit zu bearbeiten.

- Die Mitarbeiter sollten rechtzeitig und umfassend über das neue Verfahren informiert werden.

Das Projekt „Kosten- und Leistungsrechnung“ wirft Fragen des Personaldatenschutzes auf, die sich aber lösen lassen, wenn unsere Hinweise berücksichtigt werden.

4.5 Statistik und Wahlen

Das Forschungsdatenzentrum der Statistischen Landesämter

Besonders Wirtschafts- und Sozialwissenschaftler fordern seit Jahren den Zugang zu sog. Mikrodaten der amtlichen Statistik, die noch nicht anonymisiert sind. Im Gutachten der vom Bundesministerium für Bildung und Forschung eingesetzten Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik „Wege zu einer besseren informationellen Infrastruktur“ wird unter anderem die Einrichtung von Forschungsdatenzentren empfohlen.

Zur Verbesserung der Handlungsgrundlagen für politische Entscheidungen sind aussagekräftige statistische Informationen zur Situation und Entwicklung von Wirtschaft und Gesellschaft von erheblicher Bedeutung. Um die statistischen Datenbestände für Wissenschaft und Forschung schneller und effektiver nutzbar machen zu können, soll ein Forschungsdatenzentrum der Statistischen Landesämter – in Brandenburg des Landesbetriebs für Datenverarbeitung und Statistik – eingerichtet werden. Dort sollen die Daten aller Landesämter zusammengeführt und für die Wissenschaft und Forschung zeitnah bereitgestellt werden.

Die Wissenschaftler sind besonders daran interessiert, aktuelle Mikrodaten für Forschungszwecke zu nutzen. Diese sind entweder gar nicht oder nur unzureichend anonymisiert und dürfen daher entsprechend dem Statistikgeheimnis nur von den Statistikämtern selbst verwendet werden. In § 16 Abs. 6 Bundesstatistikgesetz (BStatG) wird die Verwendung statistischer Einzelangaben zur Durchführung wissenschaftlicher Vorhaben geregelt. Danach dürfen Daten zur wissenschaftlichen Forschung übermittelt werden, wenn die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand Personen zugeordnet werden können (faktische Anonymisierung).

Aus datenschutzrechtlicher Sicht muss daher die Bereitstellung von Mikrodaten, die nicht den Anforderungen des § 16 BStatG genügen, abgelehnt wer-

den. Nach der derzeitigen Gesetzeslage können nur faktisch anonymisierte Daten zu Forschungszwecken bereitgestellt werden.

Diese Einschränkung sollte den Aufbau des Forschungsdatenzentrums der Statistischen Landesämter aber nicht blockieren. Auch die zentrale Bereitstellung aufbereiteten Datenmaterials ist geeignet, die Forschungsgrundlagen zu verbessern. Eine weiter gehende Öffnung des Statistikgeheimnisses zugunsten der Wissenschaft sollte der Gesetzgeber erst dann ins Auge fassen, wenn sich die bestehenden Möglichkeiten als unzureichend erwiesen haben.

Für die im Gutachten „Wege zu einer besseren informationellen Infrastruktur“ geforderte Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik können nur aufbereitete und anonymisierte Daten verwendet werden.

4.6. Kommunales

4.6.1 Privatdetektive auf Müllsuche

Ein Landrat in seiner Funktion als untere Abfallwirtschaftsbehörde hatte eine unkonventionelle Idee, die illegale Entsorgung von Abfällen zu unterbinden. Er beauftragte – zunächst in einem Pilotprojekt – eine private Detektei, jede Nutzung von Containerstandorten aus verdeckter Position mittels Videotechnik aufzuzeichnen. Die Aufzeichnungen wurden der Abfallbehörde übergeben und von ihr ausgewertet. Die Videoaufzeichnung verfolgte in erster Linie das Ziel, Beweismittel für die Verfolgung von Ordnungswidrigkeiten zu erhalten. Daneben sollte die Videoaufzeichnung auch dazu dienen, durch einen gewissen Abschreckungseffekt der illegalen Entsorgung von Abfällen vorzubeugen.

Nach eingehender datenschutzrechtlicher Prüfung haben wir festgestellt, dass das begrüßenswerte Ziel des Landrats nicht mit einer verdeckten Videoaufzeichnung durch Privatdetektive erreicht werden kann, weil es dafür keine rechtliche Grundlage gibt.

Die im Verfahren zur Verfolgung von Ordnungswidrigkeiten zum Teil anwendbare Strafprozessordnung (StPO) enthält in § 100c eine Befugnis zur Herstellung verdeckter Bildaufzeichnungen für den Fall, dass der Sachverhalt auf andere Weise weniger Erfolg versprechend oder nur erschwert festgestellt werden kann. Diese hoheitliche Befugnis steht nur der für die Verfolgung zuständigen Behörde zu und kann wegen einer fehlenden ausdrücklichen gesetzlichen Beleihung nicht auf Private übertragen werden.

Private Auftragnehmer dürfen nur als so genannte Verwaltungshelfer eingesetzt werden. Soweit sie personenbezogene Daten verarbeiten, ist dies im Rahmen einer Datenverarbeitung im Auftrag grundsätzlich zulässig. Ihre Tätigkeit muss sich jedoch auf untergeordnete Hilfstätigkeiten beschränken. Sie dürfen keinen eigenen Entscheidungsspielraum haben und müssen strikten Weisungen des Auftraggebers unterliegen.

Die verdeckte Videoaufzeichnung ist deshalb unzulässig, weil § 100c StPO eine Aufzeichnung jeder – also auch der rechtmäßigen – Benutzung nicht zulässt. Die Herstellung heimlicher Videoaufnahmen greift erheblich in die Persönlichkeitsrechte der betroffenen Personen ein und ist deshalb nur zulässig, wenn ein konkreter Anfangsverdacht besteht, dass jemand illegal Müll entsorgt. Personen, die sich ganz offenkundig legal verhalten, dürfen nicht aufgezeichnet werden. Den erforderlichen Anfangsverdacht kann nur die aufzeichnende Person feststellen. Eine solche Feststellung würde aber wiederum einen Entscheidungsspielraum der Detektive voraussetzen, den diese nach dem oben Gesagten nicht haben dürfen.

Im Ergebnis darf eine Privatdetektei nicht mit der Herstellung verdeckter Videoaufzeichnungen zur Verfolgung von Ordnungswidrigkeiten beauftragt werden. Diese Auffassung wird sowohl vom Ministerium der Justiz und für Europaangelegenheiten als nunmehr auch von der zuständigen obersten Abfallbehörde, dem Ministerium für Landwirtschaft, Umweltschutz und Raumordnung, geteilt.

Darüber hinaus weisen wir erneut darauf hin, dass die permanente Videoaufzeichnung der im öffentlichen Straßenland befindlichen Containerstellplätze zu Zwecken der Vorbeugung und Gefahrenabwehr ebenfalls unzulässig ist, weil die Videoüberwachung von Straßen und Plätzen ausschließlich der Polizei vorbehalten ist.[48]

Private Unternehmen dürfen im Auftrag von öffentlichen Stellen keine Videoaufzeichnungen herstellen, um damit Beweismittel für die Verfolgung von Ordnungswidrigkeiten zu erhalten. Die anlassunabhängige Videoüberwachung öffentlicher Straßen und Plätze ist ausschließlich der Polizei vorbehalten.

4.6.2 Zugang zu den eigenen Daten

In der Praxis bestehen nach unseren Erfahrungen gerade in den Kommunen Unsicherheiten, wenn Bürgerinnen und Bürger in bestimmten Si-

[48] vgl. Tätigkeitsbericht 2002, A 4.7.3; Tätigkeitsbericht 2001, A 1.5.2

tuationen Auskunft oder Akteneinsicht hinsichtlich ihrer eigenen personenbezogenen Daten begehren.

4.6.2.1 Wer hat mich angeschwärzt?

Häufig werden wir sowohl von Bürgern als auch von öffentlichen Stellen gefragt, ob die Verwaltung die Identität eines Informanten offenbaren darf. In einem Fall hatte jemand die Verwaltung darüber informiert, dass auf einem bestimmten Grundstück baurechtswidrige Zustände herrschten. In einem anderen beschwerte sich jemand bei der Verwaltung über Lärmbelästigungen, die von einem bestimmten Grundstück ausgingen. In beiden Fällen wollten die Grundstückseigentümer jeweils wissen, von wem die Hinweise kamen.

Das Brandenburgische Datenschutzgesetz (BbgDSG) garantiert in § 18 allen von der Verarbeitung ihrer personenbezogenen Daten Betroffenen das Recht, Auskunft über die zu ihrer Person gespeicherten Daten und über deren Herkunft zu erhalten. Soweit die Daten in Akten gespeichert sind, ist den Betroffenen auf Verlangen Akteneinsicht zu gewähren.

Die Identität eines Informanten oder Anzeigeerstatters gehört nicht nur zu dessen personenbezogenen Daten, sondern auch zu denen des Betroffenen. Wer wissen will, wer ihn bei einer Behörde angezeigt hat, will auch etwas über die Herkunft seiner eigenen Daten wissen. Insofern besteht hinsichtlich der Person eines Anzeigeerstatters oder Informanten ein Anspruch auf Auskunft und Akteneinsicht.

Wie bei jedem Antrag nach § 18 BbgDSG ist auch hier im Einzelfall zu prüfen, ob überwiegende berechtigte Interessen des Informanten der Auskunftserteilung bzw. Akteneinsicht entgegenstehen. Solche Interessen stehen ausnahmsweise dann entgegen, wenn der Hinweisgeber auf Grund der von ihm gegebenen Informationen mit erheblichen Nachteilen oder Repressalien rechnen muss oder wenn die Verwaltung zur Erfüllung ihrer Aufgaben auf anonyme Hinweise angewiesen ist. Dies ist beispielsweise bei bestimmten Kriminalitätsformen oder auch bei der Korruptionsbekämpfung der Fall.[49]

In ordnungsbehördlichen Verfahren, bei denen es um die Einhaltung ordnungsrechtlicher Vorschriften geht, haben Informanten dagegen in der Regel kein berechtigtes Interesse, anonym zu bleiben. Dies gilt auch dann, wenn der Hinweisgeber ausdrücklich anonym bleiben möchte. Ein Informant müsste in einem eventuellen Gerichtsverfahren ohnehin damit rechnen, als Zeuge seine Identität offenbaren zu müssen. Darauf sollte die Verwaltung Informanten hinweisen, die anonym bleiben wollen.

[49] vgl. dazu Urteil des BVerwG v. 27. Februar 2003, NJW 2003, S. 3217

Soweit keine besonderen Gründe vorliegen, die Identität eines Hinweisgebers geheim zu halten, ist dem Betroffenen darüber Auskunft zu erteilen oder Akteneinsicht zu gewähren.

4.6.2.2 Zugang zu internen Unterlagen

Zur Entscheidung über das Bauvorhaben eines Bürgers musste von der betroffenen Gemeinde das Einvernehmen nach dem Baugesetzbuch eingeholt werden. Da der insoweit zuständige Ausschuss der Gemeindevertretung nicht über hinreichende Sach- und Rechtskenntnisse verfügte, hat das Bauamt der Amtsverwaltung eine entsprechende Zuarbeit geleistet. Der betroffene Bürger beantragte nunmehr Akteneinsicht in diese interne Zuarbeit.

Die Zuarbeit des Amtes bezieht sich auf ein konkretes Bauvorhaben des Bürgers und enthält daher dessen personenbezogene Daten. Der Bürger hat deshalb einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten nach § 18 Brandenburgisches Datenschutzgesetz (BbgDSG). Da die Zuarbeit als schriftlicher Vermerk in der Verwaltung abgelegt ist, besteht außerdem ein Anspruch auf Akteneinsicht.

Dabei kommt es nicht darauf an, ob das Verfahren noch läuft oder bereits abgeschlossen ist. Ebenso wenig ist von Bedeutung, dass es sich lediglich um eine verwaltungsinterne Zuarbeit ohne Außenwirkung handelt. Der Anspruch des Betroffenen nach § 18 BbgDSG sieht derartige Einschränkungen nicht vor und geht insoweit über das Jedermannsrecht nach dem Akteneinsichts- und Informationszugangsgesetz hinaus. Einzige Voraussetzung ist das Vorhandensein personenbezogener Daten des Auskunftsersuchenden.

Auch dürfte das Amt den Bürger nicht an die das Verfahren führende Stelle (also hier das Bauordnungsamt) verweisen. Der Anspruch richtet sich vielmehr gegen die Daten verarbeitende Stelle selbst.

Der Anspruch auf Auskunft und Akteneinsicht über die zur eigenen Person gespeicherten Daten besteht unabhängig vom Stand des Verfahrens und vom rechtlichen Charakter der begehrten Informationen. Sind an einem Verfahren mehrere Behörden beteiligt, richtet sich der Anspruch gegen jede dieser Behörden, wenn sie die personenbezogenen Daten des Betroffenen speichert.

4.6.2.3 Auskunft und Akteneinsicht nach Eigentümerwechsel

Nach einem Eigentümerwechsel begehrte der neue Eigentümer beim zuständigen Wasser- und Abwasserzweckverband Einsicht in die das Grundstück betreffenden Akten, soweit sie den Erschließungsbeitrag für die Abwasseranlage zum Gegenstand hatten. Der Beitragsbescheid war gegenüber den Voreigentümern ergangen und seit Jahren bestandskräftig. Der Zweckverband lehnte die Akteneinsicht u. a. deshalb ab, weil personenbezogene Daten des neuen Eigentümers nicht in den Akten gespeichert seien.

Die Auffassung des Zweckverbandes ist unzutreffend. Die neuen Eigentümer des Grundstücks haben einen Anspruch auf Auskunft und Akteneinsicht nach § 18 Brandenburgisches Datenschutzgesetz (BbgDSG).

Die Akten zum Erschließungsbeitrag enthielten personenbezogene Daten des neuen Eigentümers, obwohl sein Name darin noch nicht auftauchte. Nach dem Brandenburgischen Datenschutzgesetz sind personenbezogene Daten auch Angaben über sachliche Verhältnisse, die einer bestimmbaren natürlichen Person zugeordnet werden können. Dies ist hier ohne Weiteres hinsichtlich des neuen Eigentümers der Fall. Die Akten über den Erschließungsbeitrag beinhalten Angaben über das Grundstück, d. h. Angaben über sachliche Verhältnisse. Das Kommunalabgabengesetz stellt dies noch einmal ausdrücklich klar, indem es festlegt, dass Erschließungsbeiträge als öffentliche Last auf dem Grundstück ruhen.

Diese Angaben lassen sich nicht nur der Person zuordnen, die zum Zeitpunkt des Bescheiderlasses Eigentümer war, sondern selbstverständlich ohne großen Aufwand auch dem neuen Eigentümer des Grundstücks. Somit handelt es sich bei den Akten unzweifelhaft auch um personenbezogene Daten des neuen Eigentümers.

Der Anspruch auf Akteneinsicht ist mit den Geheimhaltungsinteressen Dritter abzuwägen. Hier kommen vor allem die Interessen der Voreigentümer in Betracht. Das Akteneinsichtsinteresse dürfte allerdings regelmäßig überwiegen, da berechtigte Interessen der Voreigentümer an der Geheimhaltung kaum denkbar sind.

Bei sachbezogenen Verwaltungsakten wie z. B. einem Bescheid über Erschließungsbeiträge zu einem bestimmten Grundstück enthalten die darüber geführten Akten auch personenbezogene Daten des jeweiligen aktuellen Eigentümers, auch wenn einer der Voreigentümer Adressat des Bescheides war. Jeder aktuelle Eigentümer hat daher einen Anspruch auf Auskunft und Akteneinsicht nach § 18 BbgDSG.

4.6.3 Zugriff des Administrators auf personenbezogene Daten

Im Zuge unserer Kontrolltätigkeit stellten wir in einer Stadtverwaltung fest, dass ein Administrator unberechtigter Weise auf personenbezogene Daten zugegriffen hat.

Moderne Netzwerkbetriebssysteme ermöglichen eine restriktive Vergabe von Zugriffsrechten. Die Systeme können so konfiguriert werden, dass die Anwender nur auf die personenbezogenen Daten einen Zugriff erhalten, die sie zur Aufgabenerfüllung benötigten. Der Systemadministrator hat dagegen standardmäßig fast alle Rechte im System.

Einerseits sollten Maßnahmen getroffen werden, die einen Missbrauch von personenbezogenen Daten durch den Administrator wirksam verhindern, andererseits sollten diese Maßnahmen aber auch zum Schutz des Administrators realisiert werden. Erfolgt z. B. eine unberechtigte Weitergabe von personenbezogenen Daten, so ist der Administrator immer in einer schlechten Situation, da er in den meisten Fällen nicht nachweisen kann, dass er nicht der „Schuldige“ war. Eine sinnvolle technisch-organisatorische Maßnahme ist die verschlüsselte Speicherung personenbezogener Daten. Dadurch wird erreicht, dass nur die berechtigten Mitarbeiter auf die Daten zugreifen können. Die Schlüsselverwaltung darf dabei natürlich nicht dem Systemverwalter übertragen werden.

Weiterhin sollte in einer Dienstanweisung festgelegt werden, unter welchen Umständen ein Systemverwalter auf welche personenbezogenen Daten im Ausnahmefall (z. B. Fehlerbeseitigung) zugreifen darf. Die Zugriffe sind in jedem Fall zu protokollieren.

Durch Einsatz von Verschlüsselungsverfahren kann ein Zugriff des Systemverwalters auf personenbezogene Daten verhindert werden. Die Rechte des Systemverwalters sollten in einer Dienstanweisung geregelt werden.

4.7 Sonstiges / Verwaltungsrecht

4.7.1 Geheimhaltungsinteresse eines am Verwaltungsverfahren Beteiligten

Im Rahmen der Genehmigung einer Steganlage ist die Fischereibehörde von der zuständigen Genehmigungsbehörde zu beteiligen. Ein Fischereiberechtigter, der in diesem Verfahren Gelegenheit zur Stellungnahme erhält, ging davon aus, dass seine Stellungnahme an die zuständige

Genehmigungsbehörde und den Antragsteller weitergereicht wurde und befürchtete Repressalien.

Zum Schutz der Interessen und Belange der Fischereibehörde sowie der Fischereiberechtigten und Pächter des Fischereirechts steht es diesen Beteiligten nach § 23 Fischereiordnung des Landes Brandenburg frei, innerhalb des Genehmigungsverfahrens für wasserbauliche Anlagen Stellung zu nehmen. Eine sachgerechte Bearbeitung solcher Stellungnahmen kann nur erfolgen, wenn Fischereiberechtigte und Pächter, die Bedenken vorgetragen haben, für Nachfragen zur Verfügung stehen und weiterhin in das Verfahren einbezogen werden können. Auf Grund dessen besteht kein Geheimhaltungserfordernis hinsichtlich der Person des Stellungnehmenden. Ungeachtet dessen, halten wir allerdings eine generelle und pauschale Weiterleitung von Kopien der Stellungnahmen durch die Fischereibehörde an die zuständige Genehmigungsbehörde für nicht erforderlich. Die Fischereibehörde ist vielmehr gehalten, diese nach den fischereilichen Erfordernissen zusammenzustellen, zu bewerten und das Ergebnis der zuständigen Genehmigungsbehörde mitzuteilen. Eine Weiterleitung von Kopien der vollständigen Stellungnahmen kann höchstens im Einzelfall sinnvoll und erforderlich sein.

Ein im Verwaltungsverfahren Beteiligter muss nicht in jedem Fall damit rechnen, dass seine Stellungnahme direkt an die Genehmigungsbehörde und damit an die Antragsteller weitergeleitet wird.

4.7.2 Darf der Datenverarbeiter sich selbst kontrollieren?

In einer Behörde wurde dem Leiter der Personalstelle zugleich auch die Funktion des behördlichen Datenschutzbeauftragten übertragen.

Alle Daten verarbeitenden Stellen des Landes Brandenburg sind nach § 7a Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) verpflichtet, eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten zu bestellen.

Das Gesetz umschreibt zwar nicht genau, welche Personen diese Position übernehmen dürfen, doch setzt es einige Rahmenbedingungen. Neben der erforderlichen Fachkunde und Zuverlässigkeit muss gewährleistet sein, dass sie keinen Interessenkonflikten mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Im Idealfall – vor allen bei größeren Behörden und Einheiten – sollte die Aufgabe daher hauptamtlich ausgeübt werden. In kleineren Behörden, ist dies auf Grund der Stellensituation häufig nicht möglich, sodass neben dem Datenschutz zumeist weitere Aufgabenfelder zum Tätigkeitsbereich der beauftragten Person zählen.

Zu den Pflichten der oder des behördlichen Datenschutzbeauftragten gehört es, auf die Einhaltung der unterschiedlichen Datenschutzvorschriften zu achten. An sie oder ihn können sich alle Beschäftigten der jeweiligen Einrichtung wenden, wenn sie der Auffassung sind, dass datenschutzrechtliche Bestimmungen oder Regeln der Datensicherheit beim Umgang mit personenbezogenen Daten nicht hinreichend beachtet werden. Um die Wirksamkeit der Arbeit zu verstärken, hat der oder die behördliche Datenschutzbeauftragte Stillschweigen über die Identität der Beschwerde führenden Person zu bewahren und kann zudem Einsicht in alle Verfahren nehmen, in oder mit denen personenbezogene Daten verarbeitet werden. Gestärkt wird diese Position dadurch, dass sie oder er im Bereich der Ausübung dieser Position fachlich weisungsfrei bleibt.

Aus den Umrissen der Stellung und Befugnisse folgen implizit Regeln für Unvereinbarkeiten mit anderen Tätigkeiten: Wer an exponierter Stelle mit der Daten verarbeitenden Technik in einer Behörde umgeht, möglicherweise sogar die Leitung der EDV-Abteilung inne hat, darf nicht zugleich für ihre Kontrolle eingesetzt werden.

Gleiches gilt insoweit für die Leitungsfunktion in einer Personalstelle. Gerade die Personalstelle stellt mit ihrer Vielzahl von personenbezogenen Vorgängen naturgemäß auch die Stelle dar, in der beim Umgang mit diesen Daten möglicherweise Fehler auftreten können, die schon durch das Eingebundensein in die speziellen Verwaltungsabläufe dort vielleicht gar nicht wahrgenommen werden. Außerdem können sich die Beschäftigten nicht unbefangen mit ihren Beschwerden und Eingaben an die Leitung der Personalstelle wenden, da diese gleichzeitig die personalrechtliche Entscheidung in der Angelegenheit trifft. Auf Grund dieses offensichtlichen Interessenkonflikts darf die Leitung der Personalstelle nicht zugleich mit dem Datenschutz beauftragt werden.

Die Position der oder des behördlichen Datenschutzbeauftragten setzt voraus, dass sie ohne Interessenkonflikte ausgeübt werden kann. Die gleichzeitige Übernahme von Leitungsfunktionen in EDV- oder Personalabteilungen ist mit ihr unvereinbar.

5 Justiz und Europaangelegenheiten

5.1 Der Richtervorbehalt im DNA-Analyse-Verfahren

Bislang werden in Brandenburg DNA-Analysen von Beschuldigten und verurteilten Straftätern für zukünftige Strafverfahren nach der Strafprozessordnung in jedem Fall nur auf richterliche Anordnung vorgenommen. Die Ministerin der Justiz und für Europaangelegenheiten will diese Praxis

nun auf dem Erlasswege[50] ändern und den Richtervorbehalt als „bürokratisches“ Hindernis durch die Einwilligung des Betroffenen ersetzen.

