Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2001

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 5. März 2001 vorgelegten Tätigkeitsbericht 2000 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2001 ab.

Die „Dokumente zu Datenschutz und Informationsfreiheit 2001“, 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 Internet-Angebot 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: 03 32 03 / 356-0
Fax: 03 32 03 / 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 B
Akteneinsicht und Informationszugang

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

Anlagen

Behördenverzeichnis

Gliederungspunkt

Einleitung

Dies ist der Zehnte Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, der seit vier Jahren auch für die Wahrung des Rechts auf Akteneinsicht einzutreten hat. Am 16. März 1992 nahm der erste Landesbeauftragte für den Datenschutz in Brandenburg, Dr. Dietmar Bleyl, seine Tätigkeit auf. Das am 23. Januar 1992 in Kraft getretene Brandenburgische Datenschutzgesetz hat seitdem wesentlich dazu beigetragen, dass die Menschen in Brandenburg, die zuvor in der DDR einer systematischen informationellen Bevormundung ausgesetzt waren, zunehmend von ihrem Grundrecht auf informationelle Selbstbestimmung und Datenschutz (Art. 11 Landesverfassung) Gebrauch machen.

Zugleich stehen die Freiheitsrechte des Einzelnen und damit auch das Grundrecht auf Datenschutz seit den Anschlägen vom 11. September 2001 vor einer harten Bewährungsprobe. Angesichts der terroristischen Bedrohung reagierte der Gesetzgeber mit einem Bündel von Gesetzesverschärfungen, die die Sicherheitsgesetze der neuen Bedrohungslage anpassen sollte. Allein mit dem Terrorismusbekämpfungsgesetz vom Dezember 2001[1] wurden zwanzig Einzelgesetze in großer Eile verändert. Dabei blieb das rechtsstaatlich gebotene Augenmaß teilweise auf der Strecke. Die Begründungslast, die nach unserer Verfassung grundsätzlich der trägt, der in Freiheitsrechte eingreifen will, wurde zunehmend auf diejenigen verlagert, die sich gegen Grundrechtseingriffe wandten.

Es versteht sich von selbst, dass freie Gesellschaften, die in ihrer Existenz bedroht werden, geeignete Maßnahmen zu ergreifen suchen, um die Sicherheit der Bevölkerung soweit wie möglich zu gewährleisten. Zu diesem Zweck können auch Einschränkungen von Freiheitsrechten Einzelner hingenommen werden, wenn sie geeignet sind, der Bedrohung zu begegnen, und die Grundrechte nur in verhältnismäßigem Umfang beschränken. Dabei hat sich das Verständnis von Sicherheit grundlegend verändert. Fatal ist, dass Selbstmordattentäter vor ihrer Tat weitgehend unauffällig leben und sich nichts zu Schulden kommen lassen. Angesichts dieser Bedrohung gibt es keine vollständige Sicherheit und der Staat sollte sie seinen Bürgerinnen und Bürgern auch nicht in Aussicht stellen.

Indem die Sicherheitsbehörden immer weiter reichende Befugnisse zur Datenerhebung und Beobachtung bereits im Vorfeld eines konkreten Verdachts erhalten, steigt die Tendenz, ganzen Bevölkerungsgruppen oder der Bevölkerung insgesamt zu misstrauen. Dies wiederum löst auf der anderen Seite in der Bevölkerung Misstrauen gegenüber dem staatlichen Handeln aus. Der

[1] dazu im Einzelnen unter A 1.1

Richter am Bundesverfassungsgericht Prof. Dr. Wolfgang Hoffmann-Riem hat bei einem vom Landesbeauftragten veranstalteten Symposium in Potsdam im Oktober 2001 auf die Gefahren hingewiesen, die von einer solchen Spirale wechselseitigen Misstrauens gerade in Zeiten der Bedrohung ausgehen[2]. Die gesetzlichen Befugnisse der Nachrichtendienste und Strafverfolgungsbehörden lassen sich nicht beliebig ausweiten. Grundrechte unterliegen im Rechtsstaat nicht der Verfügung des Gesetzgebers, sondern begrenzen dessen Handeln. Der Europäische Gerichtshof für Menschenrechte hat schon 1977 betont, dass die Unterzeichnerstaaten der Europäischen Menschenrechtskonvention selbst im Namen des Kampfes gegen Spionage und Terrorismus nicht berechtigt sind, alle Maßnahmen zu ergreifen, die sie für angemessen halten. Die Reaktion des Gesetzgebers darf nicht die Grundlagen der Demokratie mit der Begründung in Frage stellen, eben diese zu verteidigen. Die Terroristen hätten eines ihrer erklärten Ziele erreicht, als eine Folge ihrer Anschläge, dass Freiheitsrechte zur Disposition gestellt würden.

Auch in anderen Zusammenhängen wurden im vergangenen Jahr Rufe laut, auf Gefahren und gesellschaftliche Probleme mit massenhafter Verarbeitung von personenbezogenen Daten zu reagieren.

Als Reaktion auf Gewaltverbrechen an Kindern wurde vorgeschlagen, alle Männer sollten sich vorsorglich einer DNA-Analyse unterziehen, deren Ergebnisse in einer zentralen Datenbank zu speichern wären. Dieser Vorschlag stieß zu Recht auf überwiegende Ablehnung. Seine Realisierung würde elementare rechtsstaatliche Grundsätze in Frage stellen, indem die Hälfte der Bevölkerung als potentielle Straftäter behandelt würde[3]. Zum anderen wird auch deutlich, wie weit verbreitet die Annahme ist, man könne mit der flächendeckenden Verarbeitung von personenbezogenen Daten ohne konkreten Anlass Gefahren effektiv vorbeugen oder den Schutz vor Kriminalität erhöhen. Selbst wenn Sexualstraftäter sich durch das erhöhte Risiko der Strafverfolgung von ihrem Tun abschrecken ließen – was mit guten Gründen bezweifelt wird -, rechtfertigt dies jedoch nicht, dass der Staat zur Durchsetzung seines Strafanspruchs ganze Bevölkerungsteile präventiv registriert.

Auch der Vorschlag zur Einführung einer Medikamenten-Chipkarte geht – in einem ganz anderen Zusammenhang – auf eine verfehlte Annahme zurück: Die zahlreichen Probleme des Gesundheitswesens lassen sich nicht dadurch lösen, dass man alle Versicherten rechtlich oder faktisch dazu zwingt, sensible medizinische Daten nicht nur dem Hausarzt anzuvertrauen, sondern sie

---

[2] Voraussetzungen der Informationsfreiheit, Internationales Symposium „Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union“, 8./9.10.2001, Potsdamer Materialien zu Akteneinsicht und Informationszugang, Band 2, S. 23 ff., 42

[3] vgl. die Entschließung der Datenschutzkonferenz vom 12.3.2001, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.2

auf einer Chipkarte und gleichzeitig in einer Datenbank personenbezogen speichern zu lassen. Auch wenn diese Pläne bisher nicht realisiert wurden oder inzwischen modifiziert werden sollen, machen sie doch deutlich, dass in der möglichst flächendeckenden Verarbeitung sensibler personenbezogener Daten einerseits ein Allheilmittel bei der Bewältigung schwierigster Probleme gesehen wird, andererseits aber der massive Eingriff in das Grundrecht auf informationelle Selbstbestimmung verkannt oder als hinnehmbar betrachtet wird. Der freiheitliche Rechtsstaat darf seine Bürgerinnen und Bürger jedoch nicht zu bloßen Objekten staatlicher Datenverarbeitung machen.

Transparenz staatlichen Handelns und Zugang zu Verwaltungsinformationen für jedermann sind wichtige Voraussetzungen dafür, dass die Menschen zu Subjekten der Informations- und Wissensgesellschaft werden und ihr Gemeinwesen politisch mitgestalten können. Mehrere Entwicklungen im Berichtszeitraum haben zu einer weiteren Ausbreitung des Transparenzgedankens beigetragen. Seit Anfang 2002 verfügt nun auch das frühere Partnerland Brandenburgs, Nordrhein-Westfalen, als bevölkerungsreichstes Bundesland über ein Informationsfreiheitsgesetz; die Europäische Transparenzverordnung stellt sicher, dass Dokumente der Organe der Europäischen Union im Grundsatz überall frei zugänglich sind. Auch die Anwendung des Akteneinsichts- und Informationszugangsgesetzes in Brandenburg wird zunehmend Bestandteil einer normalen, unaufgeregten Verwaltungspraxis, auch wenn hier und da noch Einzelfragen der Klärung bedürfen. Brandenburg ist damit bundesweit zum Beispiel dafür geworden, dass Transparenz und Leistungsfähigkeit sich in einer modernen Verwaltung nicht widersprechen, sondern gegenseitig bedingen.