Darüber hinaus unterstützt die Landesregierung die Initiative einiger Bundesländer im Bundesrat, die Strafprozessordnung mit dem Ziel zu ändern, dass in Zukunft den Betroffenen ein sog. „genetischer Fingerabdruck“ von der Polizei ohne Einschaltung des Richters auch gegen ihren Willen als Teil der herkömmlichen erkennungsdienstlichen Behandlung abgenommen und analysiert werden kann.

Nach der derzeitigen Rechtslage sieht die Strafprozessordnung in § 81a Abs. 2 vor, dass die Entnahme von Körperzellen grundsätzlich nur durch den Richter angeordnet werden kann, nur bei Gefahr im Verzug kann die staatsanwaltschaftliche oder polizeiliche Anordnung ausreichen. Die Möglichkeit der Einwilligung des Betroffenen erstreckt sich lediglich auf die Art der zu entnehmenden Probe (Blut- oder Speichelprobe) nicht aber auf die Entnahme selbst. Die anschließende molekulargenetische Untersuchung der Probe zum Zweck der Aufnahme in die DNA-Analysedatei beim Bundeskriminalamt darf nur der Richter anordnen. Dabei muss er eine Prognoseentscheidung darüber treffen, ob wegen der Ausführung der Tat, der Persönlichkeit des Täters oder auf Grund sonstiger Erkenntnisse mit hinreichender Wahrscheinlichkeit angenommen werden kann, dass in Zukunft wieder gegen den Betroffenen wegen einer Straftat von erheblicher Bedeutung ermittelt werden muss. Einer Eilkompetenz der Staatsanwaltschaft oder der Polizei wie bei der Zellentnahme bedarf es hier schon deshalb nicht, weil die zu analysierende Probe bereits vorliegt und mit den modernen Methoden der Molekulargenetik auch noch nach längerer Zeit ausgewertet werden kann.

Anders verhält es sich bei den nur auf freiwilliger Basis durchführbaren DNA-Massentests[51], deren Ergebnisse nicht in der zentralen Analysedatei beim Bundeskriminalamt gespeichert werden dürfen. Es ist bezeichnend für solche Massenverfahren, dass sich zwar der gesuchte Täter mit hoher Wahrscheinlichkeit in der Menge der einbezogenen Teilnehmer befindet, der einzelne Proband aber dennoch unverdächtig und damit nicht polizeipflichtig ist. Somit besteht keine gesetzliche Verpflichtung, sich der Maßnahme zu unterziehen und die Einwilligung ist die einzige Voraussetzung für die Teilnahme. Die Frage der richterlichen Anordnung stellt sich hier erst gar nicht. Allerdings setzt eine wirksame Einwilligung voraus, dass die Probanden hinreichend präzise über die Verwertung ihrer Daten informiert werden.

---

[50] Die bisherige Praxis ist geregelt im Erlass v. 20. Dezember 2000 zur Umsetzung des DNA-Identitätsfeststellungsgesetzes (410 III.9/19SH2, Justizmitteilungsblatt 2001, 18)

[51] vgl. dazu auch A 4.1.6

Unbestreitbar hat die Anwendung der DNA-Analyse auch in Brandenburg erheblich zur Aufklärung selbst lange zurückliegender Gewaltverbrechen beigetragen. Dennoch sprechen gewichtige Gründe dagegen, diese neue Methode der Kriminaltechnik ebenso routinemäßig und unter unscharfen rechtlichen Voraussetzungen einzusetzen wie die herkömmliche erkennungsdienstliche Behandlung. Schon der häufig verwendete Begriff des „genetischen Fingerabdrucks“ ist irreführend und verharmlosend. Anders als bei der Abnahme von Finger- bzw. Handflächenabdrucken werden nicht nur begrenzte äußerliche Merkmale des Einzelnen erhoben. Vielmehr wird damit in die individuelle Persönlichkeitsstruktur eingegriffen und Randbereiche der Wesensstruktur des Einzelnen werden mit dem Ziel analysiert, sie zur Strafverfolgung zu nutzen. Bereits heute fallen bei einer DNA-Analyse mehr Erkenntnisse (z. B. Geschlecht, Haar-, Augen- und Hautfarbe, ethnische Herkunft) an, als nach § 81e Strafprozessordnung zulässigerweise verwendet werden dürfen. Nur die zusätzliche Bestimmung des Geschlechts mit molekulargenetischen Methoden wird ab dem 1. April 2004 zulässig sein[52]. Weitere Überschussinformationen, die nicht nur das äußere Erscheinungsbild, sondern die innerste Persönlichkeitssphäre, z. B. die Veranlagung zu bestimmten Krankheiten, betreffen, sind in Zukunft auch bei den gegenwärtig genutzten Analyseverfahren nicht auszuschließen. Wegen dieser von der Nutzung der DNA-Analyse ausgehenden Risiken für die Persönlichkeitsrechte der Betroffenen wollte der Gesetzgeber mit dem Richtervorbehalt einen vorbeugenden Grundrechtsschutz gewährleisten. Der Richtervorbehalt ist damit mehr als nur eine zusätzliche bürokratische Hürde, die den zügigen Verfahrensgang aufhält. Sowohl das Bundesverfassungsgericht als auch das Verfassungsgericht des Landes Brandenburg haben mehrfach diese grundrechtssichernde Funktion des Richtervorbehalts betont. Der Bundesgesetzgeber hat sich dadurch jüngst veranlasst gesehen, die Anforderungen an die Prognoseentscheidung des Richters noch weiter zu präzisieren[53].

Aber nicht allein dieser Aspekt, sondern auch praktische Erwägungen stehen der Abschaffung des Richtervorbehalts entgegen. Die richterliche Prognoseentscheidung über eine vom Betroffenen ausgehende Wiederholungsgefahr ist durch dessen Einwilligung nicht sinnvoll zu ersetzen. Auch nach umfassender Aufklärung des Betroffenen über die Konsequenzen seiner Einwilligung – nach dem Datenschutzrecht eine unabdingbare Voraussetzung jeder wirksamen Einwilligung – ist eine wirklichkeitsnahe Prognose von ihm nicht zu erwarten. Bei Strafermittlungsverfahren ist die freie Willensentscheidung der Betroffenen von vornherein zu hinterfragen. Es ist eher davon auszugehen, dass ein Betroffener nur deshalb in die in Rede stehenden Maßnahmen

[52] Art. 3 des Gesetzes zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften v. 27.12.2003, BGBl. I, S. 3007

[53] Ebda.

einwilligt, weil er bei einer Verweigerung Nachteile befürchtet. In solchen Fällen kann nicht mehr von Freiwilligkeit gesprochen werden.

Die DNA-Analyse zur Identitätsfeststellung ist mit dem herkömmlichen Fingerabdruck nicht zu vergleichen. Bei ihr fallen bereits jetzt Überschussinformationen zu Eigenschaften der untersuchten Person an, die über ihre Identität weit hinausgehen. Dieser Umstand und die Einstellung der Ergebnisse von DNA-Analysen in die zentrale Datei beim Bundeskriminalamt erfordern zwingend die Beibehaltung der richterlichen Prognoseentscheidung als grundrechtssichernde Maßnahme. Die Einwilligung eines Beschuldigten oder verurteilten Straftäters in eine so weit reichende Maßnahme kann die Entscheidung des Richters nicht ersetzen.

5.2 Einsichtsrechte in Ermittlungsakten bei Staatsanwaltschaft und Gericht

Immer wieder wenden sich Privatpersonen an uns, die in staatsanwaltschaftliche Ermittlungsakten einsehen wollen. Viele berufen sich dabei auf das ihnen nach dem Akteneinsichts- und Informationszugangsgesetz zustehende Recht.

Rechtsgrundlage für die Einsichtnahme in die Akten eines Strafermittlungsverfahrens ist jedoch nicht das Akteneinsichts- und Informationszugangsgesetz, sondern allein die Strafprozessordnung. Zugänglich sind nur diejenigen Akten bei der Staatsanwaltschaft, die dem Gericht nach Abschluss der Ermittlungen übergeben werden oder übergeben werden müssten, wenn öffentlich Klage erhoben würde. Das Recht auf Einsichtnahme erstreckt sich nicht auf die Handakten der Staatsanwaltschaft.

Ausschlaggebend für den Umfang der Einsichtnahme ist die Rolle des Antragstellers in dem Ermittlungsverfahren. Dem Beschuldigten steht gem. § 147 Strafprozessordnung (StPO) über seinen Verteidiger ein grundsätzlich uneingeschränktes Einsichtsrecht in die Ermittlungsakten zu. Nur wenn der Untersuchungszweck während eines noch nicht abgeschlossenen Ermittlungsverfahrens durch die Einsichtnahme gefährdet würde, kann sie für einen beschränkten Zeitraum versagt werden. Nach Abs. 7 der Vorschrift kann die Staatsanwaltschaft auch dem Beschuldigten selbst Auskunft erteilen bzw. ihm Abschriften aus der Akte zur Verfügung stellen, wenn dem weder schutzwürdige Interessen Dritter noch eine Gefährdung des Untersuchungszwecks entgegen stehen.

Gem. § 406e StPO hat ein als Nebenkläger am Verfahren beteiligter Verletzter bzw. Geschädigter einer Straftat dieselben Einsichtsrechte wie der Beschuldigte. Soweit jemand aus diesem Personenkreis nicht Nebenkläger ist,

stehen ihm die o. g. Rechte nur zu, wenn er ein berechtigtes Interesse darlegen kann. Ein solches Interesse liegt beispielsweise schon vor, weil der Antragsteller durch die rechtswidrige Tat geschädigt worden ist. Für den Nebenkläger entfällt diese Darlegungspflicht.

Schließlich können aber auch am Verfahren nicht beteiligte Privatpersonen, vertreten durch einen Rechtsanwalt, gem. § 475 StPO Einsicht in Ermittlungsakten nehmen oder Auskünfte erhalten, soweit sie dafür ein berechtigtes Interesse darlegen und die Betroffenen, also neben den oben Genannten bspw. die Zeugen, kein schutzwürdiges Interesse an der Versagung der Akteneinsicht haben. Unter denselben Voraussetzungen kann die Staatsanwaltschaft auch einer nicht durch einen Rechtsanwalt vertretenen Privatperson Auskunft aus den Akten erteilen.

Einem nicht durch einen Rechtsanwalt vertretenen Antragsteller stehen keine Einsichtsrechte in staatsanwaltschaftliche Ermittlungsakten zu. Die Staatsanwaltschaft kann jedoch nach pflichtgemäßem Ermessen in diesem Fall Auskunft erteilen bzw. Abschriften herausgeben, wenn dadurch weder die schutzwürdigen Interessen Dritter noch der Untersuchungszweck beeinträchtigt oder gefährdet werden.

5.3 Daten von Grundstückseigentümern für ein privates Bauvorhaben

Eine Bürgerinitiative, die in Zeiten knapper öffentlicher Kassen beabsichtigt, den Bau einer Straße selbst in die Hand zu nehmen, beantragt bei der Gemeinde die Herausgabe der Daten aller von dem Bauvorhaben betroffenen Grundstückseigentümer und -eigentümerinnen.

Angaben über die Eigentumsverhältnisse an Grundstücken sind Einzelangaben über die sächlichen Verhältnisse bestimmter Personen und somit personenbezogene Daten i. S. d. Brandenburgischen Datenschutzgesetzes (BbgDSG).

Nach § 16 BbgDSG können personenbezogene Daten an eine Stelle außerhalb des öffentlichen Bereichs übermittelt werden, wenn unter anderem der Antragsteller ein berechtigtes Interesse geltend macht und der Betroffene der Datenübermittlung nicht widersprochen hat.

Dass die Absicht der Bürgerinitiative, den Bau einer Straße selbst zu organisieren, als berechtigtes Interesse zu betrachten ist, dürfte unstrittig sein. Allerdings ist die Frage nach dem Widerspruch der betroffenen Grundstückseigentümer nur zu klären, wenn diese überhaupt über das Anliegen der Bürgerinitiative sowie über ihr Widerspruchsrecht informiert sind. An Stelle eines

aufwändigen Zustimmungsverfahrens haben wir vorgeschlagen, ein Adressmittlungsverfahren durchzuführen:

Die Bürgerinitiative legt ihr Anliegen in Schreiben an die Grundstückseigentümer dar und übergibt diese Schreiben versandfertig an die Gemeinde zwecks Adressierung und Versand. Die Empfänger werden in den Briefen gebeten, sich – auf freiwilliger Basis – bei der Gemeinde zurückzumelden und zu äußern, ob sie mit der Herausgabe ihrer Daten einverstanden sind. Nur wenn dies der Fall ist, erhält die Bürgerinitiative die gewünschten Informationen. Um Missverständnisse zu vermeiden, sollte das Schreiben die Grundstückseigentümer auch über das Vorgehen bei einem Adressmittlungsverfahren informieren.

Grundsätzlich verfügt das Amtsgericht als Grundbuch führende Stelle über dieselben Informationen, die dort auf der Grundlage von § 12 Grundbuchordnung einsehbar sind. Hier genügt die Darlegung des berechtigten Interesses; eines Adressmittlungsverfahrens bedarf es nicht. Die Grundbuchordnung gilt allerdings nicht für die Gemeinde, bei der die Herausgabe der Informationen beantragt wurden. Ein Verweis auf das Grundbuchamt wäre in diesem Fall eine Alternative zu dem aufwändigeren Adressmittlungsverfahren.

Bei Vorliegen eines berechtigten Interesses ist den Grundbuchämtern die Weitergabe von Daten der Grundstückseigentümer erlaubt. Gemeindeverwaltungen, die über dieselben Daten verfügen, sind auf die Durchführung eines Adressmittlungsverfahrens angewiesen, um die Zustimmung der Betroffenen einzuholen.

6 Bildung, Jugend und Sport

6.1. Was Hänschen nicht lernt ... Datenschutzgerechte Nutzung des Internets an Schulen

Der Nutzung des Internets kommt auch an den Schulen immer größere Bedeutung zu. So haben die Schülerinnen und Schüler an der großen Mehrzahl der Schulen die Möglichkeit, für schulische – nicht selten aber auch außerhalb des Unterrichts für private – Zwecke das Internet zu nutzen. Eine zunehmende Zahl von Schulen betreibt zudem eine eigene Homepage, die oft von Schülerinnen und Schülern gestaltet wird.

Um die häufig an den Schulen bestehende erhebliche Unsicherheit beim Umgang mit dem Internet zu beheben, hat die Kultusministerkonferenz rechtliche Hinweise zur Nutzung des Internets an Schulen erarbeitet. Allerdings hat sie die Datenschutzbeauftragten der Länder nur unzureichend an der

Entwicklung der rechtlichen Hinweise beteiligt, sodass datenschutzrechtliche Aspekte kaum berücksichtigt wurden. Um diesem Mangel abzuhelfen, hat das Ministerium für Bildung, Jugend und Sport mit uns datenschutzrechtliche Empfehlungen zur Anwendung der rechtlichen Hinweise der Kultusministerkonferenz erarbeitet.

Das Ministerium für Bildung, Jugend und Sport hat die rechtlichen Hinweise zusammen mit den datenschutzrechtlichen Empfehlungen in einem Rundschreiben bekannt gemacht.[54] Die Schulen sind damit verpflichtet, die Hinweise und Empfehlungen zu berücksichtigen. Aus datenschutzrechtlicher Sicht sind insbesondere folgende Maßgaben zu beachten:

- Für die Nutzung des Internets durch Schülerinnen und Schüler ist eine Nutzungsordnung zu erstellen, die den Schülerinnen und Schülern bekannt zu machen ist. Dort sind die Bedingungen der Internetnutzung klar festzulegen. Dazu gehört auch, unter welchen Voraussetzungen welche konkreten Daten über die Schülerinnen und Schüler gespeichert und ausgewertet werden.

- Ist den Schülerinnen und Schülern die Nutzung bestimmter Inhalte verboten, darf das Nutzungsverhalten nur soweit kontrolliert werden, wie dies für die Erfüllung des mit der Nutzung des Internets bezweckten Bildungsziels unabdingbar ist. Bevor das Surfverhalten aller Schülerinnen und Schüler protokolliert wird, sind zunächst alle Möglichkeiten auszuschöpfen, die ohne oder mit geringeren Eingriffen auskommen, also beispielsweise der Einsatz von Filterprogrammen, oder eine unmittelbare Kontrolle durch die aufsichtsführende Lehrkraft.

- Die Speicherung von IP-Adressen der von den Schülerinnen und Schülern genutzten Rechner ist nur zulässig, wenn ein konkreter Verdacht des Missbrauchs besteht. Unabhängig davon können Stichproben vorgenommen werden.

- Wird die private Nutzung des schulischen Internet-Anschlusses erlaubt, darf die Schule dies in der Nutzungsordnung an einschränkende Bedingungen – beispielsweise eine stichprobenartige Protokollierung der Zugriffe – geknüpft werden. Dieser Eingriff in das Fernmeldegeheimnis kann nur auf eine Einwilligung der Schülerinnen und Schüler (bei Minderjährigen der Eltern) gestützt werden. Allerdings kann die Schule eine private Nutzung bei Verweigerung dieser Zustimmung gänzlich ausschließen.

---

[54] Rundschreiben 4/03 v. 12. Mai 2003, ABl. MBJS Nr. 6/2003, S. 158, im Internet abrufbar unter http://www.brandenburg.de/sixcms/media.php/1240/ABl_Bildg_06_2003.pdf

- Die private Nutzung eines schulischen E-Mail-Accounts etwa nach dem Muster Vorname.Name@xy-Schule.de sollte untersagt werden, da anderenfalls eine Inhaltskontrolle gegen das Fernmeldegeheimnis verstieße. Für das Versenden privater E-Mails sind die Schülerinnen und Schüler auf Webmail-Angebote zu verweisen. Diese dürfen von der Schule nicht kontrolliert werden; sie ist dafür auch nicht verantwortlich.

- Die Veröffentlichung von personenbezogenen Daten der Schülerinnen und Schüler, der Eltern sowie der Lehrkräfte ist grundsätzlich nur mit deren Einwilligung zulässig. Das gilt auch für die Veröffentlichung von Bildern auf der Homepage der Schule. Ausnahmen gelten nur für besondere Funktionen als Gremienmitglieder (Schulelternsprecher, Schülersprecher der Schule) sowie Lehrkräfte mit Funktionen, die auf den Kontakt zur breiten Öffentlichkeit angelegt sind (z. B. Mitglieder der Schulleitung).[55]

Die rechtlichen Hinweise der Kultusministerkonferenz mit unseren ergänzenden Empfehlungen bieten eine gute Basis zur datenschutzgerechten Nutzung des Internets an den Schulen.

6.2 Dürfen Datenspuren eines anonymen Diskussionsteilnehmers verfolgt werden?

Das Ministerium für Bildung, Jugend und Sport (MBJS) bietet auf seiner Homepage Diskussionsforen an, die auch anonym genutzt werden können. Ein Forumsteilnehmer fühlte sich durch einen anonymen Beitrag in seiner Ehre verletzt und bat deshalb das Ministerium, ihm den Namen dieses Internetnutzers mitzuteilen. Die Behörde verweigerte die Auskunft mit der Begründung, dass es bei Gästen, die sich ohne Namen einloggen, über keine Daten verfüge.

Nach Auskunft des Ministeriums für Bildung, Jugend und Sport gibt es für seine angebotenen Foren folgende drei Beteiligungsstufen:

1. Stufe: Registrierung als Forumsmitglied mit Name und E-Mail-Adresse

2. Stufe: Eingabe des Benutzers als „Gast“ und als Passwort „Gast“ mit Lese- und Schreibzugriff

3. Stufe: keine Registrierung, lediglich Lesezugriff.

[55] vgl. dazu Faltblatt des LDA Brandenburg „Schulen, Internet und Datenschutz“, abrufbar unter http://www.lda.brandenburg.de

Unabhängig davon, um welchen speziellen Dienst es sich bei der Homepage des Ministeriums für Bildung, Jugend und Sport handelt, regeln § 4 Abs. 7 Teledienstedatenschutzgesetz (TDDSG) sowie § 20 Abs. 1 Mediendienste-Staatsvertrag (MDStV) den Auskunftsanspruch der Nutzer hinsichtlich der Daten, die ein Teledienste- bzw. Mediendiensteanbieter über sie gespeichert hat. Der Auskunftsanspruch bezieht diejenigen Daten des Nutzers ein, die zu seinem Pseudonym gespeichert sind. Für Daten die anonym gespeichert sind, kann es einen personenbezogenen Auskunftsanspruch naturgemäß nicht geben.

Das Ministerium für Bildung, Jugend und Sport als Diensteanbieter hat dem Nutzer entsprechend den gesetzlichen Vorgaben die Inanspruchnahme von Tele- und Mediendiensten und ihre Bezahlung anonym ermöglicht. Eine Pflicht zur Identifikation für Diskussionsteilnehmer sieht das geltende Recht aus guten Gründen nicht vor.

Die Beiträge des Gastes im Rahmen des Diskussionsforums entsprechen somit den gesetzlichen Vorgaben und begründen keine Auskunftspflicht des MBJS den einzelnen Teilnehmern gegenüber.

Selbst wenn dem Ministerium für Bildung, Jugend und Sport Daten über den Gastteilnehmer vorliegen sollten, wäre keine Rechtsgrundlage vorhanden, die es dem Ministerium für Bildung, Jugend und Sport erlauben würde, einem Dritten zu rein privaten Zwecken Daten über einen weiteren Teilnehmer seines Diskussionsforums mitzuteilen. Dies gilt auch, wenn es um Inhalte geht, die gegen Bestimmungen des Strafgesetzbuches verstoßen. Allerdings könnten die Strafverfolgungsbehörden auf diese Informationen zugreifen.

Nach § 11 Teledienstegesetz (TDG) / § 9 MDStV sind Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, auch nicht verantwortlich. Sie müssen aber unverzüglich tätig werden, wenn sie Kenntnis von den rechtswidrigen Handlungen erlangen. Das Ministerium für Bildung, Jugend und Sport hat uns versichert, dass es entsprechend dieser Verantwortlichkeitsregeln verfährt. Es hat außerdem unsere Empfehlung aufgegriffen, auf seiner Homepage deutlicher über die möglichen Formen der Beteiligung an Diskussionsforen zu informieren.

Tele- bzw. Mediendiensteanbieter haben die Pflicht, den Nutzern eine Wahlmöglichkeit zwischen der Nutzung eines „personalisierten“ oder anonymen/pseudonymen Angebots einzuräumen und sie auch rechtzeitig vor Nutzung des Angebots auf diese Möglichkeiten hinzuweisen. Wenn sich der Nutzer dann gegen eine Registrierung entscheidet, darf der Anbieter keine möglichen Datenspuren verfolgen.

7 Wissenschaft, Forschung und Kultur

7.1 Wind unter den Talaren – zur Evaluation der Lehre

Viele Hochschulen sind bestrebt, zwecks Feststellung der Qualität ihres Lehrangebots auch die Studierenden in anonymer Form zu Wort kommen zu lassen. Bei der Evaluation der Lehrveranstaltungen werden häufig Fragebögen eingesetzt, mittels derer nicht nur der Inhalt der Kurse erkundet, sondern auch dazu aufgefordert wird, die Dozentinnen und Dozenten zu bewerten.

Die Bewertung von Lehrveranstaltungen nach ihren Inhalten und der Art und Weise der Vermittlung durch die einzelnen Vortragenden stellt eine Erhebung personenbezogener Daten dar, da sie geeignet ist, Aussagen über die Fähigkeiten der Lehrpersonen zu treffen. Geschieht eine solche Erhebung durch die Hochschule selbst, so bedarf sie einer rechtlichen Grundlage.

Zwar ermöglicht § 5 Abs. 3 Brandenburgisches Hochschulgesetz die Evaluation von Lehrveranstaltungen, allerdings sind wir – anders als das Ministerium für Forschung, Wissenschaft und Kultur – der Auffassung, dass das Gesetz allein hierfür keine ausreichende Grundlage bietet. Vielmehr ermächtigt es die Landesregierung lediglich zum Erlass einer Rechtsverordnung, die bisher nicht existiert.

Sobald diese Rechtsverordnung erlassen wird, steht einer personenbezogenen Befragung zu den Lehrveranstaltungen sowie der Auswertung und Erörterung deren Ergebnisse zumindest im Rahmen der Universitätsöffentlichkeit aus unserer Sicht nichts entgegen. Dennoch dürfen die Ergebnisse zwar als Anknüpfungspunkt für personalrechtliche Maßnahmen mit dem Ziel der Verbesserung der Lehre verwendet, aber nicht direkt in die Personalakte der Lehrkräfte aufgenommen werden.

Die Befragung von Studierenden nach der Qualität von Lehrveranstaltungen ist auch dann zulässig, wenn dabei die Dozentinnen und Dozenten bewertet werden sollen. Zwar können die Ergebnisse erörtert und für die Verbesserung der Lehre verwendet werden, gehören jedoch nicht in die Personalakte.

7.2 Alle Zwillinge in ein Register?

Zur Durchführung von Forschungsprojekten strebte eine Universität die Übermittlung von Daten zu Zwillingen durch die Meldebehörden an und beabsichtigte, diese für künftige Forschungsvorhaben in einem bundesweiten Zwillingsregister vorzuhalten.

Grundsätzlich haben alle Menschen, deren Daten zu Forschungszwecken abgefragt werden sollen, das Recht, selbst zu bestimmen, ob sie der Wissenschaft Angaben zu ihrer Person zur Verfügung stellen möchten. Die Einwilligung der Betroffenen in die Datenübermittlung ist somit erforderlich. Allerdings ist die Wissenschafts- und Forschungsfreiheit nach dem Werteverständnis des Grundgesetzes ebenfalls ein hochrangiges Rechtsgut. Aus diesem Grunde enthalten viele Gesetze so genannte Forschungsklauseln, die das Einwilligungserfordernis unter bestimmten Voraussetzungen ersetzen.

Die Weitergabe von Daten einer Vielzahl namentlich nicht bezeichneter Personen durch die Meldebehörden an andere öffentliche Stellen ist nach § 28 Brandenburgisches Meldegesetz gestattet, soweit es deren Aufgabenerfüllung dient. Universitäten, zu deren Aufgaben die Durchführung von Forschungsvorhaben nach § 3 Brandenburgisches Hochschulgesetz fällt, können solche Angaben daher erhalten. Allerdings dürfen die Daten nur für ein konkret umschriebenes Vorhaben und nicht für eine beliebige Anzahl noch unbestimmter, künftiger Projekte übermittelt werden.

Ein vom konkreten Forschungsvorhaben unabhängiges bundesweites Register mit Daten aller Zwillinge ist ohne deren Einwilligung unzulässig. Aber selbst unter der Voraussetzung, dass die Zustimmung der Betroffenen vorliegt, wäre ein bundesweites Zwillingsregister nur unter hohem Aufwand zu realisieren. So könnte von Zwillingspaaren das jederzeit widerrufliche Einverständnis eingeholt werden, nicht nur ihre Daten zu verarbeiten, sondern sie auch künftig im Hinblick auf die Teilnahme an weiteren Forschungsprojekten anzusprechen. Problematisch ist das Zustimmungsverfahren insbesondere bei Minderjährigen: Die Datenübermittlung bedarf sowohl ihrer Zustimmung als auch der der Sorgeberechtigten. Hinsichtlich der Daten von Kindern, die ausschließlich auf Wunsch der Eltern in das Register aufgenommen werden, ist das persönliche Einverständnis der Betroffenen zudem zu einem späteren Zeitpunkt einzuholen.

Allerdings ist die Brauchbarkeit eines zentralen Zwillingsregisters unabhängig von den rechtlichen Voraussetzungen schon deshalb fraglich, weil es – im Gegensatz zum Melderegister – nicht ständig gepflegt wird und somit auch weiterhin Nachfragen beim Melderegister notwendig wären.

Private Forschungseinrichtungen können auf Grund melderechtlicher Vorschriften lediglich Angaben über bestimmte namentlich ausdrücklich bezeichnete Personen erhalten oder müssen sich eines Adressmittlungsverfahrens[56] bedienen. In der Praxis bleiben sie damit – wie beispielsweise die Pharmaforschung – weit gehend auf die Werbung von Probanden per Annonce beschränkt.

Auch Hochschulen, denen Meldedaten zu Forschungszwecken übermittelt werden können, dürfen ein projektunabhängiges zentrales Zwillingsregister nicht ohne ausdrückliche Einwilligung der Betroffenen einrichten. Da der für die Pflege eines solchen Registers notwendige administrative Aufwand kaum zu vertreten ist, sollte sich die Forschung personenbezogene Daten nur für konkrete Vorhaben beschaffen.

7.3 Forschungseinwilligung – kein Freibrief zur Veröffentlichung

Nachdem ein Zeitzeuge der Nutzung personenbezogener Daten für ein historisches Forschungsprojekt zugestimmt hatte, wurden Interviews mit ihm geführt und sein Lebenslauf ausgewertet. Die Ergebnisse des Projekts wurden unter voller Namensnennung des Betroffenen, jedoch ohne seine Einwilligung, in einer Ausstellung veröffentlicht.

Personenbezogene Daten dürfen zu Forschungszwecken auch dann genutzt werden, wenn es sich um besonders sensitive Daten handelt. Welche Angaben verwendet werden dürfen, entscheidet allerdings die „beforschte“ Person (siehe oben Teil A, Punkt 7.2). Die Einwilligung bedarf einer eingehenden Information der Betroffenen über den konkreten Verwendungszweck der Daten und sie muss schriftlich erfolgen. Je sorgfältiger diese Information erfolgt, umso leichter kann der Beforschte das Forschungsvorhaben nachvollziehen und wird umso eher bereit sein, am Erreichen des Forschungsziels mitzuwirken.

Die Betroffenen sind unter anderem darüber zu informieren, wie mit den Daten während der Dauer des Forschungsprojekts sowie nach dessen Abschluss umgegangen wird. Je nach Sensitivität der Daten hat die forschende Stelle zudem ein Datensicherheitskonzept zu erstellen, das Regelungen für den Datenzugang und die Datenaufbewahrung vorsieht. Es ist sicherzustellen, dass ein konkreter und für Dritte erkennbarer Personenbezug möglichst frühzeitig unkenntlich gemacht wird und Forschungsergebnisse nur anonymisiert veröffentlicht werden.

[56] vgl. A 5.3

Insbesondere ist die Einwilligung zur Teilnahme an einem Forschungsvorhaben deutlich von dem Einverständnis mit der Veröffentlichung der eigenen Daten zu unterscheiden. Nicht jeder, der der Auswertung seines Lebenslaufs oder seines beruflichen Werdegangs zustimmt, möchte schließlich seinem Bild und seinem Namen in einer öffentlichen Ausstellung begegnen.

Sowohl bei naturwissenschaftlichen, als auch bei den meisten sozialwissenschaftlichen Studien wird eine Anonymisierung der Forschungsergebnisse ohne Weiteres möglich sein. Handelt es sich aber um die Erforschung konkreter politischer oder zeithistorischer Ereignisse, bei denen es gerade auf die beteiligten Personen ankommt, muss eine Abwägung stattfinden: Nur herausragende Personen – so genannte Personen der Zeitgeschichte – müssen es hinnehmen, dass auch ohne ihre Einwilligung über sie geschrieben und diskutiert wird. Dies betrifft allerdings nur den Bereich ihres öffentlichen Handelns – ansonsten haben auch Politiker und andere, in ähnlich herausgehobener Position tätige Personen, ein Recht auf Datenschutz.

Die Einwilligung in die Auswertung der eigenen Daten im Rahmen eines Forschungsvorhabens bedeutet nicht, dass der Betroffene mit der personenbezogenen Veröffentlichung der Forschungsergebnisse einverstanden ist. Hierfür ist eine weitere, ausdrückliche Zustimmung einzuholen.

7.4 Mikroverfilmung von Archivunterlagen für die Ahnenforschung

Wiederholt fragten öffentliche Archive von Gemeinden, aber auch Bürgerinnen und Bürger bei uns nach, ob es denn zulässig sei, dass Unterlagen – hier Adress- und Sterbebücher aus dem 17. bis Mitte des 19. Jahrhunderts – von Privaten auf Mikrofilme übertragen werden dürfen, um mit diesen Ahnenforschung zu betreiben.

Bei den infrage kommenden Unterlagen handelt es sich zweifelsfrei um solche mit Personenbezug. Angesichts ihres Alters ist jedoch sicher, dass keine lebenden Personen mehr betroffen sind. Daher fallen sie nicht unter den Schutzbereich des Brandenburgischen Datenschutzgesetzes (BbgDSG), das lediglich die Daten noch lebender natürlicher Personen schützt.

Werden die Daten wie hier in öffentlichen Archiven aufbewahrt, richtet sich der Umgang mit ihnen nach dem Brandenburgischen Archivgesetz (BbgArchivG). Unter anderem sollen beim Umgang mit Archivmaterial auch die „schutzwürdigen Belange Dritter“ berücksichtigt werden. Archivgut sind in diesem Zusammenhang Unterlagen öffentlicher Stellen, die für die aktuelle Arbeit nicht mehr benötigt werden und aus diesem Grund ausgesondert wurden. Beziehen sie sich dem „wesentlichen Inhalt“ nach auf eine natürliche

Person, dürfen sie im Regelfall erst nach dem Ablauf von zehn Jahren nach dem Tod der betroffenen Person zur Einsicht freigegeben werden (§ 10 BbgArchivG). Mit Ablauf der Schutzfrist ist nach § 9 Abs. 1 BbgArchivG jede Person, die ein berechtigtes Interesse glaubhaft macht, befugt, Einblick in das Archivgut zu erhalten.

Mit dieser Regelung hat der Gesetzgeber eine Abwägung zwischen den Interessen der Beteiligten vorgenommen. Der Wahrnehmung von Persönlichkeitsrechten von Verstorbenen durch ihre Ahnen werden zugunsten der Interessen von Forschern und anderen Interessierten Grenzen gesetzt. Vor dem Hintergrund, dass das so genannte „postmortale Persönlichkeitsrecht“ mit zunehmenden zeitlichen Abstand zur Lebenszeit der betroffenen Person abnimmt, bis es schließlich gänzlich erlischt, erlauben die gegenwärtigen Archivregelungen nach unterschiedlichen Fristen den freien Zugang zu Archiven auch dann, wenn dabei personenbezogene Daten offenbart werden. Darüber hinaus wird zunehmend darüber diskutiert, ob das herkömmliche Archivrecht mit seinen Sperrfristen nicht stärker dem allgemeinen Informationszugangsrecht angepasst werden muss, das für aktuelle Verwaltungsvorgänge unter Wahrung des Datenschutzes einen sofortigen voraussetzungslosen Zugang für jedermann vorsieht.[57]

Die Anforderungen an die Darlegung und Glaubhaftmachung eines berechtigten Interesses der Einsicht nehmenden Person sind nach geltendem Recht bereits erfüllt, wenn die Benutzung der Unterlagen zu wissenschaftlichen, heimatkundlichen, familiengeschichtlichen, publizistischen, unterrichtlichen oder Bildungszwecken geschehen soll. Eine Nutzung ist nur für den Fall zu versagen, dass schutzwürdige Belange Betroffener oder Dritter erheblich überwiegen.

Im speziellen Fall ging es um Lebens- und Adressdaten mit einem Alter von 150 Jahren und mehr, sodass naturgemäß nicht mehr die Belange der Betroffenen selbst, sondern nur noch die der Nachfahren berührt werden können. Angesichts des allgemeinen Charakters der Daten sind sie zudem nicht geeignet, weitere Einzelheiten der Privatsphäre einer einzelnen Person oder einer Familie wiederzugeben. Überwiegende schutzwürdige Belange, die eine Nutzung von Archivgut derart hohen Alters aus Gründen des Persönlichkeitsschutzes unzulässig erscheinen ließen, waren damit nicht gegeben.

[57] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, B I

Personenbezogene Daten Verstorbener unterliegen nicht dem Schutz des Brandenburgischen Datenschutzgesetzes. Befinden sie sich in öffentlichen Archiven, regelt das Brandenburgische Archivgesetz den Umgang mit ihnen. Je älter und allgemeiner sie sind, desto weniger spricht gegen ihre Nutzung für Ahnenforschung oder andere wissenschaftliche Zwecke.

8 Arbeit, Soziales, Gesundheit und Frauen

8.1 Gesundheit

8.1.1 Gesundheitsreform

Bei der derzeitigen Diskussion um die am 1. Januar 2004 in Kraft getretene Gesundheitsreform geht es vor allem um die Praxisgebühr. Bisher ist jedoch noch wenig bekannt, dass die Reform innerhalb der nächsten zwei Jahre auch die Einführung einer neuen elektronischen Infrastruktur vorsieht, die den Datenschutz vor völlig neue Herausforderungen stellt.

Eine bundesweite Infrastruktur für neue elektronische Verfahren soll nach dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung[58] sowohl die Gesundheitsversorgung verbessern als auch die Kosten im Gesundheitswesen dämpfen. Der Schlüssel zu dieser Infrastruktur wird die elektronische Gesundheitskarte sein, die als Krankenversichertenkarte der zweiten Generation die jetzt verwendete Karte ablösen soll. Sie wird in einem verpflichtenden administrativen Teil neben einem Lichtbild und Angaben zum Zuzahlungsstatus dieselben Informationen enthalten wie die bisherige Krankenversichertenkarte. Zudem soll dieser Teil der Gesundheitskarte die Basis für das elektronische Rezept enthalten.

Daneben wird den Patienten in einem medizinischen Teil der Gesundheitskarte die Möglichkeit angeboten, Diagnosen, Notfallinformationen, Informationen über eingenommene Medikamente, elektronische Arztbriefe, eine Arzneimitteldokumentation, die neu eingeführte Patientenquittung bis hin zur elektronischen Patientenakte zu speichern. Allerdings verbleibt – auch auf Grund der Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder[59] – die ausschließliche Verfügungsgewalt über die auf ihr gespeicherten Gesundheitsdaten bei den Patientinnen und Patienten. Sie müssen sich auch gegen eine Speicherung von Gesundheitsdaten auf der Karte entscheiden können, ohne Nachteile zu befürchten. Die genaue Ausgestaltung der Gesundheitskarte wird durch die Selbstverwaltungsgremien des Gesund-

[58] BGBl. 2003 I S. 2190

[59] Vgl. schon Tätigkeitsbericht 2002, A 8.2 und Anlage 2

heitswesens oder durch das Bundesgesundheitsministerium noch festgelegt werden.

Im Zusammenhang mit der elektronischen Gesundheitskarte stellt sich die Frage, ob und in welcher Weise ein zusätzlicher, zentraler Datenpool notwendig ist. Beispielsweise wird für den Fall des Verlusts der Karte erwogen, dass die Informationen nach wie vor in einem zentralen Datenpool verfügbar sein sollen. Aus datenschutzrechtlicher Sicht sollte eine solche Zentralisierung von Patientendaten unbedingt vermieden werden. Allenfalls dürfen darin ausschließlich pseudonymisierte Daten gespeichert werden[60].

Der Gesetzgeber hat im Gesundheitsmodernisierungsgesetz auch eine Forderung der Datenschutzbeauftragten aufgegriffen, indem er das strafprozessuale Beschlagnahmeverbot auch auf solche Patientendaten erstreckt hat, die sich im Besitz eines Dienstleisters befinden, der die Daten im Auftrag verarbeitet. Dies betrifft beispielsweise Unternehmen, die für die Ärzte als Verrechnungsstelle lediglich die Abrechnung von Leistungen durchführen und hierfür Patienteninformationen benötigen, ohne allerdings selbst medizinisch tätig zu werden. Durch das Beschlagnahmeverbot wurde eine wesentliche Schutzlücke für sensitive Gesundheitsinformationen geschlossen.

Im Rahmen der Einführung einer elektronischen Infrastruktur innerhalb der kommenden zwei Jahre wird es darauf ankommen, bei der konkreten Ausfüllung der gesetzlichen Regelungen die Entstehung von patientenbezogenen zentralen Datenpools auszuschließen und Benachteiligungen für solche Versicherten zu unterbinden, die eine Speicherung von Gesundheitsinformationen auf der elektronischen Gesundheitskarte nicht wünschen.

8.1.2 Screening-Programme

8.1.2.1 Neugeborenen-Screening – Ein Vorrat von Millionen genetischer Codes ?

Seit Jahrzehnten wird in Deutschland bei etwa 98% aller neugeborenen Kinder ein so genanntes Neugeborenen-Screening durchgeführt. Dabei wird dem Kind Blut aus der Ferse entnommen, auf Testkarten aus Filterpapier aufgetropft und in einem Labor auf angeborene Krankheiten untersucht, die ohne rechtzeitige Behandlung zu einer schweren geistigen und körperlichen Behinderung des Kindes bis hin zum Tod führen würden. Nach der Analyse der Blutprobe verbleibt ein Blutrest im Teststreifen, der nicht vernichtet, sondern aufgehoben wird. Auf Grund dieser

[60] vgl. die Entschließung der 65. Datenschutzkonferenz vom September 2003, Dokumente zu Datenschutz und Informationsfreiheit 2003, A 1.3

Verfahrensweise existieren bereits riesige Archive von Restblutproben unserer Bevölkerung, aus denen noch Jahre nach der Blutentnahme persönliche Gesundheitsdaten, einschließlich des genetischen Codes, ermittelt werden können. Die Errichtung einer gesamtdeutschen Gendatei ist also potenziell möglich.

Die Notwendigkeit dieser Vorsorgeuntersuchung zum rechtzeitigen Erkennen gesundheitlicher Risiken für das Kind steht außer Frage. Datenschutzrechtlich problematisch erscheint jedoch die zurzeit praktizierte nahezu unbegrenzte Archivierung der Filterkarten mit den Restblutmengen. Bei ihnen handelt es sich ohne Zweifel um eine personenbezogene Datensammlung. In einem bundesweiten Vergleich haben die Datenschutzbeauftragten der Länder festgestellt, dass es hierzu keine einheitliche Verfahrensweise gibt. Eine gesetzliche Legitimation für die Aufbewahrung der Restblutproben fehlt gänzlich.

In Brandenburg gehen die Blutproben aller neugeborenen Kinder in der Carl-Thiem-Klinik in Cottbus (Screeningzentrum) ein. Hier werden die Proben auf fünf Erkrankungen untersucht. Mit einer neuen Methode, der Tandem-Massenspektrometrie, können seit kurzem zusätzlich mehr als 15 weitere Erkrankungen frühzeitig erkannt werden. Diese Untersuchungen werden in einem Labor in Heidelberg durchgeführt. Hierfür wird nicht die gesamte Filterpapierkarte verschickt, sondern nur ein Teil der Blutspots. Diese werden mit einer Nummer codiert, sodass in Heidelberg keine Patientendaten vorliegen. Diese Proben werden nicht aufbewahrt, sondern vernichtet.

In der Carl-Thiem-Klinik werden seit ca. drei Jahren Filterpapierkarten benutzt, bei denen die Blutspots von dem Teil der Karte, der die personenbezogenen Daten enthält, abgetrennt werden können. Damit ist eine getrennte Aufbewahrung möglich. Diese Trennung erfolgt zwei Jahre nach dem Screening. Mittels einer Nummer ist es der Klinik möglich, jederzeit eine Reidentifizierung vorzunehmen. Insofern sind die Daten lediglich pseudonymisiert. Bei älteren Testkarten erfolgt eine namentliche Aufbewahrung, da eine Abtrennung der Blutspots nicht möglich ist.

Ist das Neugeborenen-Screening abgeschlossen, verfügt das Screeningzentrum über die Daten aus der Analyse, die personenbezogenen Daten von Mutter und Kind und zusätzlich über die Restblutproben.

Das Neugeborenen-Screening ist eine freiwillige Vorsorgeuntersuchung. Für die Durchführung bedarf es der Einwilligung der Eltern des Kindes. Eine ausdrückliche schriftliche Einwilligung wird in der Praxis bisher nicht eingeholt. Dies wäre aber in jedem Falle erforderlich, wenn das Screening auf bisher nicht behandelbare Defekte erweitert werden sollte.

Die notwendige Einwilligung zum Screening kann bei Abschluss des Behandlungsvertrages erteilt werden. Vorraussetzung für eine wirksame Einwilligung in dieser Form ist aber eine hinreichende Information der Eltern. Mittels eines Merkblattes, welches den Eltern vor Abschluss des Behandlungsvertrages ausgehändigt wird, informiert das Screeningzentrum die Eltern über die Notwendigkeit einer Untersuchung des Neugeborenen, den Verfahrensablauf, die Versendung der Filterkarte und die Art und Weise der Mitteilung des Untersuchungsergebnisses. Dieses Merkblatt enthält bisher aber keinen Hinweis auf die dauerhafte personenbezogene Aufbewahrung der Trockenblutproben im Screeningzentrum.

In der bisher unbefristeten Aufbewahrung der Restblutproben liegt ein erheblicher Eingriff in das Recht des Einzelnen auf informationelle Selbstbestimmung, wofür eine gesetzliche Grundlage fehlt.

Ein solcher Eingriff in das Selbstbestimmungsrecht ist auch nicht aus Gründen des Arzthaftungsrechts gerechtfertigt. Blut- und Gewebeproben werden in der medizinischen Praxis in der Regel gerade nicht aufbewahrt. Lediglich bezüglich der Befunde besteht eine Aufbewahrungs- und Dokumentationspflicht.

Eine Archivierung zum Zwecke der Forschung ist nur dann zulässig, wenn es sich um ein konkretes Forschungsvorhaben handelt. Daran fehlt es im Zeitpunkt des Screenings in aller Regel. Für künftige Vorhaben muss es genaue Festlegungen geben. Eine Einwilligung von den Betroffenen kann diesbezüglich sicher eingeholt werden.

Aus medizinischen Gründen, wie Kontrolluntersuchungen bei eventuellen Spätmanifestationen ist eine Aufbewahrung nur für einen kurzen, bestimmbaren Zeitraum im Rahmen des Behandlungsvertrages zulässig. Die Carl-Thiem-Klinik hat uns inzwischen zugesagt, alle Restblutproben, die älter als zwei Jahre sind, zeitnah zu vernichten, und alle übrigen Proben zunächst mit einem Pseudonym zu versehen und zwei Jahre nach dem Ende des Jahres der Probenentnahme zu vernichten. Außerdem will die Carl-Thiem-Klinik das Merkblatt für die Eltern um einen entsprechenden Hinweis ergänzen.