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Das Grundrecht auf Datenschutz in der Bewährung

Das Jahr 2001 hat wie kaum ein Jahr zuvor seit dem In-Kraft-Treten der ersten Datenschutzgesetze deutlich gemacht, dass der effektive Schutz der informationellen Selbstbestimmung des Einzelnen immer wichtiger wird. Diese Feststellung mag paradox erscheinen, denn nach den Terroranschlägen vom 11. September 2001 überboten sich die Politiker gegenseitig mit Vorschlägen, wie der Datenschutz weiter eingeschränkt werden könne. Man konnte fast den Eindruck gewinnen, die deutsche Datenschutzgesetzgebung sei eine wesentliche Ursache der Terroranschläge in den USA gewesen.

Auch wenn niemand sich ausdrücklich zu dieser absurden Behauptung verstieg, nutzten die Sicherheitsbehörden den Schockzustand der Gesellschaft dazu, den größten Teil ihrer schon lange vor dem 11. September erhobenen Forderungen nach einer drastischen Ausweitung ihrer Befugnisse in Gesetzesform gießen zu lassen. Der brandenburgische Minister der Justiz und für Europaangelegenheiten wurde in einer Potsdamer Tageszeitung mit der Bemerkung zitiert, er kenne alle die zur Diskussion gestellten Befugniserweiterungen aus seiner Zeit als Staatssekretär im Bundesinnenministerium, wo er sie bereits unterstützt habe.

Der Bundesminister des Innern legte den Entwurf eines Terrorismusbekämpfungsgesetzes vor, der in Teilen eindeutig verfassungswidrig war. Neben einer verdachtsunabhängigen Initiativermittlungskompetenz des Bundeskriminalamtes sollte der Bundesinnenminister ermächtigt werden, durch Rechtsverordnung die Aufnahme nicht näher bestimmter biometrischer oder gar genetischer Merkmale in Personalausweise und Pässe sowie in Identifikationspapiere von Ausländern anzuordnen. Der Eingriff in das Grundrecht auf Datenschutz der gesamten Bevölkerung sollte ohne weitere Konturen der Exekutive überantwortet werden.

Das Terrorismusbekämpfungsgesetz wurde – wie der Bundesinnenminister selbst feststellte – unter hohem Zeitdruck und völlig unzureichender Gelegenheit zur gründlichen Beratung am 14. Dezember 2001 vom Bundestag beschlossen und trat zum 1 . Januar 2002 in Kraft[4]. Seine Bezeichnung ist

[4] BGBl. I 2002 S. 361

irreführend: Die in zahlreichen Sicherheitsgesetzen vorgesehenen Befugniserweiterungen für die Behörden dienen nicht der Bekämpfung des internationalen Terrorismus. Sie beruhen nicht auf einer sorgfältigen Analyse möglicher bisher bestehender Befugnislücken bei den Sicherheitsbehörden. Eine solche Analyse und Evaluation der schon bestehenden und in den vergangenen Jahren ständig erweiterten Überwachungsbefugnisse hat auch nach dem 11. September 2001 nicht stattgefunden, obwohl dies – gerade auch zum Schutz der Bevölkerung – notwendig gewesen wäre. Es ist daher fraglich, ob das Terrorismusbekämpfungsgesetz tatsächlich einen effektiven Beitrag zur Verhinderung terroristischer Anschläge in der Zukunft wird leisten können.

Gegenüber dem ursprünglichen Entwurf des Bundesinnenministeriums weist das in Kraft getretene Gesetz nur geringfügige Verbesserungen auf. Die Verfassungsschutzbehörden des Bundes und der Länder sowie der Militärische Abschirmdienst erhalten weit reichende neue Befugnisse, um von Kreditinstituten, Finanzdienstleistern und Luftfahrtunternehmen Auskünfte über deren Kunden zu verlangen, wenn tatsächliche Anhaltspunkte für schwer wiegende Gefahren durch Spionage und terroristische Bestrebungen vorliegen. Selbst ohne derartige Anhaltspunkte können die Geheimdienste darüber hinaus Auskünfte von Telekommunikations-, Teledienst- und Postdienstanbietern verlangen.

Zwar sind die befragten Unternehmen in diesen Fällen nicht verpflichtet, den Geheimdiensten die verlangten Auskünfte zu erteilen. Auch hat der Verfassungsschutz nach wie vor keine polizeilichen Befugnisse[5]. Dennoch besteht die Gefahr, dass die neuen weit reichenden Datenerhebungsbefugnisse des Verfassungsschutzes das im Grundgesetz und in der brandenburgischen Landesverfassung verankerte Trennungsgebot zwischen den Aufgaben des Verfassungsschutzes einerseits und den Aufgaben der Strafverfolgungs- und Polizeibehörden andererseits in fragwürdiger Weise relativieren. Die entsprechenden Datenerhebungen können auf Antrag des Leiters der Verfassungsschutzbehörde durch den Bundesinnenminister angeordnet werden; sie werden lediglich durch die G 10-Kommission des Deutschen Bundestages und das Parlamentarische Kontrollgremium nach dem G 10-Gesetz überprüft. Der Rechtsweg ist insoweit ausgeschlossen.

Die Länder dürfen ihren Verfassungsschutzbehörden diese Befugnisse erst dann einräumen, wenn sie entsprechende Berichtspflichten und Kontrollrechte im Landesrecht geregelt haben, was in Brandenburg bisher nicht geschehen ist. Entscheidend ist aber, dass die Unternehmen, die den Geheimdiensten Auskunft erteilen, den Betroffenen hierüber nicht informieren dürfen. Er hat – da er von der heimlichen Datenerhebung nichts erfährt – keine Möglichkeit, die Rechtmäßigkeit dieses Vorgehens wenigstens im Nachhinein ge-

[5] § 8 Abs. 3 BVerfSchG

richtlich überprüfen zu lassen. Nach dem im Berichtszeitraum ebenfalls geänderten G 10-Gesetz kann ihm eine entsprechende Information auch vom Verfassungsschutz unter bestimmten Umständen auf Dauer vorenthalten werden[6]. Damit ist das Grundrecht auf effektiven Rechtsschutz als Kernbestandteil des Rechtsstaatsprinzips in einer Weise eingeschränkt worden, die mit der Rechtsprechung des Bundesverfassungsgerichts[7] nur schwerlich zu vereinbaren ist. Zudem ist zweifelhaft, ob diese generelle Ausdehnung des parlamentarischen Kontrollmechanismus auf neue nachrichtendienstliche Datenerhebungsbefugnisse zu Lasten eines effektiven Rechtsschutzes angemessene und effektive Garantien gegen den Missbrauch dieser Befugnisse darstellen, die der Europäische Gerichtshof für Menschenrechte als Voraussetzung für die Vereinbarkeit eines staatliches Systems der heimlichen Überwachung zur Spionage- und Terrorismusbekämpfung angesehen hat[8].

Außerdem soll das Bundesamt für Verfassungsschutz zur Überwachung des Mobilfunkverkehrs, insbesondere zur Feststellung von Geräte- und Kartennummern und zur Ermittlung des Standortes von Mobilfunkteilnehmern, sog. IMSI-Catcher einsetzen dürfen. Die Voraussetzungen dafür sind im Gesetz nur unscharf festgelegt. Auch hat es der Gesetzgeber versäumt, zunächst die technischen Bedenken der Mobilfunkbetreiber auszuräumen, die darauf hingewiesen haben, dass der Einsatz von IMSI-Catchern die Stabilität und Funktionsfähigkeit eines ganzen Telekommunikationsnetzes zeitweise gefährden kann. Da der IMSI-Catcher technisch im Netz als eine scheinbare Basisstation agiert, fängt er alle in einem bestimmten Umkreis ausgesendeten Kennungen von Mobilfunkgeräten auf und kann unter Umständen auch das Absetzen von Notrufen unmöglich machen.

Gegen die ursprüngliche Absicht des Bundesinnenministers, auf dem Verordnungswege nicht näher benannte biometrische und möglicherweise sogar genetische Merkmale in die Pässe und Personalausweise der Bundesbürger aufzunehmen, hatten auch die Datenschutzbeauftragten des Bundes und der Länder entschiedenen Widerspruch angemeldet[9]. Im Zuge der parlamentarischen Beratung wurde der Gesetzentwurf in diesen Punkten insoweit etwas verbessert, als nun der Gesetzgeber zumindest wesentliche Entscheidungen selbst getroffen hat, wie es die Verfassung bei Grundrechtseingriffen gebietet.