Eine längerfristige namentliche Aufbewahrung wäre nur in den Fällen einer festgestellten Erkrankung und nur mit schriftlicher Einwilligung der Eltern zulässig. Eine solche Verfahrensweise würde auf Grund der geringen Anzahl der Fälle keine umfassende Gendatei der Bevölkerung zur Folge haben, die mit der Verfassung nicht zu vereinbaren wäre.

Die bisherige Praxis beim Neugeborenen-Screening genügte nicht den Grundsätzen des Datenschutzrechts. Insbesondere bedarf es für die Durchführung der Blutuntersuchung einer informierten Einwilligung der Eltern. Die Restblutproben dürfen nicht unbegrenzt aufbewahrt werden, weil sonst eine Datenbank über die gesamte Bevölkerung bestünde, die auch für genetische Analysen genutzt werden könnte. Änderungen zur datenschutzgerechten Durchführung des Neugeborenen-Screenings sind uns zugesagt worden.

8.1.2.2 Mammographie-Screening – Brustkrebs rechtzeitig erkennen

Ein bevölkerungsbezogenes Mammographie-Screening soll nun auch in Deutschland eingeführt werden. Auf Beschluss des Deutschen Bundestages im Jahr 2002 soll dieses schrittweise und auf Grundlage der europäischen Leitlinien bis 2005 geschehen. Beabsichtigt ist, allen Frauen zwischen 51 und 69 Jahren im Abstand von zwei Jahren eine Röntgenuntersuchung der Brust zur Früherkennung von Brustkrebs anzubieten. Die entsprechenden bundeseinheitlichen Richtlinien sind am 1. Januar 2004 in Kraft getreten. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hat den Landesbeauftragten hierzu frühzeitig um Beratung gebeten.

Um möglichst alle betroffenen Frauen zu dieser Vorsorgeuntersuchung einladen zu können, werden Adressdaten benötigt, die durch die Melderegister zur Verfügung gestellt werden müssten. Eine Bereitstellung allein durch die gesetzlichen Krankenkassen oder über die Ansprache niedergelassener Ärzte wäre dafür nicht ausreichend, denn diese enthalten nicht wie die Melderegister einen umfassenden Datenbestand der teilnahmeberechtigten Frauen. Nur über den Datenbestand des Melderegisters werden auch Privatversicherte und Sozialhilfeempfängerinnen erreicht.

Die regelmäßige Datenübermittlung vom Melderegister an eine öffentliche Stelle ist nach dem Brandenburgischen Meldegesetz zulässig, wenn nach der Meldedatenübermittlungsverordnung eine Übermittlungsbefugnis zum Zwecke des Mammographie-Screenings besteht. Dies ist bisher nicht der Fall.

Vorgesehen ist, dass die Kassenärztliche Vereinigung, der Landesverband der Krankenkassen und der Verband der Ersatzkassen auf Landesebene eine öffentliche Zentrale Stelle unter Berücksichtigung landesrechtlicher Bestimmungen errichten, die zur Teilnahme am Früherkennungsprogramm unter Verwendung von Meldedaten einladen soll. Allerdings ist dabei zweifelhaft, ob es zur deren Aufgabe gehört, Daten auch nicht gesetzlich Krankenversicherter zu verarbeiten. Damit würde es an einer wesentlichen Voraussetzung für eine rechtmäßige Datenübermittlung der Meldeämter an die zentrale Stelle fehlen. Um hierfür die erforderliche Rechtsgrundlage zu schaffen, haben

wir vorgeschlagen, in das Gesetz über den öffentlichen Gesundheitsdienst eine Regelung aufzunehmen, mit der der Zentralen Stelle eine entsprechende bevölkerungsbezogene Aufgabe zugewiesen wird. Die Zentrale Stelle muss zudem unabhängig von der Kassenärztlichen Vereinigung und den Verbänden der Kranken- und Ersatzkassen organisiert sein, weil sie auch Daten von Privatversicherten verarbeitet, auf die die Kassenärzte und Kranken- bzw. Ersatzkassen kein Zugriffsrecht haben.

Auch die Untersuchung selbst bedarf einer informierten Einwilligung der betroffenen Frauen. Besonderes Augenmerk haben wir deshalb darauf gerichtet, dass das Einladungsschreiben bzw. ein beigefügtes Merkblatt so gefasst wird, dass der Empfängerin eine echte Entscheidung darüber ermöglicht wird, ob sie an der Maßnahme teilnehmen möchte oder nicht. Von dieser Wahlfreiheit kann nur Gebrauch machen, wer die notwendigen Informationen hat. Das Selbstbestimmungsrecht der Patientin setzt eine möglichst umfassende Information voraus. Dazu gehört, die Empfängerin z. B. über mögliche Schäden und notwendige Behandlungen infolge der Untersuchungen zu informieren. Entscheidet sich die eingeladene Frau, am Screening nicht teilzunehmen, entfällt die Legitimation zur weiteren Verarbeitung ihrer Daten. Die Daten werden aus dem Einladungsverfahren herausgefiltert, sodass die Frauen, die ein Screening nicht wünschen, keine weiteren Einladungsschreiben erhalten. Ihre Daten sind zu löschen.

Um festzustellen, ob in der Zeit zwischen zwei Mammographien Brustkrebs aufgetreten ist, der früher hätte entdeckt werden können, ist ein Abgleich mit dem Gemeinsamen Krebsregister vorgesehen. Voraussetzung für eine datenschutzgerechte Übermittlung ist die Einwilligung der betroffenen Frauen in den Datenabgleich. Auch hier ist eine vorherige Information erforderlich, die trotz der komplexen Datenflüsse verständlich sein muss.

Die Gespräche mit dem Ministerium über die offenen Fragen sind noch nicht abgeschlossen.

Die Krebsfrüherkennungs-Richtlinien berücksichtigen zwar bereits wichtige datenschutzrechtliche Grundsätze, allerdings steht die Lösung einiger Fragestellungen noch aus.

8.2 Soziales

8.2.1 Landespflegegesetz

Nach der flächendeckenden Sanierung der stationären und teilstationären Einrichtungen der Altenhilfe, der Behindertenhilfe und der Hilfe für chronisch kranke und suchtmittelabhängige Menschen wurde das Lan-

despflegegesetz (LPflegeG) zur Umsetzung des Elften Buches des Sozialgesetzbuchs (SGB XI) neu geordnet.

Mit der Ausgestaltung des Belegungsrechts für Pflegeeinrichtungen im Land Brandenburg als freiwillige Aufgabe der Kommunen wurden auch Vorschriften des allgemeinen Datenschutzrechts durch eine bereichsspezifische Regelung präzisiert. Dem Grundsatz der Erforderlichkeit folgend sind nur die personenbezogenen Daten zu verarbeiten, die die verarbeitende Stelle zur Erfüllung ihrer Aufgaben benötigt. Sollten also die Kommunen von ihrem Belegungsrecht Gebrauch machen, haben sie das Recht, personenbezogene Daten zum Wohnsitz und zu den Einkommensverhältnissen zu verarbeiten. Für andere Zwecke reichen anonymisierte Angaben aus.

Dem Land Brandenburg obliegt es nach dem Elften Buch Sozialgesetzbuch, die pflegerische Versorgungsstruktur im Land sicherzustellen. Um diese Aufgabe sachgerecht erfüllen zu können, wurden Daten der Träger der Pflegeeinrichtungen, der Träger der Pflegeversicherung, der privaten Versicherungsunternehmen und des Medizinischen Dienstes der Krankenkassen benötigt.

Danach sind Auskünfte nur gegenüber den statistischen Landesämtern und gegenüber den für Planung und Investitionsfinanzierung der Pflegeeinrichtung zuständigen Landesbehörden zulässig. Falls die statistische Erhebung vom Landesbetrieb für Datenverarbeitung und Statistik durchgeführt wird, kann das Ministerium selbst nicht über diese Daten verfügen. Das Ministerium kann dann ebenso wie alle anderen Stellen nur die Ergebnisse der Statistik erhalten, nicht aber die ihr zu Grunde liegenden Daten. Zur Klarstellung war zu entscheiden, welche Institution die Statistik durchführen soll.

Da es sich bei der Datenerhebung um sekundärstatistische Erhebungen handelt, müssen die Träger der Pflegeheime also nur die Daten übermitteln, die im Rahmen ihrer Aufgabenerfüllung ohnehin angefallen sind. Eine darüber hinausgehende Datenerhebung ist ohne Rechtsgrundlage unzulässig.

Für den Zweck der Planung und Investitionsfinanzierung sind zudem keine personenbezogenen Daten erforderlich. Er lässt sich vielmehr mit anonymisierten Daten erfüllen. Die Übermittlung anonymisierter Daten wurde im Gesetzentwurf festgeschrieben.

Das Ministerium hat unsere Vorschläge aufgegriffen. Datenschutzrechtliche Aspekte, wie der Grundsatz der Erforderlichkeit, wurden berücksichtigt. Mit der Aufnahme bereichsspezifischer Vorschriften zum Datenschutz wird der Umgang mit dem Datenschutzrecht erleichtert.

8.2.2 Privatisierung der Arztabrechnung für Sozialhilfeempfänger oder: Wer kontrolliert Was?

Das Sozialamt eines Landkreises plant, die aufwändige Abrechnung medizinischer Leistungen effektiver und damit kostengünstiger zu gestalten. Ein Privatunternehmen mit Sitz außerhalb Brandenburgs soll damit beauftragt werden, die Abrechnung für diejenigen Empfänger von Sozialhilfe und Grundsicherung sowie für Asylbewerber vorzunehmen, die nicht in einer Krankenkasse versichert sind.[61]

Soweit Rechnungen über die medizinische Behandlung von Sozialhilfeempfängern oder Empfängern von Grundsicherung betroffen sind, sind sämtliche Angaben als Sozialdaten durch das Sozialgeheimnis geschützt. Die personenbezogenen Daten der Asylbewerber unterliegen hingegen den allgemeinen datenschutzrechtlichen Bestimmungen. Auf Grund der möglichen Rückschlüsse auf die gesundheitlichen Verhältnisse der Betroffenen ist in jedem Falle von besonders sensitiven Daten auszugehen.

Der Auftragnehmer soll nach den Vorstellungen des Sozialamtes insbesondere die Rechnungen prüfen und die Beträge an die Leistungserbringer (z. B. Ärzte und Zahnärzte) auszahlen. Daneben ist geplant, dass der Auftragnehmer die Rechnungen archiviert und für die Leistungserbringer eine Hotline betreibt.

Nach unserer Auffassung ist die Auslagerung als Datenverarbeitung im Auftrag sowohl für die Sozialdaten als auch für die personenbezogenen Daten der Asylbewerber grundsätzlich zulässig[62]. Sie setzt allerdings voraus, dass der Auftragnehmer eng an die Vorgaben des Auftraggebers gebunden ist und lediglich Hilfstätigkeiten durchführt. Eigene inhaltliche und rechtliche Prüfungen hinsichtlich der zu erbringenden Leistungen darf der Auftragnehmer nicht erbringen. Um dies zu erreichen, waren zahlreiche Änderungen des Vertragsentwurfs erforderlich, die vollständig eingearbeitet wurden.

Die für die Verarbeitung von Sozialdaten im Auftrag einschlägige Vorschrift des § 80 Zehntes Buch Sozialgesetzbuch schreibt darüber hinaus vor, dass beim Auftragnehmer das gleiche Datenschutzniveau herrschen muss wie beim Auftraggeber. Zudem darf ein Auftrag nur erteilt werden, wenn der Auftragnehmer die Arbeiten erheblich kostengünstiger erledigen kann und der überwiegende Teil der Daten beim Auftraggeber gespeichert bleibt. Auch diese Voraussetzungen konnten erfüllt werden.

---

[61] vgl. schon Tätigkeitsbericht 2001, A 8.1.1.2

[62] vgl. auch A 1.2

Schließlich ist der Auftragnehmer verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen. Dies war im vorliegenden Falle insofern schwierig, als der Auftragnehmer ähnliche Aufgaben im Auftrag einer großen Zahl weiterer Kommunen im gesamten Bundesgebiet durchführt und unterschiedliche Vorgaben der Auftraggeber zu berücksichtigen sind. Die von uns insbesondere für erforderlich gehaltene Abschottung der jeweiligen Daten der einzelnen Auftraggeber kann hier dadurch gewährleistet werden, dass die Mitarbeiterinnen und Mitarbeiter des Auftragnehmers nur sehr restriktive Zugriffsrechte auf die einzelnen Abrechnungsdaten haben. Dazu werden die Papierbelege mit einem Barcode versehen. Ausschließlich mit dessen Hilfe ist es möglich, auf die in digitaler Form vorhandenen Daten zuzugreifen. Die damit gegebene Möglichkeit, lediglich auf einen jeweils geringen Teil von Daten allerdings verschiedener Auftraggeber zuzugreifen, wird von uns als ausreichend angesehen. Allerdings darf die Abschottung auf der Ebene der Vorgangsbearbeitung nicht durch eine Allzuständigkeit aller im Call-Center des Dienstleisters Beschäftigten durchbrochen werden. Da dies jedoch der Fall war, haben wir dem Landkreis empfohlen, telefonische Rückfragen der Hilfeempfänger weiterhin selbst zu beantworten.

Zurzeit sind noch einzelne Fragen des technischen und organisatorischen Datenschutzes offen, die noch nicht zufriedenstellend gelöst sind, sodass der Vertrag noch nicht unterzeichnet wurde.

Unabhängig von unserer grundsätzlich positiven materiell-rechtlichen Bewertung sind eine Reihe von formellen Anforderungen zu beachten. Bei der Verarbeitung von Sozialdaten im Auftrag muss der Auftraggeber seine Aufsichtsbehörde rechtzeitig vor Auftragserteilung über seine Pläne umfassend unterrichten. Für die Sozialämter ist hier das Ministerium für Arbeit, Soziales Gesundheit und Frauen zuständig.

Bei der Datenverarbeitung im Auftrag hinsichtlich der Rechnungen der Asylbewerber gilt hingegen das Brandenburgische Datenschutzgesetz, wonach eine Genehmigung des Ministeriums des Innern eingeholt werden muss.

Im vorliegenden Falle haben beide Ministerien unserer Bewertung zugestimmt.

Da der Auftragnehmer zudem auch noch eine nicht-öffentliche Stelle mit Sitz außerhalb Brandenburgs ist, unterliegt dieser der Kontrolle der dortigen Datenschutzaufsichtsbehörde. Sie kann in den Geschäftsräumen des Auftragnehmers auch datenschutzrechtliche Prüfungen vornehmen. Diese Prüfung beschränkt sich hinsichtlich der konkreten Datenverarbeitung im Auftrag allerdings auf die Feststellung der für die datenschutzrechtliche Bewertung re-

levanten Sachverhalte, insbesondere der getroffenen technischen und organisatorischen Maßnahmen.

Die rechtliche Bewertung, ob und in welchem Umfang die Beauftragung als solche zulässig ist, wird ausschließlich durch die für den Auftraggeber zuständigen Behörden – im vorliegenden Falle also durch den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie das Ministerium für Arbeit, Soziales Gesundheit und Frauen – vorgenommen.

Auf Grund der neuesten Entwicklungen durch das Gesundheitsmodernisierungsgesetz[63] wird die beabsichtigte Beauftragung möglicherweise obsolet, da in Zukunft alle Sozialhilfeempfänger in der gesetzlichen Krankenversicherung versichert werden sollen.

Die Beauftragung privater Unternehmen mit der Prüfung und Begleichung von Rechnungen über medizinische Leistungen für Hilfeempfänger kann im Rahmen einer (Sozial-)datenverarbeitung im Auftrag zulässig sein. Dies setzt allerdings einen hohen rechtlichen, organisatorischen und technischen Aufwand voraus. Vor Realisierung eines solchen Projektes sollte eine sorgfältige Prüfung der Wirtschaftlichkeit erfolgen. In jedem Fall sind der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht sowie die zuständigen Aufsichtsbehörden frühzeitig zu beteiligen.

9 Finanzen

9.1 Neues Personenkennzeichen statt Steuernummer

Am 20. Dezember 2003 trat das Zweite Gesetz zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2003) in Kraft[64]. Es enthält eine versteckte, aber weit reichende Ergänzung der Abgabenordnung, wonach zukünftig jedem steuerpflichtigen Einwohner ein Identifikationsmerkmal zugeteilt werden soll, das zentral für die gesamte Bevölkerung der Bundesrepublik beim Bundesamt für Finanzen und zusätzlich in den kommunalen Melderegistern gespeichert wird. Die Meldebehörden haben die Daten jedes Neugeborenen an das Bundesamt für Finanzen weiterzuleiten.

Die neue Identifikationsnummer ist kein bloßer Ersatz für die bisherige Steuernummer. Auch wenn die gesetzlichen Regelungen eine Zweckbindung der Identifikationsnummer für das Besteuerungsverfahren vorsehen, ist festzuhal-

63 vgl. o. A 8.2.1

64 s. BGBl. I S. 2645

ten, dass hier die Daten jedes Säuglings zentral beim Bundesamt für Finanzen gespeichert werden sollen, bevor feststeht, ob dieser überhaupt jemals Steuerpflichtiger wird. Das bisherige Besteuerungsverfahren, das dezentral organisiert ist, rechtfertigt eine zentrale Verwaltung von Identifikationsnummern der gesamten Bevölkerung nicht. Auch unter Berücksichtigung der vorgesehenen Zweckbindungsregelungen ist kein Grund erkennbar, weshalb ein derartiges zentrales Einwohnerregister notwendig sein sollte. Offenbar sollen Datenabgleichsverfahren auf Bundesebene ermöglicht werden, die im bisherigen System des Besteuerungsverfahrens keinen Platz hatten.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist ein Personenkennzeichen mit dem Grundrecht auf informationelle Selbstbestimmung nicht zu vereinbaren.

Mit der Einführung des Identifikationsmerkmals in das Steuer- und Melderecht hat der Bundesgesetzgeber die Grundlage für eine zentrale Erfassung der gesamten bundesdeutschen Bevölkerung gelegt, für die es kein steuerliches Erfordernis gibt und deren Vereinbarkeit mit der Verfassung bezweifelt werden muss.

9.2 Einsichtsrechte eines Gesellschafters: Hat die Finanzverwaltung etwas zu verheimlichen?

Seit mehr als einem Jahr begehrt ein Gesellschafter, der lediglich eine Minderheit der Anteile an einer GmbH hält, erfolglos Akteneinsicht in die bei den Finanzbehörden über ihn und das Unternehmen geführten Akten, um zu prüfen, ob er das Land auf Schadenersatz nach dem Staatshaftungsgesetz in Anspruch nehmen kann.

Der Landesbeauftragte hat die Verweigerung der Akteneinsicht beanstandet. Demgegenüber meint das Ministerium der Finanzen zu Unrecht, der Gesellschafter habe keinen Anspruch auf Einsicht in die unternehmensbezogenen Akten. Es vermag eine enge Verflechtung der Gesellschaft mit dem Gesellschafter in personeller, finanzieller oder wirtschaftlicher Hinsicht nicht zu erkennen. Selbst bei einer Minderheitengesellschaftsbeteiligung können auch personenbezogene Daten des Gesellschafters betroffen sein; auf die Höhe seines Anteils kommt es nicht an. Informationen sind auch dann personenbezogen, wenn sie Rückschlüsse auf die sachlichen Verhältnisse einer Person wie etwa ihr Vermögen zulassen. Die Daten von Mitgesellschaftern sind bei der Einsichtsgewährung nötigenfalls unkenntlich zu machen.

Darüber hinaus hat das Ministerium die unzutreffende Auffassung vertreten, dass Unterlagen, die keinen Bezug zu personenbezogenen Daten haben, nicht der Kontrolle des Landesbeauftragten unterliegen. Ob Daten personen-

bezogen sind, muss der Landesbeauftragte als unabhängige Kontrollinstanz im Rahmen seines gesetzlichen Auftrags selbst überprüfen können. Ansonsten könnte sich die Finanzverwaltung in jedem Fall auf den Standpunkt stellen, dass keine personenbezogenen Daten in den Akten vorhanden seien und somit das Akteneinsichtsrecht von vornherein ohne rechtliche Überprüfung einer Kontrollinstanz ausschließen.

Der Fall zeigt beispielhaft, dass eine Behörde durch Verletzung datenschutzrechtlicher Auskunftspflichten beim Bürger die Annahme auslöst, sie habe etwas (z. B. rechtswidriges Verhalten) zu verbergen. Durch die Gewährung von Akteneinsicht könnte im Gegenteil ein unnötiger Rechtsstreit vermieden werden, wenn der Betroffene feststellt, dass die Verwaltung korrekt gehandelt hat und eine Klage deshalb aussichtslos wäre.

Auch ein geringer Prozentsatz eines Gesellschaftsanteiles kann einen Anspruch des Minderheitsgesellschafters auf Einsicht in die Akten einer GmbH gem. § 18 Abs. 4 Brandenburgisches Datenschutzgesetz begründen.

9.3 Akteneinsicht durch den Landesbeauftragten bei den Finanzbehörden

Ein Beschluss der für die Abgabenordnung zuständigen Referatsleiter der Finanzministerien sieht vor, dass die Finanzbehörden über die Art und Weise von Aktenübersendungsersuchen des Bundes- und der Landesbeauftragten für den Datenschutz „nach pflichtgemäßem Ermessen“ entscheiden sollen.

Dieser Beschluss widerspricht geltendem Recht, da die Finanzbehörden insoweit keinen Ermessensspielraum haben. Nach § 24 Abs. 2, Abs. 4 Nr. 1 und Abs. 6 Bundesdatenschutzgesetz besteht ein von weiteren gesetzlichen Voraussetzungen unabhängiges Kontrollrecht der Datenschutzbehörden des Bundes und der Länder. Das schließt umfassende Auskunftspflichten der Finanzbehörden sowie Akteneinsichtsbefugnisse und Zutrittsrechte der Datenschutzbeauftragten und ihrer Mitarbeiter ein. Die Erteilung von Auskünften und die Gewährung von Akteneinsicht sind Pflichten, die von keiner weiteren Vorentscheidung und von keiner Ermessensausübung der kontrollierten Dienststelle abhängig gemacht werden dürfen. Die landesrechtlichen Datenschutzbefugnisse zur Kontrolle der Landesfinanzbehörden stimmen mit dieser bundesrechtlichen Regelung überein.

Das Kontrollrecht des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht gilt für die Finanzbehörden genauso wie für alle anderen Behörden des Anwendungsbereichs des Brandenburgischen Datenschutzgesetzes. Eine Ermessensentscheidung über das Informationsrecht des Landesbeauftragten steht ihnen nicht zu.

9.4 Darf das Gewerbeamt von Steuerschulden eines Unternehmers erfahren?

Ein Unternehmer hatte erhebliche Steuerschulden. Das Finanzamt versuchte in einem Zeitraum von über sieben Jahren diesen Betrag erfolglos einzutreiben. Schließlich teilte es dem Gewerbeamt die hohen Steuerrückstände des Betroffenen mit und regte an, ein Gewerbeuntersagungsverfahren wegen Unzuverlässigkeit einzuleiten. Als der Betroffene sich an den Landesbeauftragten wandte, verweigerten uns die Finanzbehörden unter Berufung auf das Steuergeheimnis jegliche Auskünfte.

Auch die Steuerrückstände eines Unternehmens unterliegen der Abgabenordnung (AO). Das Finanzamt darf sie dem Gewerbeamt nur mitteilen, soweit hieran ein zwingendes öffentliches Interesse besteht (§ 30 Abs. 4 Nr. 5 AO).

Die Pflichtverstöße des Steuerpflichtigen oder seine Rückstände müssen derart schwer wiegen, dass er sich nicht mehr – oder nur eingeschränkt – wirtschaftlich betätigen darf. Hohe betriebsbedingte Steuerschulden können dazu führen, dass eine gewerberechtliche Unzuverlässigkeit vorliegt und dem Gewerbetreibenden sein Gewerbe untersagt werden kann.

Auf unsere Anfrage nach den für die Entscheidung erheblichen Umständen verweigerte die Oberfinanzdirektion jegliche Auskünfte. Sie begründete dies damit, dass die Vorschrift des § 24 Abs. 2 Nr. 2 i. V. m. Abs. 6 Bundesdatenschutzgesetz die Offenbarung der gem. § 30 AO geschützten Verhältnisse gegenüber dem Landesdatenschutzbeauftragten nicht legitimiere.

Für die Finanzbehörde im Land Brandenburg gilt das Brandenburgische Datenschutzgesetz (BbgDSG) auch dann, wenn sie Bundesrecht (z. B. die Abgabenordnung) ausführt. Ein Vorrang bereichsspezifischer Regelungen in der Abgabenordnung besteht nach § 2 Abs. 3 Satz 2 BbgDSG nur, soweit diese eine Verarbeitung personenbezogener Daten zulassen. Enthalten sie keine Regelungen über die Zulässigkeit, findet das Landesdatenschutzgesetz Anwendung, und zwar neben der Geheimhaltungsvorschrift über das Steuergeheimnis. Da die Abgabenordnung außer dem Steuergeheimnis keine den Sachverhalt betreffende weitere bereichsspezifische Datenschutzregelungen enthält, kann nur durch eine ergänzende Anwendung der materiellen Verarbeitungsbefugnisse des allgemeinen Datenschutzrechts sichergestellt wer-

den, dass die gesamte Datenverarbeitung in der Finanzverwaltung auf der rechtsstaatlich gebotenen gesetzlichen Grundlage stattfindet.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat die mangelnde Kooperation der Oberfinanzdirektion beanstandet. Das Ministerium der Finanzen hat auf Grund dieser Beanstandung das Finanzamt aufgefordert uns die erbetenen Auskünfte zu erteilen.

In der Sache selbst lag kein Verstoß gegen datenschutzrechtliche Vorschriften vor. Das Finanzamt hat dem Gewerbeamt nur die für die Anregung des Gewerbeuntersagungsverfahrens erforderlichen Daten mitgeteilt. Somit durfte das Finanzamt die Höhe der betriebsbedingten Steuerschulden (Umsatzsteuer), das Abgabeverhalten bezüglich der Steuererklärung, die Tatsache der Abgabe der eidesstattlichen Versicherungen und die Schlussfolgerung hieraus dem Gewerbeamt auf Grund des zwingenden öffentlichen Interesses gem. § 30 Abs. 4 Nr. 5 AO übermitteln.

Die Bestimmungen des allgemeinen Datenschutzrechts über die unabhängige Kontrolle durch die Datenschutzbeauftragten sind auch im Geltungsbereich der Abgabenordnung anzuwenden. Folglich ist der Landesbeauftragte auch für die Überprüfung der rechtmäßigen Übermittlung von Steuerdaten zuständig.

Teil B

Akteneinsicht und Informationszugang

1 Entwicklung des Informationszugangsrechts

Die rechtlichen Rahmenbedingungen für den freien Informationszugang haben sich im zurückliegenden Jahr auf europäischer, nationaler und Landesebene höchst unterschiedlich entwickelt.

1.1 Europa

In der Europäischen Union sieht der bisher nicht beschlossene Entwurf des Konvents für eine Europäische Verfassung vom 20. Juni 2003 neben der Verankerung des Transparenzprinzips für die Arbeit der Institutionen die Aufnahme der Europäischen Grundrechtecharta und mit ihr des Rechts aller Unionsbürger auf Zugang zu Dokumenten der Unionsorgane[65] vor.

Am 1. Januar 2004 ist die Richtlinie des Europäischen Parlaments und des Rates über die Weiterverwendung von Dokumenten des öffentlichen Sektors in Kraft getreten[66], die die Zugangsbedingungen zu Informationen des öffentlichen Sektors in der Union angleichen soll, um den Wettbewerb im Binnenmarkt auch in diesem immer wichtiger werdenden Bereich zu garantieren[67]. Diese Richtlinie verpflichtet die Mitgliedstaaten zwar nicht zur Schaffung eines allgemeinen Informationszugangsanspruchs im innerstaatlichen Recht, sondern regelt nur die weitere Verwendung von Informationen, die durch Geltendmachung eines solchen Anspruchs erlangt worden sind. Es besteht aber kein Zweifel daran, dass auch diese Richtlinie die europäische Entwicklung zu mehr Transparenz, die auf der Ebene der Unionsorgane bereits verbindlich festgelegt ist, auch in den Mitgliedstaaten verstärken wird. Auch die jetzt in Kraft getretene Fassung der Richtlinie, die von den Mitgliedstaaten bis zum 1. Juni 2005 umgesetzt werden muss, verpflichtet nicht dazu, bei der Festsetzung von Gebühren für die kommerzielle Verwertung von Informationen des öffentlichen Sektors den kommerziellen Nutzen des Informationsempfängers bei der Gebührenhöhe zu berücksichtigen. Deshalb war und ist eine Änderung des Brandenburgischen Akteneinsichts- und Informationszugangsgesetzes, das bisher diese Berücksichtigung nicht vorsah[68], auch zukünftig vom Unionsrecht nicht vorgeschrieben.

---

[65] Art. I - 49, II - 42; s. dazu Tätigkeitsbericht 2000, Teil B 1.1

[66] s. ABl-EU L 345, 90 f. 31. Dezember 2003

[67] vgl. dazu Tätigkeitsbericht 2002, B 1.1

[68] vgl. dazu näher unten, B 1.3

Gerade bei der Weiterverwendung von Informationen des öffentlichen Sektors für kommerzielle Zwecke kommt der Berücksichtigung des Datenschutzes große Bedeutung zu. Hierzu hat die Gruppe der Europäischen Datenschutzbeauftragten nach Artikel 29 der EG-Datenschutzrichtlinie Kriterien entwickelt, die für die Umsetzung der Richtlinie und ihre Interpretation auf nationaler Ebene eine wichtige Orientierung geben[69]. Die neue Richtlinie zur Weiterverwendung von Informationen des öffentlichen Sektors hat keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und lässt die geltenden Rechtsvorschriften hierzu unberührt. Die Balance zwischen Informationszugang und Datenschutz muss deshalb in jedem Einzelfall sorgfältig bestimmt werden, um unzulässige Beschränkungen sowohl des Grundrechts auf Datenschutz als auch des Grundrechts auf Informationszugang zu vermeiden.

Die Richtlinie zur Weiterverwendung von Informationen des öffentlichen Sektors strebt die Harmonisierung der Zugangsbedingungen auf einem gemeinschaftsweiten Mindestniveau an und lässt ausdrücklich die geltenden Zugangsregelungen der Mitgliedstaaten unberührt. Sie gilt nicht in den Fällen, in denen Bürger oder Unternehmen im Rahmen der Zugangsregelung ein besonderes Interesse am Zugang zu den Dokumenten nachweisen müssen[70].

Nach der Richtlinie sollten die öffentlichen Stellen ermutigt werden, alle ihre Dokumente zur Weiterverwendung bereitzustellen. Für den Fall, dass das nationale Recht keine Fristen für die rechtzeitige Bereitstellung der Dokumente festlegt, müssen die öffentlichen Stellen im Regelfall innerhalb von höchstens zwanzig Arbeitstagen nach Eingang des Antrags dem Antragsteller die Dokumente zur Weiterverwendung bereitstellen. Schließlich ist hervorzuheben, dass die Mitgliedstaaten durch die Richtlinie verpflichtet werden, sicherzustellen, dass praktische Vorkehrungen getroffen werden, die die Suche nach verfügbaren Dokumenten erleichtern, wie vorzugsweise online verfügbare Bestandslisten der wichtigsten Dokumente und Internet-Portale, die mit dezentralisierten Bestandslisten verbunden sind[71].

Auch wenn die Hauptzielrichtung dieser neuen Richtlinie die Angleichung der Zugangsbedingungen und des Gebührenrahmens für die Weiterverwendung bereits zugänglich gemachter Dokumente der öffentlichen Verwaltung ist, lässt die Richtlinie dennoch keinen Zweifel daran, dass die Nutzung von Informationsquellen des öffentlichen Sektors für kommerzielle wie für nicht kommerzielle Zwecke eine wesentliche Voraussetzung für die Entwicklung der Informationsgesellschaft in der Gemeinschaft ist.

---

[69] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A II

[70] Artikel 1 Abs. 3 der Richtlinie

[71] Artikel 9 der Richtlinie

Im Bereich des Zugangs zu Umweltinformationen besteht seit 1990 eine Verpflichtung der Mitgliedstaaten, ihren Bürgerinnen und Bürgern solche Informationen weit gehend zugänglich zu machen. Nachdem die Europäische Gemeinschaft ebenso wie ihre Mitgliedstaaten 1998 die Konvention von Aarhus[72] unterzeichnet hatte, wurden die Rechte auf Zugang zu Umweltinformationen noch stark erweitert. Zur Umsetzung der Aarhus-Konvention ist die Richtlinie über den Zugang der Öffentlichkeit zu Umweltinformationen vom 28. Januar 2003 erlassen worden[73], die bereits bis zum Februar 2005 in nationales Recht umgesetzt werden muss. Neben einer erheblichen Ausweitung des Begriffs der offenzulegenden Umweltinformation wird der Kreis der verpflichteten Stellen sehr viel größer sein. Dazu werden etwa auch Unternehmen der Daseinsvorsorge unabhängig davon zählen, ob sie in Form von Eigenbetrieben oder als juristische Personen des Privatrechts organisiert sind.

Der Ministerausschuss des Europarates hatte bereits im Februar 2002 eine Empfehlung an die Mitgliedstaaten zum Zugang zu amtlichen Dokumenten beschlossen[74]. Da diese Empfehlung keinen rechtsverbindlichen Charakter hat, wird im Europarat mittlerweile über die Möglichkeit diskutiert, eine rechtsverbindliche völkerrechtliche Konvention über den Zugang zu amtlichen Dokumenten zu erarbeiten. Eine solche Konvention hätte erhebliche Auswirkungen auch für die Bundesrepublik, in der auf Bundesebene noch ein allgemeines Informationszugangsrecht fehlt.

Europa bleibt der Motor in Sachen Informationsfreiheit. Die Umweltinformationsrichtlinie und die Weiterverwendungsrichtlinie der EU geben hier wesentliche Impulse, die sich auch beim allgemeinen Informationszugang auf nationaler Ebene auswirken werden.

1.2 Bundesrepublik Deutschland

Fortschritte bei den Arbeiten für ein Informationsfreiheitsgesetz auf Bundesebene, wie es die Koalitionsfraktionen nach der letzten Bundestagswahl erneut vereinbart hatten, waren im vergangenen Jahr nicht zu erkennen. Allerdings hat sich bei einer Internationalen Konferenz der Bertelsmann-Stiftung im April 2003 in Berlin erstmals der Aufsichtsratsvorsitzende eines großen bundesdeutschen Unternehmens für ein solches Gesetz eingesetzt und der Haltung des Bundesverbandes der Deutschen Industrie widersprochen, der das Vorhaben nach wie vor ablehnt. Die Bertelsmann-Stiftung hat zugleich eine Analyse mit dem Titel „Informationsfreiheit und der transparente Staat“

[72] vgl. dazu Tätigkeitsbericht 1998, B 1.1

[73] vgl. dazu Tätigkeitsbericht 2002, B 1.1

[74] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2002, B I

veröffentlicht[75], in der sie mit Recht darauf hinweist, dass ein Informationsfreiheitsgesetz von Anfang an mit den zahlreichen E-Government-Vorhaben verknüpft werden sollte. Im Übrigen hätte ein solches Gesetz auch wesentliche Vorteile für die Wirtschaft, was bisher weit gehend übersehen worden ist. So wie in den meisten demokratischen Ländern Informationsfreiheitsgesetze inzwischen selbstverständlicher Bestandteil der Rechtsordnung sind, sollten sie dies auch in der Bundesrepublik werden.

Anfang Dezember 2003 beschloss die Bundesregierung ein Aktionsprogramm „Informationsgesellschaft Deutschland 2006“[76], in dem sie umfassend die bereits laufenden und demnächst beginnenden Projekte in der Informations- und Kommunikationstechnik und beim E-Government darstellt und ihre weitere Entwicklung skizziert. Es muss befremden, dass in diesem Aktionsprogramm an keiner Stelle von einem Informationsfreiheitsgesetz für Deutschland die Rede ist.

Positiv hebt sich davon der Beschluss des Deutschen Bundestages vom 12. Dezember 2003 ab, in dem die Bundesregierung auf Antrag der Fraktionen der SPD und von Bündnis 90/Die Grünen[77] aufgefordert wird, möglichst rasch einen Entwurf eines Informationsfreiheitsgesetzes für den Zugang von Bürgerinnen und Bürgern zu amtlichen Informationen der Behörden vorzulegen und darüber hinaus zu prüfen, ob und in welcher Form eine Erweiterung des Grundrechtskatalogs hinsichtlich positiver Kommunikations- und Zugangsrechte sinnvoll ist.

Der Entwurf eines Informationszugangsgesetzes des Bundes sollte aus der Mitte des Deutschen Bundestages vorgelegt werden, wenn die Bundesregierung dieses für die Informationsgesellschaft zentrale Vorhaben weiter dilatorisch behandelt.

1.3 Brandenburg

Im Juli 2003 wurde bekannt, dass das Ministerium des Innern in einem Arbeitsentwurf für das Zweite Gesetz zur Entlastung der Kommunen von pflichtigen Aufgaben einschneidende Beschränkungen des Akteneinsichtsrechts plante. So sollte die Akteneinsicht in all den Fällen ausgeschlossen werden, in denen sie von der Zustimmung bestimmter Behörden, Personen oder Unternehmen abhängt. Personenbezogene Daten sollten im Rahmen der Akteneinsicht selbst dann nicht offenbart werden dürfen, wenn die betroffenen Personen dem zugestimmt hätten. Im Zusammenhang damit sollte auch die

[75] verfügbar unter http://www.begix.de/informationsfreiheit

[76] s. BR-Drs. 976/03

[77] s. BT-Drs. 15/1988

Verpflichtung der Verwaltung (nicht nur der Kommunen) entfallen, auf Verlangen des Antragstellers die Zustimmung dritter Stellen oder Personen einzuholen, von denen die Akteneinsicht abhängt. Außerdem sah der Arbeitsentwurf vor, dass bei der Gebührenfestsetzung für die Akteneinsicht die Bedeutung oder der sonstige Nutzen des Informationszugangs für den Antragsteller berücksichtigt werden sollte. Schließlich enthielt der Entwurf eine klarstellende Regelung für die Erhebung von Gebühren und Auslagen durch Gemeinden und Gemeindeverbände.

Der Landesbeauftragte wandte sich daraufhin an den Ministerpräsidenten und den Innenminister und wies daraufhin, dass ein Ausschluss der Akteneinsicht in allen Fällen der Drittbetroffenheit mit dem Grundrecht auf Akteneinsicht nach Artikel 21 Abs. 4 der Landesverfassung nicht zu vereinbaren wäre. Zudem würde die Aufnahme neuer unbestimmter Rechtsbegriffe wie „der Bedeutung oder des sonstigen Nutzens für den Antragsteller“ die Kommunen und die Verwaltung insgesamt vor zusätzliche Auslegungsprobleme stellen, da sie keine Möglichkeit hätten, hierüber gesicherte Erkenntnisse zu gewinnen. Bis Ende 2003 war die geltende Gebührenordnung zum Akteneinsichts- und Informationszugangsgesetz befristet, um praktische Erfahrungen zu sammeln. Die Evaluation dieser Gebührenordnung sollte abgewartet werden, bevor die gesetzliche Gebührenregelung abgeändert werde.

Der Landesbeauftragte hat zudem Zweifel geäußert, ob das Gesetz, das entgegen seinem Titel die Entlastung nicht nur der Kommunen, sondern auch der gesamten Landesverwaltung im Bereich der Akteneinsicht bezweckte, zu einer wirklichen Entlastung führen würde. Stattdessen sollten die Ausnahmetatbestände kritisch überprüft und möglichst reduziert werden, wozu der Landesbeauftragte Ende 2000 umfangreiche Vorschläge gemacht hat.

In dem von der Landesregierung beschlossenen Gesetzentwurf blieben unsere Kritikpunkte nahezu unbeachtet und außerdem sah dieser von einer Umsetzung eines Landtagsbeschlusses ab, der die Einführung einer Bearbeitungsfrist und den Hinweis abschlägig beschiedener Antragsteller auf das Recht, den Landesbeauftragten für das Recht auf Akteneinsicht anzurufen, vorgesehen hatte.

Im Anschluss an eine öffentliche Anhörung im Ausschuss für Inneres zu diesem Gesetzentwurf, bei der der Landesbeauftragte seine Kritik erläuterte, brachten die Fraktionen der SPD und der CDU einen gemeinsamen Änderungsantrag im Innenausschuss ein, der die Berücksichtigung des Landtagsbeschlusses vom April 2002 und die Streichung der Kriterien „Bedeutung und sonstiger Nutzen für den Antragsteller“ vorsah. Der Landtag verabschiedete in seiner Sitzung am 11. Dezember 2003 – offenbar auf Grund eines Versehens – die Änderung des Akteneinsichts- und Informationszugangsgesetzes

in einer Fassung, die zwar den Landtagsbeschluss vom April 2002 berücksichtigte, nicht aber die Streichung der Gebührenerhebung unter Berücksichtigung des Nutzens für den Antragsteller[78].

Es ist zu begrüßen, dass der Landtag den Versuch der Landesregierung, seinen Beschluss vom April 2002 zur Stärkung des Akteneinsichtsrechts zu übergehen, nicht hingenommen hat. Mit der Einführung einer einmonatigen Bescheidungsfrist für Anträge auf Akteneinsicht ist zugleich ein Gleichklang mit den Regelungen der Gemeindeordnung erzielt worden. Die Verwaltung hat zudem einen Zwischenbescheid zu erteilen, wenn sie nicht innerhalb eines Monats über den Antrag entscheiden kann. Akteneinsicht kann künftig auch per E-Mail beantragt werden[79]. Positiv zu bewerten ist auch die Tatsache, dass der Antragsteller in einem Ablehnungsbescheid zukünftig auf sein Recht hinzuweisen ist, den Landesbeauftragten für das Recht auf Akteneinsicht anzurufen.

Welche Konsequenzen die Streichung der Pflicht der Verwaltung zur Einholung der Zustimmung Dritter in der Praxis haben wird, ist noch nicht abzusehen. Der Landesbeauftragte hat im Gesetzgebungsverfahren darauf hingewiesen, dass ein Antragsteller, der Akteneinsicht begehrt, nicht wissen kann, bei wem etwaige Zustimmungen eingeholt werden müssen. Die Akten führende Stelle ihrerseits darf dem Antragsteller Namen und Anschriften der Dritten nicht ohne deren Zustimmung mitteilen, wenn es sich nicht um Behörden anderer Bundesländer handelt. Also hat die Verwaltung nur zwei Möglichkeiten: Entweder sie führt ein aufwändiges Adressmittlungsverfahren durch, bei dem sie dem Antragsteller anbietet, seine Bitte um Erteilung der Zustimmung an den Dritten zu adressieren und weiterzuleiten, oder sie lehnt den Antrag ohne Weiteres ab. Das aber liefe auf eine unzulässige Verkürzung des Grundrechts auf Akteneinsicht hinaus.

Hinzu kommt, dass der Akten führenden Stelle bei der möglicherweise erforderliche Einholung der Zustimmung Dritter (auch der Behörden anderer Bundesländer, wenn in deren Akten Einsicht genommen werden soll) kein Ermessen zusteht. Sie ist vielmehr aus rechtsstaatlichen Erwägungen auch dann verpflichtet, diese Zustimmung einzuholen, wenn das Gesetz es nicht ausdrücklich vorschreibt. In Brandenburg sieht die Landesverfassung ein Grundrecht auf Akteneinsicht vor. Daher dürfen Behörden, bei denen Akteneinsicht beantragt wird, deren Zulässigkeit von der Zustimmung Dritter abhängt, den Bürger nicht einfach „ins Leere“ laufen lassen, sondern müssen alle Anstrengungen unternehmen, um die Akteneinsicht im gesetzlichen

[78] s. GVBl. I, S. 294

[79] Art. 6 des Gesetzes zur Anpassung verwaltungsrechtlicher Vorschriften an den elektronischen Rechtsverkehr, GVBl. 2003 I, 298

Rahmen zu ermöglichen. Dazu zählt auch die Einholung der Zustimmung Dritter.

Bezüglich der Änderung der Kriterien für die Gebührenfestsetzung, die der Landtag abweichend von der tatsächlichen, aber nicht dokumentierten Beschlussfassung im Innenausschuss verabschiedet hat, ist eine kurzfristige Korrektur der Gesetzesänderung durch den Gesetzgeber wünschenswert. Der Landesbeauftragte hat sich in diesem Sinne an den Vorsitzenden des Ausschusses für Inneres gewandt.

Die Gebührenordnung zum Akteneinsichts- und Informationszugangsgesetz, die bis Ende 2003 befristet war, ist ohne inhaltliche Änderung (lediglich unter Berücksichtigung der Euro-Umstellung) in ihrer Geltung um zwei Jahre verlängert worden[80].

Der Gesetzgeber hat schließlich im Haushaltssicherungsgesetz 2003 einen Vorschlag des Landesbeauftragten aufgegriffen, indem er angeordnet hat, dass alle Gesetze, Verordnungen und Verwaltungsvorschriften bis Ende 2004 elektronisch zu erfassen sind und Verwaltungsvorschriften ihre Geltung verlieren sollen, wenn Sie bis zu diesem Zeitpunkt nicht elektronisch erfasst und durch den Adressaten abrufbar sind[81]. Die ebenfalls vorgesehene Verpflichtung zur Einstellung geltender Rechtsvorschriften ist allerdings nur auf solche Verwaltungsvorschriften erstreckt worden, die mittelbare Außenwirkung besitzen. Zudem kann eine Einstellung von Verwaltungsvorschriften im Internet unterbleiben, wenn Geheimhaltungsinteressen entgegenstehen. Der Landesbeauftragte hatte vorgeschlagen, dass eine Bereitstellung zum Abruf nur dann unterbleiben sollte, wenn Geheimhaltungsinteressen überwiegen.