---

6 s. dazu unten A 1.3

7 BVerfGE 30, 1

8 grundlegend der Beschluss vom 18.11.1977 (Fall Klass und andere), EGMR, Serie A Nr. 28, S. 23

9 Entschließung der 62. Konferenz, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.3

Danach kann durch eine – noch nicht erfolgte – Änderung des Pass- und des Personalausweisgesetzes die Aufnahme biometrischer Merkmale (Finger- oder Handabdrücke, Gesichtserkennung) zum Zweck der Identifizierung in die Personaldokumente von Deutschen vorgeschrieben werden. Die Aufnahme genetischer Informationen bleibt damit weiter ausgeschlossen. Um die Einführung eines verfassungswidrigen Personenkennzeichens und einer zentralen Registrierung der gesamten deutschen Bevölkerung zu verhindern, hat der Gesetzgeber den Aufbau einer zentralen Referenzdatei für Ausweispapiere ausdrücklich untersagt. Zudem dienen die noch festzulegenden biometrischen Merkmale ausschließlich der Überprüfung, ob der Inhaber eines Ausweispapiers auch die in diesem Papier beschriebene Person ist (Authentifikation). Sie dienen nicht dem Ausschluss von Doppelidentitäten, also der eindeutigen Identifikation der betreffenden Person. Diese wäre ohnehin im internationalen Zusammenhang nicht möglich, weil sich verdächtige Personen ausländischer Reisepässe bedienen können, die diesen Vorschriften nicht unterliegen.

Das Bundeskriminalamt hat durch das Terrorismusbekämpfungsgesetz nicht die ursprünglich geplante Kompetenz zu eigenen verdachtsunabhängigen Initiativermittlungen erhalten. Dennoch kann es in größerem Umfang als bisher Daten zur Ergänzung vorhandener Sachverhalte auch dann bei öffentlichen und nicht öffentlichen Stellen erheben, wenn die Polizeien der Länder über die erforderlichen Daten bereits verfügen. Dies steht im Widerspruch zur lediglich unterstützenden Funktion des Bundeskriminalamtes als Zentralstelle[10]. Zudem erhöht sich dadurch die Gefahr von parallelen Datensammlungen auf Bundes- und Länderebene mit einschneidenden Folgen für die Betroffenen, z. B. wenn Daten unterschiedlich lange gespeichert bleiben[11].

Neben weiteren Änderungen des Sicherheitsüberprüfungsgesetzes enthält das Terrorismusbekämpfungsgesetz weit reichende Verschärfungen des Ausländergesetzes. Während bei Deutschen der Gesetzgeber über die Aufnahme biometrischer Merkmale in Ausweispapiere entscheiden soll, kann bei Ausländern der Bundesinnenminister diese Entscheidung durch Rechtsverordnung selbst treffen. Weshalb der Gesetzgeber diese Unterscheidung vorgenommen hat, ist nicht nachvollziehbar, zumal das Grundrecht auf Datenschutz Deutschen und Ausländern gleichermaßen zusteht. Möglicherweise notwendige Einschränkungen bedürfen in jedem Fall einer gesetzlichen Grundlage.

Außerdem dürfen bei Ausländern Sprachaufzeichnungen durchgeführt werden, um deren Herkunftsland oder Herkunftsort zu bestimmen, selbst wenn dies auf andere Weise möglich wäre. Eindeutige Voraussetzungen und Lö-

[10] § 2 BKAG

[11] s. dazu unten A 4.1.1

schungsregelungen fehlen insoweit, sodass ein Datenbestand über Sprachaufzeichnungen fast aller hier lebender Ausländer geschaffen werden kann.

Die erweiterten Befugnisse der Geheimdienste und des Bundeskriminalamtes sind auf fünf Jahre befristet worden. Zuvor sollen diese Regelungen evaluiert werden.

Das Terrorismusbekämpfungsgesetz 2001 enthält eine Vielzahl neuer Befugnisse für die Sicherheitsbehörden, die nicht auf einer sorgfältigen Analyse der bereits zuvor existierenden Befugnisse beruht. Das Gesetz ist geeignet, das verfassungsrechtlich verankerte Trennungsgebot zwischen den Strafverfolgungsbehörden einerseits und den Geheimdiensten andererseits in bedenklicher Weise zu relativieren. Die Möglichkeiten der geheimen Überwachung von Kontobewegungen, Reisetätigkeiten und Kommunikationsverbindungen werden erheblich ausgeweitet, ohne dass dementsprechende Möglichkeiten des individuellen Rechtsschutzes gegenüber stehen. Insgesamt lässt das Gesetz die notwendige sorgfältige Abwägung zwischen den Freiheitsrechten einerseits und den Sicherheitserfordernissen andererseits vermissen.

1.2 Entwicklung des Datenschutzrechts

Bereits am 23. Mai 2001 trat das neue Bundesdatenschutzgesetz mit den notwendigen Anpassungen an die Europäische Datenschutzrichtlinie von 1995 in Kraft[12]. Damit wurde zwar die erste Stufe der Modernisierung des deutschen Datenschutzrechts abgeschlossen[13]; das Bundesdatenschutzgesetz 2001 macht aber in seiner jetzt geltenden Fassung die Notwendigkeit einer umfassenden Modernisierung nur um so deutlicher. Zu diesem Zweck ist im Herbst 2001 das vom Bundesministerium des Innern in Auftrag gegebene Gutachten zur Modernisierung des Datenschutzrechtes vorgelegt worden[14]. Mit einer umfassenden Novellierung des Bundesdatenschutzgesetzes ist aber vor dem Ende der Legislaturperiode nicht mehr zu rechnen.

Mit dem Gutachten sind allerdings entscheidende Eckpunkte erarbeitet worden, die der Gesetzgeber bei einer grundlegenden Modernisierung des Datenschutzrechts wird berücksichtigen müssen. Vor allem muss das Datenschutzrecht den völlig neuartigen Entwicklungstendenzen bei der Datenverarbeitungstechnik Rechnung tragen. Datenverarbeitung wird zunehmend allgegenwärtig („ubiquitous“ oder „pervasive computing“) in Alltagsgegenstände

[12] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001, BGBl. I S. 904

[13] s. dazu Tätigkeitsbericht 2000, A 1.1.1

[14] Rossnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts (herausgegeben vom Bundesministerium des Innern)

eingebaut sein. Das Auto wird mit Hilfe kontaktloser Datenübertragungstechniken seinen Besitzer erkennen, die Heizung den Hausbewohner, der Schuhabsatz oder der Ohrring den Gesprächspartner. Alle diese Gegenstände werden Wünsche der jeweiligen Berechtigten speichern, sich auf sie einstellen oder sie an notwendige Entscheidungen erinnern. In nicht allzu ferner Zukunft wird niemand mehr sicher vorhersagen können, welche Daten in welchen Gegenständen gespeichert sind und zwischen ihnen übertragen werden. Für eine solche Technologie ist das gegenwärtige Datenschutzrecht praktisch ungeeignet, obwohl der Schutz der Persönlichkeitssphäre und des informationellen Selbstbestimmungsrechts es gebietet, hierfür wirksame Regelungen zu entwickeln.

Es geht nicht mehr allein um eine Überwachung des Einzelnen durch den Staat, sondern durch die alltägliche Umgebung, also durch Gebrauchsgegenstände, deren elektronisches Gedächtnis auch von interessierten Dritten angezapft oder genutzt werden kann. Auch die Entwicklung im Internet zeigt, dass jede Form der Kommunikation oder des Informationsabrufs zunehmend registriert und überwacht werden kann, was nicht nur für staatliche Stellen, sondern ebenso für Netzbetreiber, Inhaltsanbieter, Werbetreibende, Personalchefs oder Neugierige gilt.

Die Gutachter haben eine Reihe von Vorschlägen gemacht, wie ein modernes Datenschutzrecht auf diese technische Entwicklung reagieren sollte. Im Vordergrund steht dabei die Stärkung der schon im neuen Bundesdatenschutzgesetz angelegten Vorgaben des Systemdatenschutzes, die Prinzipien der Datenvermeidung und der Datensparsamkeit sowie das Angebot effektiver Möglichkeiten des Selbstschutzes.