Die jüngste Änderung des Akteneinsichts- und Informationszugangsgesetzes bringt in zwei Punkten Verbesserungen der Rechtsstellung von Bürgerinnen und Bürgern, in dem eine Bescheidungsfrist und der Hinweis auf den Landesbeauftragten im Fall der Ablehnung vorgesehen wird. Eine wirkliche Entlastung der Verwaltung könnte erreicht werden, indem der Ausnahmenkatalog des Gesetzes kritisch überprüft und verkürzt würde.

[80] s. GVBl. 2003 II S. 706

[81] § 11 Abs. 2 des Gesetzes über Ziele und Vorgaben zur Modernisierung der Landesverwaltung (Artikel 2 des Haushaltssicherungsgesetzes 2003), GVBl. I S. 194, 198

2 Umsetzung des AIG

2.1 Eingaben und Anfragen beim Landesbeauftragten

Die Beschwerden und Fragen zum Informationszugang, mit denen sich der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht befasst, sind zwar nicht repräsentativ für die gesamte Nutzung des Akteneinsichtsrechts in Brandenburg. Sie weisen jedoch auf die Schwerpunkte der Gesetzesanwendung hin.

Während die Anzahl der Eingaben im Berichtszeitraum nur geringfügig angestiegen ist, nahm die Anzahl der Fälle, in denen Unklarheiten hinsichtlich der anzuwendenden Rechtsgrundlage für die Akteneinsicht bestehen, erheblich ab: So stellte sich in den Vorjahren noch häufig heraus, dass die Akten führenden Stellen eigentlich das Verwaltungsverfahrensgesetz für das Land Brandenburg oder das Umweltinformationsgesetz hätten anwenden müssen. Mittlerweile jedoch hat der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes sowie dessen Abgrenzung zu anderen Einsichtsgrundlagen in den brandenburgischen Behörden weitere Bekanntheit gefunden.

Erhöht haben sich im Jahre 2003 auch die Aussichten, öffentliche Stellen, die zunächst den Informationszugang verweigern, von ihrer Verpflichtung zu überzeugen, vollständig oder teilweise Akteneinsicht zu gewähren. Immerhin konnte dieses Ergebnis in 87% der im Berichtszeitraum abgeschlossenen Fälle erreicht werden, deren Ergebnis uns bekannt wurde. Bei einem Zehntel der gesamten Beschwerden mussten wir den Antragstellern allerdings mitteilen, dass die Verwaltungen ihre Einsichtsbegehren zu Recht abgelehnt haben, weil gesetzliche Ausschlussgründe einer Akteneinsicht entgegenstanden.

Nach wie vor sind die meisten Antragsteller interessierte Bürgerinnen und Bürger. Ein Drittel der Eingaben stammt wie bereits im Vorjahr von Bürgerinitiativen oder ähnlichen Vereinigungen. Die überwiegende Mehrheit der Unterlagen, für die sich die Antragsteller interessierten, waren Akten aus den Bauverwaltungen. Hier entstanden auch die meisten Konflikte, da Bauakten häufig personenbezogene Daten enthalten, deren Aussonderung in der Praxis Probleme aufwerfen kann.

Obwohl die öffentlichen Stellen in Brandenburg das Akteneinsichts- und Informationszugangsgesetz immer routinierter anwenden, kommt es vor, dass der Informationszugang zu Unrecht abgelehnt wird. Der Landesbeauftragte geht den Beschwerden betroffener Antragsteller nach und setzt sich gegenüber den öffentlichen Stellen für die Wahrung des Rechts auf Akteneinsicht ein. Er berät die Verwaltungen aber auch im Vorfeld der Bearbeitung von Einsichtsanträgen.

2.2 Informationszugang trotz „behördeninterner" Dokumente?

Nachdem ein Antragsteller Einsicht in sämtliche Akten zu einem Sportstadion nehmen konnte, bat er die Akten führende Stelle um Fotokopien bestimmter Seiten. Diese wurden ihm zugesichert. Das Verlangen nach Kopien wurde von der Stadt als separater Antrag auf Akteneinsicht behandelt, jedoch später mit Verweis auf den angeblichen Schutzbedarf der darin vorhandenen Informationen abgelehnt. Daraufhin wollte der Antragsteller erneut in die Unterlagen einsehen, da er die fraglichen Seiten nur überflogen und sich darauf verlassen hatte, die Kopien zu Hause in Ruhe auswerten zu können. Auch dies wertete die Stadt als separaten Antrag auf Akteneinsicht. Die Akten führende Stelle erließ fast zeitgleich einen Bescheid zur vollständigen Gewährung der Einsicht in die Gesamtakte. Eine Terminvereinbarung zur erneuten Einsichtnahme lehnte sie jedoch mit der Begründung ab, sie habe die Akten noch nicht auf ihren Schutzbedarf geprüft und es sei noch nicht über den Widerspruch des Antragstellers gegen die Verweigerung der Kopien entschieden worden. Während der Antragsteller Klage erhob, um die zugesicherte Akteneinsicht durchzusetzen, lehnte die Stadt sein Begehren hinsichtlich der Kopien mit der Begründung ab, ihm stünden überwiegende öffentliche Interessen – insbesondere der Schutz des internen Willensbildungsprozesses – entgegen.

Dieses Verfahren gestaltete sich mittlerweile dermaßen unübersichtlich und dauerte bereits fast ein halbes Jahr, sodass wir uns in Gesprächen mit der Behörde und dem Antragsteller um eine Interessenvermittlung bemühten. Wir begutachteten die fraglichen Dokumente und kamen zu dem Ergebnis, dass keine öffentlichen Interessen einer Herausgabe entgegenstanden. Sie enthielten lediglich Unterlagen zur Sachstandsermittlung, Telefonvermerke sowie fachbezogene Vermerke, die beispielsweise anderen Verwaltungsbereichen als Zuarbeit dienten. Insbesondere ließ die Akte keine Rückschlüsse auf den Prozess der Willensbildung innerhalb der Behörde i. S. v. § 4 Abs. 2 Nr. 1 Akteneinsichts- und Informationszugangsgesetz zu, wie die Stadt meinte. Diese Ausnahme beschränkt sich nämlich auf den eigentlichen Willensbildungsprozess, nicht aber auf Stellungnahmen, Gutachten, Zuarbeiten oder

ähnliche, herkömmlich als „intern“ bezeichnete Dokumente. Zwischen dem unmittelbaren Zustandekommen einer Entscheidung und den ihr zu Grunde liegenden selbständigen Entscheidungsgrundlagen ist somit zu unterscheiden.

Der Umgang der Behörde mit dem Antrag auf Akteneinsicht macht deutlich, dass die Unterlagen, in die Einsicht beantragt wird, vor der Durchführung der Akteneinsicht zu prüfen sind. Hier ist die Stadt offenbar erst darauf aufmerksam geworden, dass es sich um schutzbedürftige Daten handeln könnte, als der Antragsteller Kopien der eingesehenen Unterlagen verlangte. Ein qualitativer Unterschied zwischen der Offenlegung von Akten und der Herausgabe von Kopien besteht jedoch nicht; vielmehr ist beides vom Recht auf Informationszugang umfasst[82]. Außerdem ist das Verlangen von Fotokopien bereits eingesehener Unterlagen nicht als gesonderter Antrag auf Informationszugang anzusehen, um die Übersichtlichkeit des Verfahrens zu gewährleisten.

Das Ergebnis unserer Begutachtung teilten wir der Akten führenden Stelle mit, die dem Antragsteller daraufhin die gewünschten Kopien übersandte.

Behördeninterne Schreiben unterliegen nicht alleine schon deshalb dem Ausnahmetatbestand der „internen Willensbildung“, weil sie innerhalb der Behörde verbleiben. Gutachten, Stellungnahmen, Zuarbeiten oder ähnliche Informationen, die lediglich eine Entscheidungsgrundlage darstellen, sind davon nicht betroffen. Es ist vielmehr gerade der Zweck des Akteneinsichts- und Informationszugangsgesetzes, diese zugänglich zu machen.

2.3 Transparenz beim Verkauf kommunaler Grundstücke

Im Rahmen einer Ausschreibung für den Verkauf eines gemeindeeigenen Grundstücks beabsichtigte ein Bieter, das Zustandekommen der Verkaufsentscheidung bzw. seine Vermutung, es könne Amtsmissbrauch und Korruption im Spiel gewesen sein, zu überprüfen. Das zuständige Amt stellte die Gewährung der Akteneinsicht lediglich nach umfangreicher Schwärzung in Aussicht. Diese hätte zur Folge gehabt, dass inhaltliche Zusammenhänge aus den Unterlagen kaum noch erkennbar gewesen wären.

Um uns ein Bild von dem geltend gemachten Schutzbedarf der Daten machen zu können, haben wir die strittige Akte angefordert und überprüft. Dabei stellte sich heraus, dass ein Großteil der Dokumente keineswegs schutzbedürftige Daten enthielt und somit offen zu legen war. Allerdings wiesen insbesondere die Informationen über die Bieter einen eindeutigen Schutzbedarf

[82] vgl. auch Tätigkeitsbericht 2002, Teil B 2.8

auf. Eine einfache Anonymisierung, d. h. eine Schwärzung der Namen der Bieter, schied aus, da der gegebene Zusammenhang noch immer Rückschlüsse auf deren Identität zugelassen hätte. Wir haben dem Amt daher empfohlen, die einzelnen Bieter beispielsweise mit Pseudonymen wie „Bieter A“, „Bieter B“ etc. zu kennzeichnen und ihre Angebote anstatt mit dem tatsächlich gebotenen Betrag mit Klassifizierungen wie „höchstes Gebot“, „niedrigstes Gebot“ etc. zu versehen. Damit wäre ein wesentlicher Aspekt der Informationen für den Antragsteller zugänglich gewesen, ohne dass Daten mit Bezug zu den Betroffenen offenbart würden. In Anbetracht der geringen Zahl der Bieter wäre durch dieses Vorgehen auch kein unvertretbarer Aufwand entstanden.

Indem der Antragsteller angab, seinen Verdacht auf Amtsmissbrauch und Korruption überprüfen und auf rechtmäßige Zustände in der Kommunalpolitik und -verwaltung hinwirken zu wollen, ohne die entstandenen Eigentumsverhältnisse infrage zu stellen, machte er einen politischen Mitgestaltungswillen nach § 5 Abs. 2 Nr. 3 Akteneinsichts- und Informationszugangsgesetz (AIG) geltend. Danach kann die Akteneinsicht gewährt werden, wenn auf Grund besonderer Umstände des Einzelfalls das Offenbarungsinteresse des Antragstellers das Geheimhaltungsinteresse der betroffenen Personen überwiegt. Wir haben der Behörde daher empfohlen, die Betroffenen zunächst nach § 6 Abs. 3 AIG anzuhören und deren Stellungnahme mit dem nach § 6 Abs. 1 Satz 2 AIG einzuholenden Einsichtsinteresse des Antragstellers abzuwägen. Dem Amt obliegt eine Entscheidung nach eigenem, pflichtgemäßen Ermessen. Kommt es zu dem Schluss, dass das Einsichtsinteresse überwiegt, kann es die Daten auch personenbezogen weitergeben.

Darüber hinaus kann der Antragsteller von der Behörde die Einholung der Zustimmung der Betroffenen verlangen[83]. Im Unterschied zur Anhörung ist die Verwaltung dabei an die Entscheidung der Betroffenen gebunden. Im Falle einer positiven Entscheidung der Betroffenen kann so der Aufwand der Aussonderung schutzbedürftiger Daten vermieden werden. Ist bereits eine Anhörung erfolgt, erübrigt sich in der Regel die Frage nach der Zustimmung.

Soweit einzelne Informationen ausgesondert werden müssen, handelt es sich um eine teilweise Ablehnung des Antrags auf Informationszugang. Die Akten führende Stelle hat in diesem Fall die Ablehnung im Einzelnen schriftlich zu begründen. Ein Bescheid sollte zunächst eine Übersicht über die auf ihre Einsehbarkeit geprüften Dokumente enthalten. Dabei ist auf eine nachvollziehbare Nummerierung der Seiten zu achten. Jedes Dokument ist nach den Vorgaben des AIG zu bewerten und das Ergebnis (z. B. Offenlegung, teilweise Aussonderung, Reduzierung des Einsichts- auf ein Auskunftsrecht) – ebenfalls bezogen auf die einzelnen Dokumente – darzustellen. Eine ent-

[83] Das gilt auch nach der Änderung des AIG mit Wirkung vom 1. Februar 2004, s. o. B 1.3.

sprechende Bewertung der Akte haben wir vorgenommen und dem zuständigen Amt überlassen, das unsere Empfehlungen umgesetzt hat.

Genügt die Schwärzung von Namen nicht, um den Schutzbedarf von Daten der Bieter im Rahmen einer Grundstücksausschreibung zu gewährleisten, kommt eine Pseudonymisierung sämtlicher Personendaten infrage. Allerdings hat die Behörde nach pflichtgemäßem Ermessen zu entscheiden, ob solche Daten personenbezogen offen gelegt werden können, soweit der Antragsteller schlüssig geltend macht, durch die Akteneinsicht Unregelmäßigkeiten in der kommunalen Politik und Verwaltung aufdecken zu wollen.

2.4 „Akte“ und „Verfahren“ – Der kleine Unterschied

Auf einer Liegenschaft der Gemeinde wurde eine Mobilfunkanlage errichtet. Ein Einwohner des Dorfes bemühte sich bei der Amtsverwaltung um Zugang zu den dort vorhandenen Unterlagen. Das Amt teilte ihm zwar mit, dass es über eine Akte verfüge, forderte ihn jedoch auf, sich an die Bauaufsichtsbehörde des Landkreises zu wenden. Diese sei als Akten führende Stelle für den Informationszugang zuständig und verfüge auch über die Stellungnahme der Gemeinde.

Das Akteneinsichts- und Informationszugangsgesetz (AIG) enthält keine Vorgaben zur Zuständigkeit für den Informationszugang für den Fall, dass mehrere Behörden oder Gebietskörperschaften fachlich an einem Vorgang beteiligt sind. Vielmehr kommt es darauf an, bei welcher Akten führenden Stelle die Informationen vorhanden sind. Das Führen einer Akte bedeutet dabei nicht, dass diese Stelle das Verfahren auch federführend bearbeitet (wie dies im vorliegenden Fall die Bauaufsichtsbehörde tat). Deutlicher formuliert das hier ebenfalls in Betracht kommende Umweltinformationsgesetz, dass jeder einen Anspruch auf freien Zugang zu Informationen über die Umwelt hat, die „bei einer Behörde (...) vorhanden sind“. Das Amt war also verpflichtet, die ihm vorliegenden Informationen – soweit zulässig – offen zu legen, auch wenn es nicht Herr des Verfahrens ist.

Selbst wenn das Amt nicht über Unterlagen verfügt hätte, d.h. nicht für die Akteneinsicht zuständig gewesen wäre, hätte es sich bei einem bloßen Verweis auf die Bauaufsichtsbehörde schon alleine deshalb um einen Verstoß gegen § 6 Abs. 1 Satz 6 AIG gehandelt, weil diese die unzuständige Behörde verpflichtet, den Antrag unverzüglich an die zuständige Stelle weiterzuleiten und den Antragsteller hierüber zu unterrichten. Die Verwaltung sollte nicht den Bürger, sondern seinen Antrag „laufen“ lassen. Diese Unterstützung des Antragstellers ist jedoch unterblieben.

Zu Recht wies das Amt uns aber darauf hin, dass ein Nachbar nach § 64 Abs. 4 Brandenburgische Bauordnung das Recht hat, die vom Bauherrn eingereichten Bauvorlagen bei der Bauaufsichtsbehörde einzusehen. Sollte der Antragsteller Nachbar gewesen sein, hätte ihm dies jedoch unter Darlegung der Rechtsgrundlage mitgeteilt werden müssen. Nur in diesem Fall wäre der Landkreis zuständig und der Verweis rechtmäßig gewesen.

Die Zuständigkeit für die Bearbeitung eines Antrags auf Akteneinsicht obliegt der Stelle, bei der die beantragten Informationen vorhanden sind. Es kommt nicht darauf an, ob diese das zu Grunde liegende Verfahren führt.

2.5 Nicht-öffentliche Sitzung einer Gemeindevertretung

Vor zehn Jahren hatte die Gemeindevertretung in nicht-öffentlicher Sitzung beschlossen, den Baurechtsvertrag mit einem Investor zu ändern. Der Eigentümer einer davon betroffenen Wohnung hielt die infolge der Vertragsänderung höhere Erbzinslast gegenüber der Gemeinde, die Eigentümerin des Grundstücks ist, für unzulässig und beantragte eine Fotokopie des Beschlusses der Gemeindevertretung, um den Vorgang zu prüfen. Zunächst beabsichtigte die Gemeinde, den Antrag abzulehnen.

Zwischen der Niederschrift einer nicht-öffentlichen Sitzung der Gemeindevertretung und dem aus ihr resultierenden Beschluss ist zu unterscheiden: Während sämtliche Beschlüsse nach § 49 Abs. 5 Gemeindeordnung grundsätzlich in ortsüblicher Weise bekannt zu machen sind, gilt dies nicht für die Protokolle der nicht-öffentlichen Sitzungen. Auch diese können jedoch offen gelegt werden, wenn das Interesse an der Einsichtnahme das entgegenstehende öffentliche Interesse im Einzelfall überwiegt (§ 4 Abs. 2 Akteneinsichts- und Informationszugangsgesetz). Hierzu ist das Einsichtsinteresse des Antragstellers einzuholen und gegen das öffentliche Geheimhaltungsinteresse abzuwägen. Wird das Geheimhaltungsinteresse von vornherein als geringfügig eingestuft, kann auf die Einholung des Einsichtsinteresses verzichtet und das Protokoll offen gelegt werden.

Im vorliegenden Fall interessierte sich der Antragsteller allerdings nicht für das Protokoll, sondern lediglich für den Beschluss. Da aus diesem weder personen- noch unternehmensbezogene Daten hervorgingen und er ohnehin zum Zeitpunkt seiner Fassung bekannt gemacht wurde, stand der Herausgabe einer Fotokopie nichts entgegen. Ein Verweis auf die Quelle der ursprünglichen Veröffentlichung vor zehn Jahren ist hingegen nicht zulässig, da dem Antragsteller eine Recherche nach so langer Zeit nicht mehr zuzumuten ist.

Nachdem wir die Gemeinde auf die Rechtslage hingewiesen haben, hat der Antragsteller die gewünschte Fotokopie erhalten.

Die Beschlüsse von nicht-öffentlichen Gemeindevertretersitzungen sind grundsätzlich offen zu legen, während Protokolle dieser Sitzungen nur bei einem überwiegendem Einsichtsinteresse des Antragstellers herausgegeben werden müssen.

2.6 Planungsunterlagen: Einmal ausgelegt, für immer verschlossen?

Ein Einwohner wollte Einsicht in Unterlagen zum ländlichen Wegebau nehmen, um sich über die Planungen in der Umgebung seines Ortes zu informieren. Die Akten führende Stelle teilte ihm daraufhin mit, dass eine Einsicht nicht möglich sei, weil die Planungsunterlagen lediglich während der Auslegung im Rahmen der Bürgerbeteiligung zugänglich seien und verwies für weitere Auskünfte an den Planungsträger.

Das Recht auf Informationszugang beschränkt sich nicht auf bestimmte Planungsphasen. Zwar bedarf es während der Phase der Auslegung von Planungsunterlagen keines gesonderten Antrages auf Akteneinsicht, da diese innerhalb einer bestimmten Frist jederzeit möglich ist. Jedoch bedeutet dies nicht, dass der Informationszugang nach Abschluss der Auslegungsfrist verwehrt werden müsste. Hier gelten vielmehr die Regelungen des Akteneinsichts- und Informationszugangsgesetzes oder, falls Umweltinformationen betroffen sind, des Umweltinformationsgesetzes.

Soweit die Akten führende Stelle selbst über Planungsunterlagen verfügt, ist der Verweis auf den Planungsträger oder auf andere Behörden unzulässig. Sind hingegen keine Akten vorhanden, ist sie verpflichtet, den Antrag an die zuständige Stelle weiterzuleiten und den Antragsteller hierüber zu informieren.

Die Einsicht in die Planungsunterlagen wurde nach unseren Hinweisen auf die Rechtslage umgehend gewährt.

Auch nach dem Ende der öffentlichen Auslegung von Planungsunterlagen im Rahmen der Bürgerbeteiligung besteht jederzeit ein Recht auf Informationszugang.

2.7 Ein Rechtsanwalt entscheidet für eine Gemeinde

In unmittelbarer Nähe ihres Grundstücks errichtete eine Gemeinde eine Abwasserpumpstation sowie Schaltkästen, um deren Verlegung sich die Eigentümer bemühten. Mit Hilfe ihres Anwalts begehrten sie gegenüber

der Gemeinde Einsicht in die entsprechenden Verwaltungsvorgänge. Die Gemeinde beauftragte ihrerseits einen Rechtsanwalt, der den Antragstellern mitteilte, dass ein Informationszugang nur im Falle einer rechtlichen Begründung infrage komme.

Das Recht auf Akteneinsicht nach dem Akteneinsichts- und Informationszugangsgesetz gilt ohne Voraussetzung für alle Interessierten. Dies bedeutet, dass eine Begründung des Einsichtsbegehrens grundsätzlich nicht verlangt werden darf. Die Ablehnung des Antrags wäre also nur infrage gekommen, wenn gesetzliche Ausnahmegründe geltend gemacht worden wären.

Ein Antrag auf Akteneinsicht löst ein Verwaltungsverfahren aus, das sich, sofern keine vorrangigen Anspruchsgrundlagen vorhanden sind, nach dem Akteneinsichts- und Informationszugangsgesetz richtet. Die Entscheidung über einen solchen Antrag liegt bei der Akten führenden Stelle, in diesem Fall bei der Gemeinde. Dabei handelt es sich um einen Verwaltungsakt, der die erlassende Behörde erkennen lassen muss. Deren Entscheidung kann nicht einem Rechtsanwalt übertragen werden. Sofern die Antragsteller sich mit ihrem Begehren direkt an einen von der Gemeinde mit der Beratung beauftragten Rechtsanwalt wenden, hat dieser den Antrag zur Entscheidung an die Gemeinde weiterzuleiten. Wird der Anwalt von der Gemeinde mit einer rechtlichen Bewertung beauftragt, muss dem Bescheid dennoch zu entnehmen sein, dass die Behörde die Entscheidung selbst getroffen hat.

Die Gemeinde kann einen Rechtsanwalt mit der rechtlichen Vorbereitung einer Entscheidung zur Akteneinsicht beauftragen. Allerdings muss sie die Entscheidung selbst treffen und ihre Verantwortung und Zuständigkeit auch im Bescheid erkennen lassen.

Teil C

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Wie die Datenschutzbeauftragten im Bund und in den übrigen Ländern stand und steht der Landesbeauftragte in Brandenburg vor der Aufgabe, mit knappsten personellen und sachlichen Mitteln die gesetzlichen Aufgaben bestmöglichst zu erfüllen. Dabei muss er allerdings mit erheblich geringeren Mitteln auskommen als vergleichbare Einrichtungen in Ländern einer vergleichbaren Größe und Verwaltungsstruktur. Die Dienststelle in Brandenburg hat wie in allen anderen Bundesländern Verwaltungseinheiten zu beraten und zu kontrollieren, die über ein Vielfaches an Personal verfügen und deren EDV-Ausstattung ständig komplexer wird.