Insgesamt kommt es darauf an, dass das zukünftige modernisierte Datenschutzrecht den Herausforderungen einer schnellen technischen Entwicklung besser gerecht wird als das bisher geltende Bundesdatenschutzgesetz, ohne das Schutzniveau für die einzelnen Grundrechtsträger zu verringern. Im Gegenteil müssen Schutzlücken im bisherigen Datenschutzkonzept geschlossen und die Regelungen so technik-unabhängig gestaltet werden, dass in Zukunft mit Sicherheit zu erwartende weitere technische Entwicklungen die rechtlichen Regelungen nicht alsbald obsolet machen.

Der Datenschutz mit seinen Komponenten des Datenschutzrechts und der datenschutzfreundlichen Technik und Organisation wird angesichts der schnellen Entwicklung der Informations- und Kommunikationstechnik immer wichtiger. Die Autonomie des Einzelnen muss dauerhaft gestärkt werden. Das Gutachten zur Modernisierung des Datenschutzrechts stellt eine geeignete Grundlage für die jetzt notwendige gesetzliche Neureglung dar.

1.3 Rasterfahndung nach den Anschlägen vom 11. September

Da sich bald nach den Terror-Anschlägen die Erkenntnis verdichtete, dass einige Tatverdächtige zuvor längere Zeit in Deutschland gelebt hatten, leitete der Generalbundesanwalt entsprechende Ermittlungen gegen mögliche Mittäter ein. Er lehnte es aber ab, eine nach der Strafprozessordnung mögliche bundesweite Rasterfahndung anzuordnen. Statt dessen kamen die Landeskriminalämter und das Bundeskriminalamt überein, durch die Länder eine präventiv-polizeiliche Rasterfahndung nach möglichst einheitlichen Kriterien durchzuführen, um der Gefahr durch „Schläfer" zu begegnen, von denen in Zukunft ähnliche terroristische Aktivitäten zu erwarten sein könnten. Im Zuge dieser Rasterfahndung wurden in Brandenburg Datensätze zu einer sechsstelligen Anzahl von Personen an das Landeskriminalamt übermittelt, von denen rund 19.000 auch bei Redaktionsschluss dieses Berichts dort noch gespeichert waren.

Auf Antrag des Landeskriminalamtes hatte das zuständige Amtsgericht Eberswalde gemäß § 46 Brandenburgisches Polizeigesetz (BbgPolG) am 21. September 2001[15] zunächst angeordnet, dass alle Einwohnermeldeämter, Ausländerbehörden und Sozialämter, Universitäten und Hochschulen sowie sicherheitsrelevante nicht öffentliche Stellen des Landes Brandenburg bezogen auf die zunächst vorgesehenen Rasterkriterien

- männlich,
- Mindestalter 18, aber nicht älter als 25 Jahre,
- islamischer Religionszugehöriger bzw. Angehöriger eines relevanten Staates,
- Meldeanschrift in Brandenburg,
- legaler Aufenthaltsstatus ohne räumliche Beschränkung,
- keine kriminalpolizeilichen Erkenntnisse,
- keine eigenen Kinder,
- keine Sozialhilfeempfänger

die bei ihnen vorhandenen Daten zu

- Geschlecht,
- Alter,
- Religionsangehörigkeit,
- Meldeanschrift,
- Nebenwohnungen,

[15] Az.: 1 Gs 378/01

- Kinder

über die von 1996 bis 2001 in Brandenburg gemeldeten entsprechenden Personen an die Polizei zu übermitteln hätten. Dem Antrag des Landeskriminalamtes war eine Liste mit Herkunftsstaaten beigefügt. Wenig später modifizierte das Landeskriminalamt den ersten Antrag durch einen zweiten dahingehend, dass der Kriterienkatalog auf

- männlich,
- 18 bis 50 Jahre,
- Nationalität entsprechend der geänderten Länderliste

reduziert werden solle.

Zusätzlich wurden damit auch Staatenlose, Personen mit unbekannter Nationalität und deutsche Staatsangehörige mit nicht deutschem Geburtsort in die Rasterfahndung einbezogen.

Die Einwohnermeldeämter in Brandenburg sollten hinsichtlich der in den letzten fünf Jahren in Brandenburg gemeldeten relevanten Personen die Daten über Geschlecht, Alter, Religionsangehörigkeit, Meldeanschrift, Nebenwohnungen, Kinder mitteilen, die Ausländerbehörden Aufenthaltsort und Aufenthaltsstatus und die Sozialämter den Datenbestand um Informationen „bezüglich der Sozialhilfe“ ergänzen. Die Universitäten und Hochschulen hatten schließlich für den genannten Zeitraum die Daten über immatrikulierte oder ehemals immatrikulierte Studenten zu übermitteln.

Das Amtsgericht Eberswalde folgte diesem zweiten Antrag des Landeskriminalamtes ebenso wie dem ersten ohne Begründung und ordnete durch Beschluss vom 1.10.2001[16] die Rasterfahndung in der Weise an, dass die Polizei des Landes Brandenburg von öffentlichen Stellen und Stellen außerhalb des öffentlichen Bereiches die Übermittlung von personenbezogenen Daten „zum Zwecke des Abgleichs mit anderen Datenbeständen“ verlangen konnte.

Das Landeskriminalamt wies die verpflichteten Stellen in seinem Ersuchen um die Übermittlung der gerasterten Personendatensätze darauf hin, dass der Katalog der Rasterkriterien in der Weise anzuwenden sei, dass in Fällen, in denen zu einer Person über ein Rasterungsmerkmal bei der betreffenden Behörde keine Informationen vorlägen, dennoch alle übrigen Daten zu übermitteln seien. Dies betraf insbesondere die Meldebehörden, die zwar Daten über die Zugehörigkeit zur evangelischen oder römisch-katholischen Kirche in den Melderegistern führen, nicht jedoch über die Tatsache, dass sich eine Person zum Islam bekennt.

[16] Az.: 1 Gs 396/01

Das Landeskriminalamt richtete bis zum Ende des Berichtszeitraumes keine Übermittlungsersuchen an nicht öffentliche Stellen oder Sozialämter in Brandenburg.

Bei der Durchführung der Rasterfahndung hatten zahlreiche Meldebehörden, insbesondere in kleineren Gemeinden, erhebliche praktische Schwierigkeiten, aus ihrem Datenbestand diejenigen Personendatensätze „herauszurastern“, die dem vorgegebenen Profil entsprachen. Sie übermittelten deshalb ihren gesamten Datenbestand oder wesentlich mehr Daten als gefordert an die Polizei, bei der die erforderliche Recherchetechnik zur Durchführung der Rasterung vorhanden war. Größere Städte und Gemeinden, die über die entsprechende Software für das Meldewesen verfügten, nahmen die Rasterung dagegen selbst vor und übermittelten entsprechend dem Beschluss des Amtsgerichtes auch die Daten aller Personen deutscher Staatsangehörigkeit mit ausländischem Geburtsort, also unter anderem auch die Datensätze aller Spätaussiedler aus Russland oder die Daten von beispielsweise in den USA geborenen Studenten.

Anfang November 2001 waren alle von den beteiligten Behörden angeforderten Datensätze beim Zentraldienst für Technik und Beschaffung der brandenburgischen Polizei eingegangen, dort in ein einheitliches Datenformat umgewandelt und fortlaufend an das Landeskriminalamt übermittelt worden. Dieses übernahm die Daten in die Datei „Rasterfahndung Brandenburg“ und erstellte durch mehrere automatisierte Recherchеläufe den eigentlichen Rasterbestand, der die für die Gefahrensituation relevanten Datensätze enthält. Dieser Datenbestand umfasst selbst nach Löschung irrelevanter Informationen noch rund 19.000 personenbezogene Datensätze. Das Landeskriminalamt hat diesen Bestand nach dem Grad der potentiellen Gefährdung, die von den Betroffenen ausgehen könnte, in unterschiedliche Kategorien eingeteilt. Vorrangig hat die Polizei damit begonnen, die Personen mit einer besonderen Häufung von einschlägigen Merkmalen daraufhin zu überprüfen, ob im Einzelfall Anhaltspunkte für die Vorbereitung terroristischer Anschläge gegeben sind.

Gleichzeitig wurden die „Trefferbestände“ der Länder mit weiteren, bundesweit erhobenen Daten abgeglichen. Zu diesem Zweck ist im Bundeskriminalamt die Datei „Schläfer“ aufgebaut worden, in der Daten enthalten sind, die das Bundeskriminalamt bei zahlreichen privaten Stellen im gesamten Bundesgebiet erhoben hat. Durch den Abgleich sollen die Datensätze der Länder ergänzt werden.

Das Landeskriminalamt hat uns mitgeteilt, dass die Rasterfahndung in Brandenburg wahrscheinlich Ende April 2002 abgeschlossen sein wird. Bisher

sind lediglich die Datenträger mit den von den Melde- und Ausländerbehörden sowie den Universitäten und Hochschulen angelieferten Rohdaten vernichtet worden. Die Datensätze von Deutschen mit ausländischem Geburtsort in „unverdächtigen“ Ländern (USA, Russland) werden jeweils aus der Datei „Rasterfahndung Brandenburg“ gelöscht, wenn ein solcher Datensatz bei der Nutzung der Datei auffällt. Eine automatisierte Löschung einer größeren Anzahl von Datensätzen, die offensichtlich nicht auf „relevante Personen“, also potentielle Terroristen, verweisen, ist nach Angaben der Polizei nicht möglich, weil die Software dies nicht zulässt.

Die Rasterfahndung ist nach dem Brandenburgischen Polizeigesetz an strenge Anforderungen gebunden, denn sie macht eine große Zahl von Personen zum Gegenstand der polizeilichen Datenverarbeitung, bei denen zunächst unklar ist, ob von ihnen eine „gegenwärtige Gefahr“ ausgeht. Diese Personen sind deshalb keine Störer im polizeirechtlichen Sinne. Gleichwohl liegt in der Einbeziehung ihrer Datensätze – noch dazu mit so sensiblen Informationen wie der Religionszugehörigkeit – eine massiver Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung. Dieser Eingriff ist nur gerechtfertigt, wenn die strikten Voraussetzungen des Polizeigesetzes (§ 46) erfüllt sind. Die Rasterfahndungsvorschrift dient dem Schutz aller von dieser Maßnahme Betroffenen und hat grundrechtssichernden Charakter. Bei der Anwendung dieser Vorschrift ist daher stets zu berücksichtigen, dass der massenhafte Grundrechtseingriff zahlenmäßig und zeitlich so eng wie möglich begrenzt werden muss.

Vor diesem Hintergrund ist bis zum Ende des Berichtszeitraumes zur Rasterfahndung in Brandenburg Folgendes festzustellen:

1. Die Voraussetzung einer „gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person“ haben das Landeskriminalamt und das Amtsgericht Eberswalde unter dem Eindruck der Anschläge in den USA als gegeben angesehen. Davon hat die datenschutzrechtliche Bewertung auszugehen. Ob die Beschlüsse des Amtsgerichts Eberswalde einer weiteren gerichtlichen Überprüfung Stand gehalten hätten, ist fraglich. In anderen Bundesländern haben Gerichte das Vorliegen einer gegenwärtigen Gefahr geprüft und ähnliche Anordnungen aufgehoben oder ihre erneute Überprüfung angeordnet[17]. In Brandenburg sind die Beschlüsse nicht mit gerichtlichen Mitteln angegriffen worden und insoweit vollziehbar.

2. Das Landeskriminalamt hat entgegen dem eindeutigen Wortlaut des § 46 BbgPolG von vornherein die Erstreckung der Rasterfahndung auf die Da-

[17] OLG Frankfurt/Main, Beschluss v. 8.1.2002 - 20 W 479/01; LG Berlin, Beschluss v. 16.1.2002 – 84 T 278, 288, 289, 308, 309, 318, 351/01, 84 T 8/02

ten solcher „relevanter“ Personen beantragt, die Sozialhilfe bezogen oder beziehen. Das Polizeigesetz schließt die Einbeziehung von Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen, in die Rasterfahndung ausdrücklich aus (§ 46 Abs. 2 Satz 1 BbgPolG). Das Amtsgericht Eberswalde ist dem Antrag der Polizei auch insoweit ohne Einschränkung und ohne Begründung gefolgt. Erst mit dem In-Kraft-Treten des Terrorismusbekämpfungsgesetzes am 1. Januar 2002 ist die Durchbrechung des Sozialgeheimnisses für Zwecke der Rasterfahndung zugelassen worden. Bis zu diesem Zeitpunkt war von der zu Unrecht beantragten und angeordneten Rasterung von Sozialdaten in Brandenburg kein Gebrauch gemacht worden.

3. Das Verfahren vieler kleiner kommunaler Meldebehörden, ihren Datenbestand insgesamt dem Landeskriminalamt zu übermitteln, entsprach den polizeirechtlichen Vorgaben, soweit es ihnen wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwandes nicht möglich war, die Rasterung selbst durchzuführen. Diese sog. Überschussinformationen dürfen von der Polizei nicht genutzt werden (§ 46 Abs. 2 Satz 2 BbgPolG).

4. Die Behörden und Hochschulen, die Daten an das Landeskriminalamt übermittelt haben, waren hierzu aufgrund des Polizeigesetzes befugt und insoweit zur Amtshilfe verpflichtet. Private Stellen hätten zur Datenübermittlung dagegen nicht verpflichtet werden können, weil das Polizeigesetz hierfür keine Grundlage enthält.

5. Von zentraler Bedeutung ist die Frage, wer datenschutzrechtlich für die Rasterfahndung in Brandenburg verantwortlich ist. Dies ist nicht das Bundeskriminalamt, das keine eigene Befugnis zur Durchführung einer Rasterfahndung hat und auch nach dem In-Kraft-Treten des Terrorismusbekämpfungsgesetzes lediglich eine unterstützende Funktion als Zentralstelle für die Polizeien der Länder hat (§ 2 Abs. 1 Bundeskriminalamtsgesetz).

   Das Landeskriminalamt bleibt datenschutzrechtlich allein für die Durchführung der Rasterfahndung im Land Brandenburg verantwortlich. Personenbezogene Daten darf es dem Bundeskriminalamt im Wege einer Datenverarbeitung im Auftrag zur Verfügung stellen. Dieses hat die Daten nach den Weisungen des Landeskriminalamtes zu verarbeiten und zu nutzen (§ 2 Abs. 5 BKAG). Das gilt gerade auch bezüglich des Abgleichs brandenburgischer Daten mit der Datei „Schläfer“ und der Anreicherung der Datensätze durch Informationen, die das Bundeskriminalamt selbst bundesweit bei privaten Stellen erhoben hat.

Die Rechtmäßigkeit dieser Datenerhebung mit dem Ziel eines automatisierten Datenabgleichs stößt im Übrigen auf erhebliche Zweifel. Das Bundeskriminalamt stützt sich insoweit auf eine einfache Datenerhebungsvorschrift (§ 7 Abs. 2 BKAG) und meint, es könne auf diese Weise Daten erheben, die ihm freiwillig von privaten Unternehmen (z. B. Energieversorgungsunternehmen) und Verbänden zur Verfügung gestellt worden sind. Das rechtfertigt aber nicht die Einbeziehung dieser Daten in einen massenhaften Datenabgleich, den das Bundeskriminalamt nicht durchführen darf. Für Brandenburg ist dies relevant, da das hiesige Landeskriminalamt als Auftraggeber sicherstellen muss, dass Datensätze aus Brandenburg nur mit solchen Datensätzen abgeglichen werden, die ihrerseits rechtmäßig erhoben worden sind.

Das Landeskriminalamt hätte dem Bundeskriminalamt klare Weisungen erteilen müssen, mit welchen Datenbeständen relevante Datensätze aus Brandenburg abgeglichen werden sollen und was mit ihnen anschließend zu geschehen hat. Entsprechende Weisungen hat das Landeskriminalamt uns bisher nicht vorgelegt. Vieles deutet darauf hin, dass das Bundeskriminalamt im Zuge der bundesweiten Rasterfahndung nach dem 11. September 2001 seine gesetzliche Unterstützungsfunktion erheblich überschritten und sich faktisch zum Herren des Verfahrens gemacht hat.

6. Alle Überlegungen bei der Polizei und im Innenministerium, die darauf zielen, Erkenntnisse aus dem automatisierten Rasterungsabgleich, die in keinem Zusammenhang mit der wahrgenommenen gegenwärtigen Gefahr terroristischer Anschläge stehen (Zufallsfunde), für andere Zwecke – etwa zur Aufdeckung möglicher Fälle von Sozialleistungsmissbrauch – zu verwenden, überschreiten eindeutige rechtliche Grenzen. Das Polizeigesetz schreibt vor, dass alle übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen bzw. zu vernichten sind, sobald der Zweck der Maßnahme erreicht ist oder sich zeigt, das er nicht erreicht werden kann. Daraus folgt, dass eine Zweckentfremdung von Daten, die im Zuge des automatisierten Abgleichs anfallen, unzulässig ist. Von der Löschungsverpflichtung sind nur diejenigen Daten und Akten ausgenommen, die für ein mit dem Sachverhalt (also mit der Abwehr der gegenwärtigen Gefahr) zusammenhängendes Verfahren erforderlich sind. Jede zweckfremde Verwendung von Daten aus der Rasterfahndung ist zu beanstanden.