Auch die ständige Zunahme der Verarbeitung von Personendaten hoher Sensitivität und der wachsende Vernetzungsgrad zwingen dazu, stets zu überprüfen, ob die notwendigen Mittel zur Erfüllung der gesetzlichen Aufgaben vorhanden sind. Dabei sind auch in unserer Dienststelle naturgemäß die gleichen Überlegungen der Aufgabenkritik anzustellen, die für die Landesregierung nach dem Verwaltungsmodernisierungsgesetz[84] verbindlich sind. Der Landtag hat es allerdings zu Recht abgelehnt, die gesetzlichen Verpflichtungen aus dem Verwaltungsmodernisierungsgesetz auf den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu erstrecken, weil dies mit der Unabhängigkeit seiner Stellung nicht zu vereinbaren gewesen wäre.

Die Europäische Kommission hat in ihrem Bericht über die Durchführung der Datenschutzrichtlinie vom Mai 2003 betont, dass eine unzureichende Ausstattung der Datenschutzbeauftragten deren Unabhängigkeit beeinträchtigen kann[85]. Vor diesem Hintergrund und angesichts des bevorstehenden verstärkten Einsatzes neuer Verfahren zur Verarbeitung biometrischer und anderer personenbezogener Daten ist eine Verbesserung der Personalausstattung der Dienststelle des Landesbeauftragten notwendig.

Gegen Ende des Berichtszeitraumes trat erneut eine Dienstkraft der ersten Stunde, die Dipl.-Betriebswirtin Ursel Leunig, in den Ruhestand. Zudem wur-

---

[84] s. GVBl. 2003 I S.195

[85] Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95746) v. 15. Mai 2003, http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_de.htm

de ein besonders qualifizierter Mitarbeiter im Bereich Technik und Organisation, Dipl.-Informatiker Roy Pfitzner, auf seinen Wunsch auf einen höherwertigen Dienstposten in der neu gebildeten Abteilung Strategische Planung und Innovation im Ministerium des Innern versetzt. Wir sind bestrebt, die entstandenen personellen Lücken so schnell wie möglich zu schließen.

Mit der Bereitstellung eines Internetzugangs und eines E-Mail-Dienstes hat jeder Beschäftigte unserer Dienststelle am Arbeitsplatz die Möglichkeit, moderne Informations- und Kommunikationstechnologien zu nutzen. Im Berichtszeitraum wurde eine Dienstanweisung über die Nutzung von E-Mail und anderen Internetdiensten und eine Dienstvereinbarung über die Kontrolle der Nutzung von E-Mail und anderen Internetdiensten innerhalb unserer Dienststelle in Kraft gesetzt.

In der Dienstvereinbarung wurde festgeschrieben, dass eine vollständige Protokollierung der Zugriffe auf externe Internetseiten ohne Personenbezug erfolgt. Um eine Nutzung des Internets, die gegen geltendes Recht verstößt, zu verhindern, werden zusätzlich personenbezogene Internetzugriffe stichprobenartig in einer Protokolldatei verschlüsselt gespeichert. Im Regelfall werden täglich zehn Internetzugriffe nach dem Zufallsprinzip protokolliert. Nur bei Verdacht auf eine rechtswidrige Nutzung des Internetzugangs am Arbeitsplatz erfolgt eine gemeinsame Überprüfung durch den Behördenleiter, dem Personalrat und dem behördlichen Datenschutzbeauftragten. Es wurde dazu eine technische Lösung gefunden, die auf unserem bereits im Einsatz befindlichen Chipkartensystem beruht. Diese Lösung ließe sich auch auf andere Dienststellen des Landes übertragen.

2 Zusammenarbeit mit dem Landtag

Der 11. Tätigkeitsbericht (2002) des Landesbeauftragten mit der Stellungnahme der Landesregierung wurde gegen Ende des Berichtszeitraumes im Innenausschuss beraten. Im Mittelpunkt der Diskussion stand dabei der Hinweis des Landesbeauftragten auf die vom Brandenburgischen Datenschutzgesetz vorgeschriebenen Risikoanalysen und Sicherheitskonzepte, die bisher noch nicht in allen Behörden des Landes erstellt und umgesetzt werden. Außerdem regte der Landesbeauftragte eine Initiative der Landesregierung im Bundesrat zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen und des Vergaberechts an, um durch mehr Transparenz in diesem Bereich bei gleichzeitiger Wahrung des Schutzes von Betriebs- und Geschäftsgeheimnissen einen Beitrag zur Korruptionsbekämpfung zu leisten.

Bereits im Oktober 2003 hatte der Landesbeauftragte auf Einladung des Ausschusses für Inneres im Rahmen einer öffentlichen Anhörung zum Entwurf der Landesregierung für ein Zweites Gesetz zur Entlastung der Kommunen und die darin vorgeschlagenen Änderungen des Akteneinsichts- und Informationszugangsgesetzes Stellung genommen[86].

3 Kooperation mit behördlichen Datenschutzbeauftragten, Datenschutzbehörden und Informationszugangsbeauftragten

Die behördlichen Datenschutzbeauftragten, deren Bestellung das Brandenburgische Datenschutzgesetz allen öffentlichen Stellen im Land vorschreibt, erfüllen ergänzend zum Landesbeauftragten eine wichtige Aufgabe. Der Landesbeauftragte hat deshalb stets einer engen Zusammenarbeit mit den behördlichen Datenschutzbeauftragten große Bedeutung zugemessen. Die Kontrolle und Beratung der öffentlichen Stellen im Land Brandenburg kann durch eine stärkere Vernetzung der Tätigkeiten des Landesbeauftragten und der behördlichen Datenschutzbeauftragten nur gewinnen.

Der Abschluss der Sanierungsarbeiten an dem zweiten von unserer Dienststelle genutzten Gebäude hat erstmals die räumlichen Voraussetzungen geschaffen, die behördlichen Datenschutzbeauftragten der obersten Landesbehörden, der Landkreise, kreisfreien Städte und großen kreisangehörigen Städte zu einer Beratung in unsere Dienststelle einzuladen. Das Ziel, Fragen des Datenschutzes und des Informationszugangs aus der täglichen Praxis der behördlichen Datenschutzbeauftragten zu diskutieren, Erfahrungen auszutauschen und gemeinsame Lösungen zu erarbeiten, wurde nicht zuletzt durch zahlreiche Themenvorschläge und das große Engagement der Teilnehmerinnen und Teilnehmer voll erreicht. Im Vordergrund standen Fragen des technischen und organisatorischen Datenschutzes, der Verarbeitung von Personaldaten und der Anwendung des Akteneinsichts- und Informationszugangsgesetzes. Es ist geplant, diese Beratungen zukünftig in ähnlicher Form regelmäßig fortzusetzen.

Im Berichtszeitraum fand erstmals nach längerer Unterbrechung wieder ein Koordinationsgespräch mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Ministerium des Innern statt.

[86] vgl. dazu oben Teil B 1.3

Länderübergreifend wurde neben der bewährten Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit auch die Kooperation mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein verstärkt. Diese Behörde vergibt als einzige Datenschutzinstanz in der Bundesrepublik bisher Gütesiegel und führt Datenschutzaudits durch, die auch Auswirkungen in Brandenburg haben[87]. Wir hatten sowohl die Frage der Anwendbarkeit des § 11b Abs. 2 Brandenburgisches Datenschutzgesetz auf die in Schleswig-Holstein vergebenen Gütesiegel zu prüfen als auch im Wege der Amtshilfe dem Unabhängigen Landeszentrum für Datenschutz über unsere Prüfergebnisse zu einem Verfahren zu berichten, für das in Schleswig-Holstein ein Gütesiegel beantragt worden ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im vergangenen Jahr unter dem Vorsitz des Sächsischen Datenschutzbeauftragten, Dr. Thomas Giesen, in Dresden und Leipzig und fasste eine ganze Reihe von Entschließungen zu aktuellen Fragen des Datenschutzes. Diese sind in dem Band „Dokumente zu Datenschutz und Informationsfreiheit 2003“ abgedruckt, den wir wie in den vergangenen Jahren gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit herausgegeben haben. Im begonnenen Jahr 2004 hat der Landesbeauftragte für den Datenschutz Saarland, Karl Albert, den Vorsitz in der Konferenz übernommen. Der länderübergreifende Arbeitskreis Medien der Datenschutzkonferenz tagte im Berichtszeitraum in Potsdam und Kleinmachnow unter dem Vorsitz des brandenburgischen Landesbeauftragten. Dabei wurden mehrere Entschließungen der Datenschutzkonferenz zur Telekommunikationsgesetzgebung und zum Rundfunkrecht vorbereitet.

Auch die Zusammenarbeit der Datenschutzbeauftragten auf europäischer und internationaler Ebene nimmt weiter an Bedeutung zu. Der Landesbeauftragte hat eine von der deutschen Datenschutzkonferenz gefasste Entschließung zu automatischen Software-Updates und den Entwurf einer Stellungnahme zum Problem der RFID-Technologie in der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation erläutert und anschließend der 25. Internationalen Konferenz der Datenschutzbeauftragten vorgelegt, die beide Entschließungen annahm[88].

Im Rahmen der Europäischen Konferenz der Datenschutzbeauftragten finden regelmäßige Arbeitssitzungen des „Complaints Handling Workshop“ statt, bei denen Mitarbeiter der Datenschutzbehörden aus den Mitgliedsländern praktische Probleme der Beschwerdebearbeitung erörtern und Erfahrungen austauschen. An einer Sitzung dieser Arbeitsgruppe hat der Landesbeauftragte selbst und an zwei weiteren Sitzungen einer seiner Mitarbeiter teilgenommen.

[87] vgl. dazu Teil A 1.1

[88] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, A III

Wie im Datenschutz ist auch bei der Informationsfreiheit ein verstärkter internationaler Erfahrungsaustausch wichtig für die Lösung praktischer Probleme vor Ort. Zu diesem Zweck haben vierzehn Informationsbeauftragte und Ombudspersonen, darunter auch der Landesbeauftragte für das Recht auf Akteneinsicht in Brandenburg, am 7. April 2003 in der Europäischen Akademie für Informationsfreiheit und Datenschutz in Berlin die Internationale Konferenz der Informationsbeauftragten gegründet[89]. Die 2. Internationale Konferenz der Informationsbeauftragten wird Anfang Februar 2004 auf Einladung der südafrikanischen Menschenrechtskommission in Kapstadt stattfinden.

4 Öffentlichkeitsarbeit

4.1 Das Jahr der Informationsfreiheit 2003

Während die Modernisierung der Verwaltung in Bund und Ländern auf der politischen Agenda ganz oben steht, lässt der internationale Vergleich darauf schließen, dass die eigentlichen Kernthemen dieser Diskussion, nämlich transparente Verwaltungsverfahren, E-Government und eine größere Partizipation der Bürgerinnen und Bürger am staatlichen Handeln dabei recht kurz kommen. Gerade Informationsfreiheit stellt in vielen Staaten längst ein alltägliches Instrument in diesem Wandlungsprozess dar, führt in Deutschland aber nach wie vor eher ein Schattendasein. Um ihre Bedeutung deutlicher in den Mittelpunkt der öffentlichen Wahrnehmung zu rücken, hat die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID), der die Informationsbeauftragten der Bundesländer Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen angehören, das Jahr 2003 zum Jahr der Informationsfreiheit ausgerufen.

Im Rahmen des Jahres der Informationsfreiheit haben die Informationsbeauftragten dieser vier Bundesländer neben anderen Aktivitäten auch jeweils eine größere Veranstaltung dem Thema gewidmet. Den Auftakt bildete das Sommersymposium zur Informationsfreiheit, das von der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen durchgeführt wurde. Das Symposium unterstrich die Bedeutung der Informationsfreiheit in einer lebendigen und funktionsfähigen Demokratie und beschäftigte sich mit den Ursprüngen, der rechtlichen Einordnung von und den bisherigen Erfahrungen mit Informationsfreiheitsgesetzen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit richtete das Symposium „Informationsfreiheit und Datenschutz im Internet“ im Rahmen der Internationalen Funkausstellung in Berlin aus. Es befasste sich u. a. mit den Wirkungen des Internet bei der

[89] vgl. Dokumente zu Datenschutz und Informationsfreiheit 2003, B III

Weiterentwicklung der Informationsfreiheit sowie mit einer datenschutzrechtlichen Bewertung der Potenziale dieses Mediums bei der Verbreitung personenbezogener Daten. Unter dem Motto „Informationsfreiheit – vom Norden lernen“ ließ das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein während einer Konferenz im Dezember vor allem Experten aus den skandinavischen Ländern, in denen bereits jahrelange Erfahrungen mit der Informationsfreiheit vorliegen, zu Wort kommen. Auch der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg leistete mit dem Internationalen Symposium „Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel- und Osteuropa“, das im November in Potsdam durchgeführt wurde[90], einen Beitrag zum Jahr der Informationsfreiheit.

Die Teilnehmer aus Verwaltung, Wirtschaft und Verbänden sowie interessierte Bürgerinnen und Bürger informierten sich auf den Veranstaltungen und fanden Ansprechpartner, um Gedanken und Erfahrungen auszutauschen. Die große Resonanz machte deutlich, dass das Fehlen eines Informationsfreiheitsgesetzes in der Bundesrepublik Deutschland zunehmend als nicht mehr hinnehmbar empfunden wird. Die Informationsbeauftragten der vier Bundesländer werden dafür eintreten, dass dieses Thema auch nach dem Ende des Jahres der Informationsfreiheit auf der deutschen Tagesordnung bleibt.

4.2 Internationales Symposium „Informationsfreiheit und Datenschutz“ in Potsdam

Gut ein halbes Jahr vor dem Beitritt der mittel- und osteuropäischen Staaten zur Europäischen Union sind die rechtlichen Grundlagen für ein gemeinschaftliches Datenschutz- und Transparenzniveau geschaffen. Gleichzeitig wird sowohl in den bisherigen als auch in den neuen Mitgliedsländern die Beziehung zwischen Staat und Bürger zunehmend auf eine elektronische Basis gestellt. Wie sieht unter diesen Bedingungen die Praxis des Persönlichkeitsschutzes und der Informationsfreiheit aus?

Diese Fragestellung war das Thema des von uns am 10. und 11. November 2003 veranstalteten Internationalen Symposiums „Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel- und Osteuropa“. Es war die dritte Veranstaltung dieser seit 1999 in zweijährigem Rhythmus stattfindenden Tagungsreihe. Neben Referentinnen und Referenten aus Brandenburg und der Bundesrepublik sowie den künftigen mittel- und osteuropäischen Mitgliedsländern kamen auch Expertinnen und Experten aus Staaten zu Wort, die nicht oder noch nicht der Europäischen Union angehören. Die Vortragenden griffen einige Vorhaben zum E-Government exemplarisch her-

[90] vgl. Teil C, 4.2

aus und stellten die Erfahrungen der jeweiligen Länder mit ihrer Umsetzung und mit der dort bestehenden Rechtslage vor.

Es wurde deutlich, dass E-Government sowohl den Informationszugang für jedermann voraussetzt als auch den datenschutzrechtlichen Anforderungen genügen muss, um von den Bürgerinnen und Bürgern akzeptiert zu werden. Die Notwendigkeit einer Anpassung der Rechtslage im Rahmen der Einführung des E-Government wurde am Beispiel eines Konzepts für eine einheitliche Gesetzgebung für Datenschutz und Informationsfreiheit im eidgenössischen Kanton Zürich vorgestellt. Trotz eines deutlich unterschiedlichen Stands der Entwicklungen haben die Beispiele aus der Türkei, der Ukraine, aus Estland und Slowenien gezeigt, dass auf dem Weg zu einem von den Bürgerinnen und Bürgern akzeptierten elektronischen Behördendienst überall ganz ähnliche Hindernisse und Probleme auftreten. Eine Privatinitiative aus Polen wartet nicht länger auf ein Handeln der Regierung, sondern unterstützt die Kommunen beim Aufbau von Informations- und Kommunikationsstrukturen – nicht zuletzt im Hinblick auf den Beitritt unseres Nachbarlandes zur Europäischen Union. Ein weiterer Beitrag beschäftigte sich mit den Besonderheiten der Nutzung von E-Government-Angeboten im Gesundheitswesen. Mit dem Projekt eLoGo der Universität Potsdam wird sowohl ein Forschungsnetzwerk aufgebaut als auch die Einführung des E-Government in einem brandenburgischen Landkreis unterstützt. Ein weiterer brandenburgischer Vortrag beschäftigte sich mit Aspekten des Zugangs zu und der Nutzung von Geoinformationen.

Interessierte Bürgerinnen und Bürger, Beschäftigte der brandenburgischen Landes- und Kommunalverwaltungen sowie Vertreter von Nicht-Regierungsorganisationen und internationale Gäste nahmen an der Konferenz teil. Die Vorträge können von unserer Website abgerufen werden. Auf Anfrage stellen wir auch gerne eine gedruckte Dokumentation des Internationalen Symposiums zur Verfügung.

4.3 Der Landesbeauftragte auf dem Brandenburg-Tag

Nach den Brandenburg-Tagen in Frankfurt (Oder), Luckau und Neuruppin war in diesem Jahr die Landeshauptstadt Potsdam Gastgeberin für das Landesfest. Am Lustgarten – in der historischen Mitte Potsdams – standen die Referentinnen und Referenten des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht allen Interessierten für Fragen und individuelle Beratung zur Verfügung.

Die Landeshauptstadt Potsdam stellte sich als Stadt der Wissenschaft dar und nutzte die Chance, ihr Profil als moderner Standort für Kultur und Dialog, Wissen und Forschung weiter auszuprägen. Wir griffen dieses Thema auf und informierten insbesondere zu den Rechten der Betroffenen und den Pflichten der Forscher im Rahmen wissenschaftlicher Umfragen bzw. Studien. Forschungsvorhaben an den Schulen stellten dabei einen besonderen Schwerpunkt dar.

Das Informationszelt des Landesbeauftragten stieß auf ein reges Interesse. Informationsschriften zur Eindämmung der Werbeflut im Briefkasten, Wegweiser zur Akteneinsicht sowie das Datenscheckheft, mit dessen Hilfe Betroffene ihre Datenschutzrechte gegenüber der Verwaltung leichter wahrnehmen können, waren sehr gefragt und trotz großer Vorräte bereits am Nachmittag vergriffen. Dennoch konnten am Rande auch persönliche Gespräche mit einzelnen Besuchern geführt werden, die sich schwerpunktmäßig nach Aspekten wie dem Sozialdatenschutz oder der Sicherheit des Surfens im Internet erkundigten.

Auch auf dem kommenden Brandenburg-Tag am 4. September 2004 in Eberswalde wird der Landesbeauftragte wieder mit einem Informationszelt vertreten sein. Wir freuen uns auf Ihren Besuch und die Gespräche mit Ihnen.

4.4 Neue Website des Landesbeauftragten

Seit 1996 ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht mit einer eigenen Website im Internet vertreten. In der Zwischenzeit ist das Angebot immer umfangreicher geworden, sodass die einzelnen Beiträge einerseits zunehmend schwer auffindbar, andererseits aber auch immer aufwändiger zu administrieren waren. Mit Unterstützung des Landesbetriebes für Datenverarbeitung und Statistik konnte eine neugestaltete Website im Dezember 2003 ins Netz gestellt werden.

Neu ist – neben dem veränderten Layout – eine übersichtliche Navigation für die Nutzerinnen und Nutzer, die Möglichkeit, die meisten Dokumente als Druckfassung ausgeben zu können sowie eine umfangreiche inhaltliche Gliederung beider Aspekte unserer Aufgaben: Durch eine separate Darstellung des Datenschutzes und der Informationsfreiheit können die einzelnen Beiträge leichter als bisher aufgefunden werden. Die Stichwortsuche ermöglicht zudem eine Recherche innerhalb des gesamten Angebots. So ist es auch ein Leichtes, Artikel aus sämtlichen Tätigkeitsberichten zu einem bestimmten Thema aufzulisten.

Die noch bestehenden technischen Barrieren für eine ungehinderte Nutzung der Informationen auf unserer neugestalteten Website durch Sehbehinderte werden derzeit aus dem Weg geräumt, damit das Angebot für möglichst viele Nutzerinnen und Nutzer zugänglich ist.

Unsere Website ist nach wie vor unter www.lda.brandenburg.de zu erreichen. Während diese Adresse unverändert geblieben ist, haben sich die Standorte für die einzelnen Dokumente jedoch durchgehend geändert. Soweit von anderen Websites dokumentenscharf auf unser Angebot verlinkt worden ist, empfehlen wir eine Aktualisierung dieser Verweise.

Um die neue Website stets aktuell und nutzerfreundlich zu halten, benötigen wir Ihre Mithilfe. Bitte lassen Sie uns wissen, welche Verbesserungen Sie für notwendig halten. Wir freuen uns auf Ihre Kritik und Anregungen.

4.5 Aktuelle Publikationen des Landesbeauftragten

Als Bestandteil der Reihe Brandenburgisches Informationsgesetzbuch hat der Landesbeauftragte in diesem Jahr die archivrechtlichen Vorschriften des Bundes und des Landes Brandenburg herausgegeben. Schließlich können die Archivgesetze als „frühe Informationszugangsgesetze“ betrachtet werden. Das neue Heft beinhaltet das Bundes- und das brandenburgische Archivgesetz einschließlich der entsprechenden Kosten- und Benutzungsregelungen. Auch wenn es schwer vorstellbar ist, dass die Stasi-Unterlagen in absehbarer Zeit zu „normalem Archivgut“ werden könnten, wird gegenwärtig darüber diskutiert, ob und unter welchen Voraussetzungen sie in das Bundesarchiv überführt werden können. Vor diesem Hintergrund wurde das Stasi-Unterlagen-Gesetz ebenfalls in dem Band abgedruckt.

Bereits im Vorfeld des Beitritts Polens zur Europäischen Union haben sich die Beziehungen zwischen Brandenburg und seinem östlichen Nachbarland sowohl zwischen den Bürgerinnen und Bürgern als auch zwischen den Verwaltungen intensiviert. Das Interesse an den gesetzlichen Regelungen des Nachbarlandes ist entsprechend gestiegen. Wir haben das Brandenburgische Datenschutzgesetz und das Akteneinsichts- und Informationszugangsgesetz deshalb ins Polnische übersetzen lassen und ebenso wie die englischen Ausgaben als Broschüren herausgegeben.

Eine Dokumentation des Internationalen Symposiums „Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel- und Osteuropa“, das im November in Potsdam stattfand[91], ist in gedruckter Form erhältlich.

[91] vgl. Teil C, 4.2

Ein neues Faltblatt informiert über die datenschutzgerechte Durchführung wissenschaftlicher Untersuchungen an Schulen, ein weiteres Faltblatt enthält Hinweise, wie man den Computer vor unerwünschten Datenspionen (Spyware, Adware, Trackware) schützen kann.

Diese und weitere Publikationen stellen wir gerne – soweit vorrätig auch in größerer Stückzahl – zur Verfügung. Sie können auch von der neuen Website des Landesbeauftragten abgerufen werden.