7. Da die Rasterfahndung nur zur Abwehr einer gegenwärtigen Gefahr zulässig ist, ergibt sich zwingend, dass eine frühestmögliche Löschung all der Datensätze geboten ist, die für die Abwehr dieser Gefahr irrelevant sind. Das Landeskriminalamt beabsichtigt, die Rasterfahndung erst ein halbes Jahr nach dem Zeitpunkt für beendet zu erklären, zu dem die meisten an-

geforderten Daten angeliefert worden sind. Über diesen Zeitraum bleiben zum größten Teil Datensätze von Personen in der Datei „Rasterfahndung“ des Landeskriminalamtes, bei denen die bisherigen Datenabgleiche keinerlei Anhaltspunkte für eine Gefährder-Eigenschaft ergeben haben. Die hohe Zahl der gespeicherten Datensätze beruht vor allem auf den unscharfen Rasterkriterien, die wiederum auf die verfügbaren polizeilichen Erkenntnisse zurückzuführen sind. Das Dilemma der Polizei, einer schwer einzugrenzenden Gefahr mit unscharfen Rasterungskriterien begegnen zu müssen, darf aber nicht dazu führen, dass der massenhafte Eingriff in die Grundrechte Unbescholtener zeitlich ausufert. Das Landeskriminalamt hat erklärt, es wolle die Daten gleichwohl noch für den Fall vorhalten, dass das Bundeskriminalamt auf neue Rasterkriterien hinweist, anhand derer der gesamte Datenbestand nochmals zu überprüfen wäre. Ein solcher Abgleich ist zum einen von dem Beschluss des Amtsgerichtes Eberswalde nicht mehr gedeckt. Es müssten zuvor neue richterliche Anordnungen eingeholt werden. Zum anderen wäre ein neuerlicher Abgleich angesichts der mangelnden Aktualität der Daten auch kaum noch aussagefähig.

8. Entscheidend ist schließlich, dass das Landeskriminalamt die Rasterfahndung jetzt ohne weitere Verzögerung beenden muss. Damit sind alle für die weitere Fahndung nicht mehr benötigten Daten zu löschen (§ 46 Abs. 3 und 5 BbgPolG).

   Es ist nicht hinnehmbar, dass sensible personenbezogene Daten solcher Personen, für deren Gefährlichkeit die Polizei keine Anhaltspunkte hat, selbst ein halbes Jahr nach Beginn der Rasterfahndung noch gespeichert bleiben. Der anhaltende Eingriff in die Grundrechte dieser offensichtlich unbescholtenen Mehrzahl der vom Datenabgleich Betroffenen wird auch nicht dadurch gerechtfertigt, dass bei einem Bruchteil der „Trefferfälle“ weitere Ermittlungen stattfinden. Vollkommen inakzeptabel ist es, von einer automatischen Löschung abzusehen oder die Löschung nur „von Hand“ vorzunehmen, weil der Polizei die entsprechende Software fehlt.

9. Die Rasterfahndung sollte nach ihrem Abschluss kritisch evaluiert werden. Der Gesetzgeber ist von Verfassungs wegen gehalten, Grundrechtseinschränkungen in regelmäßigen Abständen zu überprüfen. Erweisen sie sich als ungeeignet zur Erreichung des angestrebten Zweckes, steht ihre Verfassungsmäßigkeit in Frage.

Jede Rasterfahndung führt zu massenhaften Eingriffen in die Grundrechte unverdächtiger Personen. Sie ist deshalb nur unter engsten Voraussetzungen zulässig. Die Einhaltung dieser Voraussetzungen ist strikt zu überwachen. Die Rasterfahndung in Brandenburg muss jetzt beendet und alle Datensätze, die nicht für konkrete Ermittlungen zur Abwehr einer gegenwärtigen Gefahr benötigt werden, müssen umgehend gelöscht werden. Das Ergebnis der Rasterfahndung ist kritisch zu evaluieren.

1.4 Die Überwachung der Telekommunikation weitet sich aus – mit zweifelhaftem Effekt

Die technisch vermittelte Kommunikation in Form der Sprachtelefonie, des Datenaustausches über elektronische Post oder der sekundenschnellen Übermittlung von Bild- oder Tondateien über das Internet nimmt weiter rasant zu. Eine wesentliche Voraussetzung für die Sicherheit der Infrastruktur ist die Verhinderung unbefugter Zugriffe und der Manipulation der übermittelten Daten. Dieses Vertrauen stützte sich bisher auf die verfassungsrechtliche Garantie des Telekommunikationsgeheimnisses. Das Bundesverfassungsgericht hat 1999 die zentrale - Bedeutung dieses Grundrechts für die Kommunikation in einer freien Gesellschaft hervorgehoben[18]. Zulässig ist die Fernmeldeüberwachung zwar seit langem zur Verfolgung bestimmter schwerer, auch terroristischer Straftaten, zur Bekämpfung verfassungswidriger Bestrebungen, zur Spionageabwehr und zur Kontrolle illegaler Waffenexporte. Entscheidend ist aber, dass die heimliche Überwachung der Telekommunikation stets nur im Rahmen enger rechtlicher Grenzen stattfinden darf, um den Kernbereich des Telekommunikationsgeheimnisses nicht zu gefährden.

Ob die Verfassungswirklichkeit diesem Grundsatz noch entspricht, wird zunehmend fraglich. Die Zahl der richterlichen Abhöranordnungen hat sich in den Jahren 1997 bis 2000 bundesweit mehr als verdoppelt. Dies wird von Seiten der Sicherheitsbehörden mit der stark angestiegenen Zahl von Handys und Internetzugängen begründet. Dabei lässt die Statistik das wahre Ausmaß der Überwachung nicht erkennen, weil sie nur die Überwachungsmaßnahmen nennt, ohne Auskunft über die Zahl der betroffenen Gesprächs- oder Kommunikationsteilnehmer zu geben.

Die Überwachung des Telekommunikationsverkehrs droht zu einer Standardmaßnahme der Strafverfolgungsbehörden zu werden, die nahezu routinemäßig angeordnet wird. Dies entspricht nicht dem Ausnahmecharakter dieses Eingriffs in das Telekommunikationsgeheimnis. Auch die rechtsstaatli-

18. BVerfGE 100, 313, 381; s. auch Tätigkeitsbericht 1999, A 3.1

che Begrenzungsfunktion des von der Strafprozessordnung vorgeschriebenen Verdachts einer gravierenden Straftat scheint in der Praxis an Bedeutung zu verlieren.

Die von der Bundesregierung in Auftrag gegebene wissenschaftliche Evaluation, ist immer noch nicht abgeschlossen. Von ihr wird auch abhängen, ob die von den Regierungsfraktionen des Deutschen Bundestages angekündigte kritische Überprüfung der ständig ausgeweiteten Abhörbefugnisse in Angriff genommen wird.

1.4.1 Gesetz zu Artikel 10 Grundgesetz

Bereits im Juni 2001 hatte der Bundesgesetzgeber durch das Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) die Regelungen zur Telekommunikations-, Brief- und Postüberwachung für die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst neu geregelt[19]. Auslöser dafür war die Entscheidung des Bundesverfassungsgerichts vom Juli 1999 zur verdachtslosen Rasterfahndung durch die Nachrichtendienste, deren bisherige Regelung in Teilen für verfassungswidrig erklärt worden war. Der Bundesgesetzgeber hat zum einen die festgestellten verfassungsrechtlichen Mängel im alten G10-Gesetz behoben, zum anderen aber die Eingriffs- und Übermittlungsbefugnisse der Nachrichtendienste ausgeweitet und der technischen Entwicklung angepasst. Die strategische Überwachung des internationalen Telekommunikationsverkehrs, die bisher nur beim nicht leitungsgebundenen (satellitengestützten) Verkehr zulässig war, ist auf die gesamte Telekommunikation erstreckt worden, sobald eine gebündelte Übertragung erfolgt. Mit Hilfe von Suchbegriffen und Sprachdatenbanken wird der Überwachungsvorgang automatisch ausgelöst. Auf diese Weise soll die Gefahr internationaler terroristischer Anschläge rechtzeitig erkannt und ihr begegnet werden. Wohlgemerkt: diese Erweiterung der Überwachungsbefugnisse für die Nachrichtendienste erfolgte bereits vor dem 11. September 2001. Dennoch wurden diese Befugnisse Anfang 2002 durch das Terrorismusbekämpfungsgesetz noch drastisch ausgeweitet[20].

Datenschutzrechtliche Kritik an zahlreichen Regelungen des Entwurfs zum G10-Gesetz hat der Gesetzgeber allerdings nicht berücksichtigt [21]. So wurde versäumt, die Anforderungen an die Berichtspflicht gegenüber dem parlamentarischen Kontrollgremium und dem Bundestag zu präzisieren. Die Erweiterung der Überwachungsbefugnisse auf mutmaßliche Einzeltäter auch

[19] Gesetz vom 26.6.2001, BGBl. I S. 1254

[20] s. dazu oben A 1.1

[21] vgl. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9.3.2001, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.1

außerhalb der Staatsschutzdelikte stellt zudem das verfassungsrechtliche Trennungsgebot für Nachrichtendienste und Polizei weiter in Frage. Das Bundesverfassungsgericht hat eine detaillierte Kennzeichnung von Daten, die aus G10-Maßnahmen stammen, gefordert; der Gesetzgeber lässt hiervon Ausnahmen zu, die datenschutzrechtlich äußerst bedenklich sind. Darüber hinaus ist eine dauerhafte Ausnahme von der Pflicht zur nachträglichen Benachrichtigung der überwachten Person vorgesehen, wenn die G10-Kommission bei der strategischen Fernmeldeaufklärung festgestellt hat, dass auch fünf Jahre nach dem Ende der Überwachungsmaßnahme nicht ausgeschlossen werden kann, dass die Benachrichtigung den Zweck dieser Maßnahme gefährden könnte. Diese Regelung, die der Gesetzgeber 1994 vorübergehend aus dem Gesetz gestrichen und jetzt wieder aufgenommen hat, dürfte einer verfassungsgerichtlichen Überprüfung nicht standhalten. Denn die Mitteilung an Betroffene ist die Grundvoraussetzung dafür, dass diese zumindest nachträglich die Rechtmäßigkeit der heimlichen Überwachungsmaßnahme überprüfen können. Die jetzige Regelung führt zu einem faktischen Ausschluss des grundgesetzlich garantierten Rechtsschutzes.

Bei der Neuregelung der Beschränkung des Brief-, Post- und Fernmeldegeheimnisses durch die Nachrichtendienste sind keine erheblichen datenschutzrechtlichen Verbesserungen erfolgt.

1.4.2 Telekommunikationsüberwachungsverordnung

Zur technischen Umsetzung der in der Strafprozessordnung, im G10-Gesetz und im Außenwirtschaftsgesetz vorgesehenen materiellen Überwachungsbefugnisse hat die Bundesregierung im Oktober 2001 nach kontroverser öffentlicher Diskussion die Telekommunikationsüberwachungsverordnung beschlossen[22]. Diese Verordnung enthält keine materiellen Überwachungsbefugnisse, sondern schreibt lediglich die Einrichtung von Überwachungsschnittstellen vor, die bei Vorliegen entsprechender richterlichen Anordnungen oder unter den Voraussetzungen des G10-Gesetzes die Überwachung der Telekommunikation technisch ermöglichen sollen. Zur Einrichtung solcher Überwachungsschnittstellen werden – entgegen früheren Verordnungsentwürfen – nur die lizenzpflichtigen Anbieter von Telekommunikationsdienstleistungen, also vor allem die Betreiber von Fest- und Mobilfunknetzen verpflichtet: alle anderen Anwender von Telekommunikationsanlagen und Verbindungsnetzen, Netzknoten und kleineren öffentlichen Telekommunikationsanlagen mit höchstens 1000 Teilnehmern (beispielsweise Nebenstellenanlagen) müssen zwar keine ständigen Schnittstellen einrichten, aber die Überwachung der Telekommunikation im Einzelfall ermöglichen, wenn dies angeordnet worden ist. Die Bundesregierung hat damit versucht, den vom Telekom-

[22] In Kraft seit 29.1.2002, BGBl. I 2001 S. 458

munikationsgesetz sehr weit gezogenen Kreis der Verpflichteten aus Gründen der Verhältnismäßigkeit, aber auch aus technischen Überlegungen einzuschränken.

Allerdings verpflichtet die Telekommunikationsüberwachungsverordnung auch alle Internet-Provider, die einen E-Mail-Dienst anbieten, zur Einrichtung dauernder Überwachungsfenster. Das widerspricht der Grundentscheidung des Gesetzgebers im Multimediarecht, die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreien Tele- oder Mediendienst zu betrachten. Denn wer seiner Pflicht zur Vorhaltung von Überwachungsschnittstellen nicht nachkommt, erhält nicht die notwendige Genehmigung zum Betrieb einer Telekommunikationsanlage. Die Verpflichtung der Internet-Provider macht es zudem jedenfalls technisch möglich, den gesamten Internetverkehr, also auch das bloße Surfen, zu überwachen. Dies ist nach deutschem Recht unzulässig .

Die demnächst vorgeschriebene technische Infrastruktur der Überwachung schießt über das zulässige Maß der Beobachtung von Kommunikation weit hinaus. Es muss sichergestellt werden, dass auch künftig die zunehmende Nutzung von Telediensten zu Alltagsgeschäften (E-Commerce) prinzipiell überwachungsfrei bleibt[23].

1.4.3 Nachfolgeregelung zu § 12 Fernmeldeanlagengesetz

Das Telekommunikationsgeheimnis schützt nicht nur den Inhalt eines Telefongespräches oder einer E-Mail, sondern in gleicher Weise auch die näheren Umstände der Kommunikation, also wer wann mit wem wie lange kommuniziert hat. Diese Informationen über die Begleitumstände der Telekommunikation können den Strafverfolgungsbehörden wichtige Hinweise zur Ergreifung der Täter geben.

Bisher konnte deshalb in allen strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über die Telekommunikation, also über die Verbindungsdaten zurückliegender Telefonate oder internetgestützter Kontakte nach § 12 Fernmeldeanlagengesetz verlangen. Diese Vorschrift stammte aus der Frühzeit der analogen Vermittlungstechnik und enthielt deshalb nicht die Beschränkungen auf besonders schwere Straftaten, wie sie die erst später eingeführten Befugnisse in der Strafprozessordnung zum Abhören aufweisen. Auskunft über Verbindungsdaten konnte deshalb auch bei der Verfolgung von Bagatellstraftaten verlangt werden. Dies war wegen der erheblich höheren Aussagefähigkeit der digita-

[23] Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 11.5.2001, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.2

len Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis verfassungsrechtlich seit längerem problematisch[24].

Deshalb ist es grundsätzlich zu begrüßen, dass der Bundesgesetzgeber den Auskunftsanspruch der Strafverfolgungsbehörden zu Verbindungsdaten in die Strafprozessordnung übernommen und an engere Voraussetzungen geknüpft hat[25]. Einige Landesjustizverwaltungen, darunter das Ministerium der Justiz und für Europaangelegenheiten hatten demgegenüber für eine Beibehaltung der verfassungsrechtlich problematischen Regelung des Fernmeldeanlagengesetzes plädiert.

Allerdings trägt auch die Neuregelung des Auskunftsanspruchs dem Schutzbedarf der Verbindungsdaten nicht hinreichend Rechnung. Der Gesetzgeber verpflichtet die geschäftsmäßigen Telekommunikationsanbieter auch bei solchen Straftaten zur Auskunftserteilung, bei denen ein inhaltliches Abhören der Kommunikation nicht angeordnet werden dürfte. Dieses geringere Schutzniveau der Begleitumstände einer Telekommunikation entspricht nicht den vom Bundesverfassungsgericht entwickelten Grundsätzen zum Schutzbereich des Artikel 10 GG. Es kann nicht generell davon ausgegangen werden, dass die Weitergabe von Verbindungsdaten einen weniger schwerwiegenden Eingriff in das Telekommunikationsgeheimnis darstellen als die inhaltliche Überwachung der Kommunikation; vielmehr sind auch Informationen über die Identität der Kommunikationspartner (etwa bei Gesprächen mit Ärzten oder Anwälten) als besonders schutzwürdig einzustufen.