Kleinmachnow, den 8. März 2004

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht

Anlagen

Anlage 1

Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Datenschutzbeauftragten des Bundes und der Länder

Orientierungshilfe

Datensicherheit bei USB-Geräten

Stand: 27. November 2003

1 Problem

Öffentliche Stellen können ihre Datenverarbeitung nicht nach Belieben organisieren, sondern müssen die Verwaltungs-(Verfahrens-)Vorschriften einhalten. Um dies sicherstellen zu können, dürfen ohne Wissen der Behördenleitung keine Daten verarbeitet werden. Dies gilt insbesondere für personenbezogene Daten, da deren Missbrauch zu Schäden für die Betroffenen führen kann. Deshalb schreiben einige Datenschutzgesetze explizit vor, dass Datenverarbeitungsverfahren einer Freigabe durch die Behördenleitung bedürfen (z. B. § 19 Landesdatenschutzgesetz Mecklenburg-Vorpommern).

Neben der verwendeten Software ist auch die Hardware förmlich freizugeben. Zu Recht wird häufig der Zugriff auf Laufwerke aller Art (CD-ROM, Disketten, Zip-Laufwerke etc.) unterbunden, da sie es ermöglichen, unkontrollierbare Datensammlungen anzulegen und nicht zugelassene und unerwünschte Software auszuführen. Schnittstellen für Modems und andere Datenübertragungsgeräte werden abgeschaltet, damit keine unerlaubten und unkontrollierbaren Seiteneingänge in das lokale Netz geschaffen werden können.

Seit einiger Zeit werden praktisch alle Personal Computer mit Buchsen für den Universal Serial Bus (USB) ausgestattet. Diese Schnittstellen dienen dem einfachen Anschluss verschiedener Hardwarekomponenten wie Disketten-, DVD oder CD-Rom-Laufwerken, Festspeicher-Medien oder Netzwerkhardware. Aufwändige Installationsprozeduren für Hard- und Software entfallen, da moderne Betriebssysteme die neu angeschlossenen Geräte sofort erkennen und einbinden. Dadurch sinkt die Hemmschwelle, nicht freigegebene oder auch private Technik zu nutzen. Die bisher eingerichteten Nutzungsbeschränkungen für CD- und Floppy-Laufwerke sind dann nicht mehr ausreichend wirksam. Es müssen folglich Mechanismen gefunden werden, mit denen der Zugriff auf den USB auf genau die zugelassenen Geräte beschränkt werden kann.

2 Einsatzszenarien und Bedrohungen

Die technische Entwicklung zeigt, dass der Trend zum sogenannten „legacy-free PC“ ohne die klassischen seriellen, parallelen und PS/2-Anschlüsse geht. Zumindest für Tastatur und Maus, aber auch für Arbeitsplatzdrucker wäre dann USB zwingend notwendig. Darüber hinaus sind zunehmend dienstliche PDAs in Gebrauch, deren Synchronisation mit stationären Geräten häufig über die USB-Schnittstelle stattfindet. Damit stehen ein Anschluss und ein Protokollstack zur Verfügung, die jedoch auch zum Anschluss nicht freigegebener Hardwarekomponenten genutzt werden können. Die Betriebssystemunterstützung ist in der Regel so ausgelegt, dass USB-Geräte nach dem Einstecken sofort betriebsbereit sind.

Sicherheitsrelevant ist insbesondere der Einsatz nicht zugelassener Netzwerkadapter, Modems oder ISDN-Adapter, da mit ihnen unerlaubte „Seiteneingänge“ in Netzen geschaffen werden, die die zentralen Sicherheitseinrichtungen unterlaufen. Auch über USB anschließbare Speichermedien bergen ein erhebliches Sicherheitsrisiko in sich. Das betrifft insbesondere so genannte memory sticks. Das sind handliche Geräte in der Größe eines Schlüsselanhängers mit einem nicht flüchtigem Speicher, dessen Größe ein Gigabyte übersteigen kann. Sie werden wie wechselbare Festplatten angesprochen und gestatten das Speichern von schutzwürdigen Daten, den Zugriff auf mitgebrachte private Daten sowie das Ausführen von unerlaubten und nicht freigegebenen Betriebssysteme und Programmen, mit denen auch Sicherheitsmechanismen unterlaufen werden können.

Allerdings stehen den oben genannten Risiken bei der Nutzung von USB-Peripherie auch Vorteile für die Datensicherheit gegenüber. So erscheint es durchaus sinnvoll, besonders vertrauliche Datenbestände auf memory sticks oder USB-Festplatten zu speichern. Den physischen Zugriff zu diesem Medium kann man auf einfache Weise einschränken, und so die Chancen eines potenziellen Angreifers vermindern. Dies wäre mit der Speicherung auf (größeren) Wechselmedien vergleichbar. Gegen unbefugte Zugriffe bei Verlust des Mediums bzw. des USB-Gerätes hilft die verschlüsselte Speicherung der Daten mit Produkten wie PGP-Disk oder Steganos unter Windows oder PPDD (Practical Privacy Device Driver) unter Linux.

Die genannten Aspekte verdeutlichen, dass USB-Controller in den PCs in naher Zukunft kaum noch abgeschaltet werden können. Somit kann der Zugriffsschutz folglich nur über die Konfiguration des USB-Protokollstacks oder über allgemeine Zugriffsschutzmechanismen des Betriebssystems realisiert werden.

3 Lösungsansätze

3.1 Windows

3.1.1 Setzen von ACLs; kommerzielle Produkte

Der eleganteste Weg, Geräte aller Art unter Windows 2000/XP zu kontrollieren, ist das Setzen von ACLs auf diese Geräte. (ACLs, access control lists, sind spezielle Zugriffsschutzdaten; sie werden beispielsweise Geräten und Dateien zugeordnet und vom Betriebssystem verwaltet.) Das ist auch die einzige Möglichkeit, um Schwierigkeiten im Multiuserbetrieb (z.B. auf einem Terminalserver) zu umgehen. ACLs sind bereits unter Windows NT sehr mächtig. Allerdings bietet Microsoft den vollständigen Zugriff auf ACL-Objekte nur Programmierern an (über Programmierschnittstellen, die APIs). Geeignete Konsolenprogramme oder Editoren stehen bislang nicht zur Verfügung. Leider sind sicherheitsrelevante API-Funktionen für Geräte im DDK (*Device Driver Kit*, Entwicklungssoftware für Gerätetreiber) nur spärlich dokumentiert. Dieser Weg scheidet für die meisten Anwender deshalb aus, weil sie nicht über die erforderlichen Kenntnisse in der Systemprogrammierung von Windows verfügen.

Zur Zugriffssteuerung für das USB-Subsystem bringt Windows ebenfalls standardmäßig keine Werkzeuge mit. Nach [1] ist eine entsprechende Lösung zwar geplant, jedoch bislang nicht realisiert.

SecureNT ist ein kommerzielles Tool, welches auf ACL-Basis den Zugriff auf USB-Geräte steuert (http://securewave.com/products/securent). SecureNT kann darüber hinaus auch den Zugriff auf weitere Geräte steuern, also auch auf PCMCIA-Geräte, Floppy, CD-ROMs, ZIP-Drives, memory cards usw. Mit dem Produkt Device-Lock kann der Zugriff auf USB-Geräte ebenfalls wirksam beschränkt werden.

3.1.2 Überwachen der Registry

Darüber hinaus kann nach [1] der Registrierungsschlüssel

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

überwacht werden. Neu eingebundene USB-Geräte werden hier eingetragen. In [1] ist hierzu ein VBScript-Programm beschrieben, welches auch als Dienst eingerichtet werden kann. Es antwortet bei Erscheinen unzulässiger Gerätetypen mit einer konfigurierbaren Aktion. So kann es den Rechner herunterfahren oder den Systemadministrator informieren. Es scheint nämlich zumindest

unter Windows 2000 und XP nicht möglich zu sein, die Schlüssel einfach automatisch zu löschen.

3.1.3 Überwachen der USB-Geräte mittels WBEM

Man kann den USB-Controller auch mittels eines Dienstes über die WBEM-Instanz Win32_*USBController* überwachen. (WBEM ist das Web Based Enterprise Management; die Implementation von Microsoft heißt Windows Management Instrumentation WMI) Taucht ein neues Gerät auf, überprüft der Dienst, ob der angemeldete Nutzer das Gerät nutzen darf. Dazu ist jeder bekannten USB-Device-ID eine Gruppe zugeordnet. Ist das USB-Gerät unbekannt oder ist der angemeldete Nutzer nicht Mitglied der jeweiligen USB-Zugriffsgruppe, wird das USB-Gerät gesperrt (*via SetupDiCallClassInstaller*-API). Meldet sich ein neuer Nutzer an, der seinerseits Mitglied der jeweiligen USB-Zugriffsgruppe ist, wird das USB-Gerät wieder freigegeben. Unter Umständen ist noch ein Reboot nötig. Das Verfahren funktioniert leider nicht auf Terminalservern, da es nicht multi-user-fähig ist. Diesen Dienst zu schreiben erfordert jedoch Kenntnisse in der Windows-Systemprogrammierung, in der Sprache C, eine entsprechende Entwicklungsumgebung und die Zeit, ein Programm von etwa 600 Zeilen C-Code zu erstellen und zu testen.

3.1.4 Löschen der USB-Treiber; USB-Netzwerkgeräte

Zu guter Letzt kann man auch die Treiber aus dem System entfernen, die zur Verwaltung bestimmter USB-Geräte erforderlich sind. Windows kommuniziert beispielsweise über den Treiber *usbstor.sys* mit USB-Massenspeichern. Administratoren können diesen Treiber aus dem Windows-System-Verzeichnis und aus dem Driver Cache löschen, um den Zugriff auf USB-Sticks zu unterbinden.

Das Einbinden von USB-Netzwerkadaptern sowie USB-Modems erfordert unter Windows 2000/XP Administrationsrechte. Es genügt daher, darauf zu achten, dass diese Rechte gewöhnlichen Benutzern nicht zugeteilt werden.

3.2 Linux

Um unter Linux den unbefugten Gebrauch von USB-Speichergeräten einzuschränken, sollte explizit festgelegt werden, wer überhaupt bestimmte Geräte montieren darf. Dazu müssen die Zugriffsrechte auf die entsprechenden Gerätedateien gesetzt werden. In der Regel werden USB-Geräte wie SCSI-Geräte behandelt; memory sticks und USB-Festplatten werden also mit Namen wie */dev/sda, /dev/sda1* etc. angesprochen. Es ist empfehlenswert, alle zugelassenen Benutzer in einer Gruppe zusammenzufassen und die ent-

sprechende Gerätedatei dem Eigentümer *root* und dieser Gruppe zu übergeben (mittels *chown, chgrp*).

Das unbefugte Montieren von Datenträgern kann ferner dadurch verhindert werden, dass die dazu notwendigen Einträge in der */etc/fstab* gelöscht oder in einen Kommentar umgewandelt werden. Dann bleibt diese Aktion in jedem Falle dem Systemverwalter *root* vorbehalten.

Darüber hinaus besteht die Möglichkeit, die nicht benötigten Treiber im Verzeichnisbaum unter */lib/modules* zu löschen, darunter *usb-storage.o* . Ferner kann auch die Konfiguration des für die USB-Geräte-Verwaltung zuständigen Daemons hotplug so angepasst werden, dass bestimmte Treiber nicht geladen werden (in */etc/hotplug/blacklist* aufnehmen) oder dass genau die zulässigen Treiber geladen werden (in */etc/hotplug/usb.*map*).

USB-Netzwerkadapter und USB-Modems sind Benutzern unter Linux nicht zugänglich, wenn dies nicht ausdrücklich eingerichtet ist, da die Konfigurationstools wie ifconfig nur dem Systemverwalter Änderungen gestatten. Die Rechte an entsprechenden Geräte-Dateien verbieten gewöhnlichen Benutzern standardmäßig den Zugriff. Auch die Konfigurationsdateien, die die Netzwerkkonfiguration beim Booten des Systems steuern, können von normalen Benutzern üblicherweise nicht verändert werden, weil ihnen die Rechte dafür fehlen.

3.3 Booten von USB-Geräten

Damit die oben erwähnten Zugriffsschutzmechanismen der Betriebssysteme wirksam werden können, dürfen nur die freigegebenen Betriebssysteme oder System-Konfigurationen gestartet werden können. Es sollte daher sichergestellt sein, dass das Booten von herkömmlichen CDROM-/DVD-Laufwerken, Disketten-Laufwerken und vom Netzwerk (falls zutreffend) unterbunden wird. Dies ist bereits jetzt Stand der Technik (siehe [4]).

Es ist jedoch auch möglich, von USB-Geräten zu booten, wenn sowohl das PC-BIOS als auch das USB-Gerät dazu in der Lage sind. Einige aktuelle BIOS-Versionen gestatten das Booten von memory sticks, mitunter auch von USB-Disketten- und -CDROM-Laufwerken ([2], [3]).

Um das Starten von Betriebssystemen von USB-Geräten und anderen wechselbaren Medien zu verhindern, sollte im BIOS die Boot-Optionen angepasst werden. Das Booten von USB-Geräten und anderen wechselbaren Laufwerken sollte in dem entsprechenden BIOS-Menü abgeschaltet werden. Falls dies nicht möglich ist, sollten die Boot-Optionen so konfiguriert werden, dass

USB-Geräte erst nach der System-Festplatte (oder nach dem Netzwerk, falls zutreffend) angesprochen werden.

BIOS-Einstellungen sind in jedem Fall gegen Änderungen durch Unbefugte zu sichern. Dazu muss der Passwortschutz für das BIOS-Setup aktiviert werden.

Bootfähige USB-Netzwerk-Adapter sind bislang nicht bekannt.

3.4 Grenzen beim Zugriffsschutz

Das USB-Subsystem arbeitet – ähnlich wie die PCMCIA-Karten – mit zwei Kennzeichen, die den Typ eines Gerätes eindeutig beschreiben, der Vendor ID und der Product ID. Damit ist aber keine Identifikation des einzelnen Exemplars möglich. Das Script aus [1] sowie der Linux-USB-Manager werten im Wesentlichen die genannten Kennungen aus. Der USB-Standard gestattet zwar die Implementation von Seriennummern, jedoch wird diese Möglichkeit nicht von allen Herstellern genutzt. Die Seriennummern von Datenträgern, die in verschiedenen Dateisystemen vorgesehen sind, sind demgegenüber leicht fälschbar. Man braucht lediglich bestimmte Bytes im Dateisystem zu verändern.

Eine Einschränkung auf explizit zugelassene Geräte ist somit – ähnlich wie bei anderen Datenträgern – nicht möglich. Dies gilt für alle Betriebssysteme.

4 Ergebnis

Nach derzeitigem Kenntnisstand bedroht der unkontrollierte Einsatz von USB-Massenspeichern Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten. Neben den kleinen und leichten memory sticks betrifft dies auch transportable Festplatten, MP3-Player, Digital-Kameras, CD-, Floppy- oder Karten-Laufwerke. Neben CD-[R|RW|ROM]s oder Floppies mit fest eingebauten Laufwerken stehen somit mobile Laufwerke zur Verfügung, mit denen Sicherheitsbestimmungen unterlaufen werden können.

Mit den Bordwerkzeugen von Windows kann der Zugriff auf USB-Geräte nicht auf einfache Weise verhindert werden. Mit moderatem zusätzlichem Aufwand kann die Installation nicht zugelassener Gerätetypen jedoch erkannt und blockiert werden. Dazu ist der Einsatz entsprechender Skripte oder kommerzieller Produkte erforderlich. Microsoft arbeitet an einer einfacheren Lösung.

Unter Linux ist es ebenfalls mit geringem bis moderatem Aufwand möglich, den Zugriff auf ausdrücklich benannte Geräteklassen oder -typen zu beschränken. Die dazu nötigen Schritte lassen sich aus der Dokumentation zum

USB-Subsystem ableiten. Wer auf welche Geräte zugreifen darf, wird über die Zugriffsrechte auf die entsprechenden Gerätedateien festgelegt.

Um die Zugriffsschutzmechanismen der Betriebssysteme ausnutzen zu können, muss darüber hinaus das Booten von USB-Geräten im BIOS abgeschaltet werden, wie dies schon von CDROM-, DVD- und Diskettenlaufwerken her bekannt ist. Damit diese Einstellungen wirksam bleiben, muss auch der BIOS-Passwortschutz aktiviert werden.

Prinzipbedingt können USB-Geräte nur anhand ihrer Vendor-ID und Product-ID identifiziert werden. Eine feinere Granularität ist nicht erreichbar, da Geräte-Seriennummern oft nicht implementiert sind und da sich Datenträger-Kennzeichen auf dem Speichermedium selbst leicht fälschen lassen.

5 Literatur

[1] Hohmann, R.: USB-Wächter – Digitaler Keuschheitsgürtel aus VBScript für die USB-Schnittstelle. In: c't Magazin für Computertechnik 08/2003, S. 190ff., Heinz Heise Verlag, Hannover

[2] Ilmberger, A., Baasch, K.: Daten aus der Hosentasche. In: Chip 10/2003, S. 77ff., Vogel Burda Communications, München

[3] Schmidt, J., Vahldiek, A.: Hols vom Stöckchen – Notfallsystem vom USB-Stick booten. In c't Magazin für Computertechnik 13/2003, S. 208ff., Heinz Heise Verlag, Hannover

[4] Bundesamt für Sicherheit in der Informationstechnik (Hg.): IT-Grundschutzhandbuch – Abschnitt M 4.84 Nutzung der BIOS-Sicherheitsmechanismen. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2002.

Anlage 2

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

Stand: 31. Dezember 2003

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix
Stellvertreter	Herr Urban
Sekretariat	Christine Objartel App. 10

Bereich Recht und Verwaltung

Bereichsleiter	Dr. Frank 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)	Herr Hermerschmidt App. 40
Arbeitsgebiete: - Polizei, Verfassungsschutz - Verkehrsordnungswidrigkeiten - Ausländer, Asylverfahren - Staatsanwaltschaften - Presse- und Öffentlichkeitsarbeit	Lena Schraut App. 41

Arbeitsgebiete: - Landwirtschaft, Umweltschutz und Raumordnung - Stadtentwicklung, Wohnen und Verkehr - Personaldaten allgemein	App. 45
Arbeitsgebiete: - Akteneinsicht und Informationszugang - Verwaltungsmodernisierung - Redaktion von Veröffentlichungen - Koordination des Internetangebots	Dipl. Verwaltungs-wissenschaftler Sven Müller App. 20
Arbeitsgebiete: - Finanzen - Bildung, Jugend und Sport - Wirtschaft	App. 22
Arbeitsgebiete: - Arbeit, Soziales, Gesundheit und Frauen - Sozial- und Gesundheitsdaten allgemein	Frau Oehme App. 66
Arbeitsgebiete: - Inneres	Oliver F. Hoff App. 36
Arbeitsgebiete: - Büroleitungsaufgaben - Haushaltsangelegenheiten - Beschaffungen	App. 42
Arbeitsgebiete: - Personal- und Verwaltungsangelegenheiten - Bibliothek - Schreibdienst	App. 12

Bereich Technik

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	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	Dipl.-Ingenieur (FH) Jens Budszus App. 35
Arbeitsgebiete: - Schreibdienst - Informationsmaterialien	App. 43

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

Anlage 3

Aktenplan des 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

ABl.	=	Amtsblatt
AGID	=	Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland
ASS	=	Auswerte-System Staatsschutz Brandenburg
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BGBl.	=	Bundesgesetzblatt
BGS	=	Bundesgrenzschutz
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtsgesetz
BR-Drs.	=	Bundesrats-Drucksache
BSI	=	Bundesamt für die Sicherheit in der Informationstechnik
BStatG	=	Bundesstatistikgesetz
BT-Drs.	=	Bundestagsdrucksache
BVerwG	=	Bundesverwaltungsgericht
bzw.	=	beziehungsweise
CD-ROM	=	Compact Disc - Read Only Memory
CDU	=	Christlich Demokratische Union
CSU	=	Christlich Soziale Union
d. h.	=	das heißt
DHCP	=	Dynamic Host Configuration Protocol
DNA	=	Desoxyribonuclein acid (Desoxyribonukleinsäure)
DPV	=	Deutsch-Polnische Verbindungsstelle
Drs.	=	Drucksache
DVD	=	Digital Versatile Disc
EDV	=	Elektronische Datenverarbeitung
EGGVG	=	Einführungsgesetz zum Gerichtsverfassungsgesetz
eLoGo	=	electronic local government
FDP	=	Freie Demokratische Partei
ff.	=	folgende
gem.	=	gemäß
GEZ	=	Gebühreneinzugszentrale
GmbH	=	Gesellschaft mit beschränkter Haftung
GSTOOL	=	IT-Gundschutz-TOOL
GVBl.	=	Gesetz- und Verordnungsblatt
HTML	=	HyperText Markup Language
HTTP	=	HyperText Transfer Protocol
ID	=	Identification (Benutzerkennung)
i. d. R.	=	In der Regel
INPOL	=	Informationssystem der Polizei

IP	=	Internet Protocol
IPSEC	=	Internet Protocol Security
i. S. v.	=	im Sinne von
IT	=	Informationstechnologie
IuK	=	Informations- und Kommunikationstechnik
IT	=	Informationstechnik
KLR	=	Kosten- und Leistungsrechnung
LPflegeG	=	Landespflegegesetz
LDA	=	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDS	=	Landesbetrieb für Datenverarbeitung und Statistik
LKA	=	Landeskriminalamt
LPflegeG	=	Landespflegegesetz
LVN	=	Landesverwaltungsnetz
MAC	=	Media Access Control
MDStV	=	Mediendienste-Staatsvertrag
MEGA	=	Mobile Einsatzgruppe der Polizei
NADIS	=	Nachrichtendienstliches Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder
NJW	=	Neue Juristische Wochenschrift
Nr.	=	Nummer
ORB	=	Ostdeutscher Rundfunk Brandenburg
OSCI	=	Online Services Computer Interface
PASS	=	Polizeiliches Auskunftssystem Straftaten
PC	=	Personalcomputer
Pkt.	=	Punkt
POG	=	Polizeiorganisationsgesetz
Radius	=	Remote Authentication Dial-in User Service
RBB	=	Rundfunk Berlin-Brandenburg
RFID	=	Radio Frequency Identification
s.	=	siehe
S.	=	Seite; Satz
SFB	=	Sender Freies Berlin
SGB X	=	Zehntes Buch Sozialgesetzbuch
SGB XI	=	Elftes Buch Sozialgesetzbuch
SMS	=	Short Message Service
s. o.	=	siehe oben
SPD	=	Sozialdemokratische Partei Deutschlands
SSID	=	Service Set Identifier (Funknetzkennung)
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
TCP	=	Transmission Control Protocol
TCPA	=	Trusted Computing Platform Alliance
TDDSG	=	Teledienstedatenschutzgesetz

TDG	=	Teledienstegesetz
TDSV	=	Telekommunikations-Datenschutzverordnung
TK	=	Telekommunikation
TKG	=	Telekommunikationsgesetz
TOMEG	=	Täterorientierte Mobile Einsatzgruppe der Polizei
u. a.	=	unter anderem
UNESCO	=	United Nations Educational, Scientific and Cultural Organization
URL	=	Uniform Resource Locator
USB	=	Universal Serial Bus
usw.	=	und so weiter
u. U.	=	unter Umständen
vgl.	=	vergleiche
V-Person	=	Vertrauensperson
VPN	=	Virtual Private Network
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless Local Area Network
z. B.	=	zum Beispiel
z. T.	=	zum Teil
ZD Pol	=	Zentraldienst der Polizei

Stichwortverzeichnis