Die neuen Pflichten zur Erteilung von Auskünften über Verbindungsdaten sind bis zum 1. Januar 2005 befristet. Die Bundesregierung hat dies mit ihrer Absicht begründet, nach Vorliegen der Ergebnisse der rechtstatsächlichen Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht, zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation ein Gesamtkonzept zur Regelung heimlicher Ermittlungsmaßnahmen zu erarbeiten und in die Strafprozessordnung einzustellen.

Das Telekommunikationsgeheimnis schützt nicht nur den Inhalt eines Telefonats oder einer E-Mail, sondern auch deren Verbindungsdaten.

[24] zuletzt Entschließung vom 14./15.3.2000 („Für eine freie Telekommunikation in einer freien Gesellschaft“), Dokumente zum Datenschutz 2000, A.I.1

[25] Gesetz vom 20.12.2001, BGBl. I S. 3879

1.4.4 ECHELON und Cybercrime-Konvention

Telekommunikationsüberwachung findet seit jeher auch im internationalen Rahmen statt, wobei unterschieden werden muss zwischen der Tätigkeit von Nachrichtendiensten einerseits und von Strafverfolgungsbehörden andererseits.

Schon im Sommer 2000 hatte der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Rahmen einer Expertenanhörung vor dem Bundestagsausschuss für Angelegenheiten der Europäischen Union zu dem globalen Abhörsystem Stellung genommen. Das Europäische Parlament hat in einer grundlegenden Entschließung vom September 2001 die Existenz dieses Abhörsystems, das unter dem Kürzel „ECHELON“ firmiert, bestätigt. Es wird unter Beteiligung der Vereinigten Staaten, des Vereinigten Königsreichs, Kanadas, Australiens und Neuseelands betrieben[26]. Das Europäische Parlament hat konkrete Empfehlungen zur Stärkung des Schutzes der Privatsphäre auf europäischer und internationaler Ebene gegeben und Maßnahmen zur Förderung des Selbstschutzes von Bürgern und Unternehmen empfohlen. So werden die Mitgliedstaaten aufgefordert, ihre Bürger und Unternehmen über die Möglichkeit zu informieren, dass ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden, und zugleich praktische Schritte zur Erhöhung der Sicherheit der Informationstechnik gefordert. Die Kommission und die Mitgliedstaaten werden aufgefordert, die Entwicklung benutzerfreundlicher Kryptosoftware, deren Quelltext offen gelegt ist, zu unterstützen und dafür zu sorgen, dass die öffentlichen Verwaltungen der Mitgliedstaaten Verschlüsselung von E-Mails systematisch einsetzen, um so langfristig Verschlüsselung zum Normalfall werden zu lassen. Dieser umfangreiche Forderungskatalog des Europäischen Parlaments ist auch durch die Ereignisse des 11. September 2001 nicht gegenstandslos geworden.

Der Verbesserung der internationalen Verfolgung von Datennetzkriminalität dient die am 23. November 2001 unterschriebene sog. Budapester Konvention gegen Datennetzkriminalität (Convention on Cybercrime[27]). Dieses vom Europarat initiierte Abkommen, das auch von einigen außereuropäischen Ländern unterzeichnet worden ist, tritt nach der Ratifikation durch fünf Unterzeichnerstaaten in Kraft. Es harmonisiert zum einen das materielle Computerstrafrecht, um international die gleichen Voraussetzungen für die Verfolgung entsprechender Straftaten zu schaffen; zum anderen soll die Zusammenarbeit zwischen den Strafverfolgungsbehörden nicht nur bei der Bekämp-

[26] Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) vom 5.9.2001, BR-Drs. 801/01

[27] European Treaty Series No. 185; vgl. hierzu Tätigkeitsbericht 2000, A 3.2

fung der eigentlichen Datennetzkriminalität, sondern auch bei der Verfolgung anderer Straftaten erleichtert werden, soweit zu ihrer Aufklärung rechnergestützte Informationen vorliegen und genutzt werden sollen. Die Konvention betrifft also sowohl Computer und Datennetze als Ziele krimineller Aktivität, als auch als Mittel zur Begehung von Straftaten oder der Spurensammlung zu ihrer Aufklärung.

Die von der Konferenz der Datenschutzbeauftragten geübte Kritik[28] hat nur zu wenigen Verbesserungen im Konventionstext geführt. Die Hauptkritik daran, dass Datenschutzgesichtspunkte trotz der langen Datenschutztradition des Europarates keinen Eingang in diesen ersten internationalen Vertrag zur Bekämpfung der Netzkriminalität gefunden haben, ist unberücksichtigt geblieben. Die Budapester Konvention beschränkt sich auf eine Angleichung der verfahrensmäßigen Voraussetzungen für eine zwischenstaatliche Zusammenarbeit und vernachlässigt die ebenso wichtige Harmonisierung der rechtsstaatlichen Schutzvorkehrungen für die Rechte auch unverdächtiger Dritter. Daran ändert der Umstand nichts, dass die Vertragsstaaten allgemein verpflichtet werden, einen angemessenen Schutz der Menschenrechte sicherzustellen, denn sie sind auch dann zur grenzüberschreitenden Kooperation verpflichtet, wenn der Empfängerstaat (auch außerhalb Europas) kein solches Schutzniveau vorsieht.

Allerdings schreibt die Cybercrime-Konvention keine Überwachungsschnittstelle vor und verpflichtet die Provider auch nicht, Verbindungs- oder Inhaltsdaten generell auf Vorrat für mögliche zukünftige Strafverfahren zu speichern. Die Provider im ersuchten Staat können lediglich verpflichtet werden, auf Anforderung der Strafverfolger in einem anderen Staat vorhandene Verbindungsdaten vorläufig „einzufrieren“, bis ein Richter nach nationalem Recht ihre Offenlegung in einem konkreten Strafverfahren angeordnet hat (sog. „fast freeze-quick thaw“-Verfahren).

1.4.5 Das Netz als Fahndungsplattform

International und national geben sich die Strafverfolgungsbehörden allerdings mit solchen Regelungen nicht zufrieden, obwohl von ihrer praktischen Umsetzung eine erhebliche Verbesserung der grenzüberschreitenden Zusammenarbeit und der Nutzung von Verbindungsdaten im Einzelfall zu erwarten ist. Vielmehr wird immer wieder die Forderung erhoben, Netzbetreiber und Provider sollten generell zur Speicherung aller Verbindungsdaten für eine bestimmte Mindestfrist unabhängig davon verpflichtet werden, ob diese Verbindungsdaten noch zur Abrechnung erforderlich sind. Damit sollten Verbin-

[28] vgl. Entschließung der 61. Konferenz, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.1; zur vorangegangenen Diskussion s. Tätigkeitsbericht 2000, A 3.2

dungsdaten nicht mehr nur zur Bekämpfung computergestützter oder gegen Datennetze gerichteter Kriminalität, sondern aller Straftaten dienen.

Um die Zusammenarbeit zwischen Strafverfolgungsbehörden und Telekommunikationsanbietern zu verbessern, hat die Europäische Kommission ein „Cybercrime-Forum“ ins Leben gerufen, bei dessen erster Plenarsitzung im November 2001 der Landesbeauftragte die Haltung der europäischen Datenschutzbeauftragten unterstützt hat. Anlässlich dieses Forums beschrieb ein britischer Polizeibeamter das Grundproblem der Bekämpfung von Datennetzkriminalität und die Schwierigkeit, einer Person eine im Internet begangene Straftat nachzuweisen. Das rechtfertigt es aber nicht, alle Nutzer des Netzes unter Verdacht zu stellen, indem ihre Daten für die Dauer eines Jahres gespeichert bleiben (wie es der britische Experte vorschlug). Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte sind solche pauschalen Eingriffe in das Grundrecht auf Privatsphäre nach Artikel 8 der Europäischen Menschenrechtskonvention unzulässig[29].

Eine Verwirklichung der auch im Bundesrat wiederholt erhobenen Forderungen[30] nach einer pauschalen Vorratsdatenspeicherung würde den Charakter der Telekommunikations- und Datennetze grundlegend verändern. Sie würden von Kommunikations- zu Überwachungsnetzen. Die Interessen der Strafverfolgungsbehörden rechtfertigen es in einem online-Medium ebenso wenig wie in der offline-Welt, jeden Menschen und jede seiner Bewegungen oder Äußerungen auf Vorrat zu registrieren und ihn einem Identifikationszwang zu unterwerfen. Nur im Einzelfall kann es ausnahmsweise gerechtfertigt sein, bei konkretem Verdacht und unter Einhaltung rechtsstaatlicher Verfahren auf ohnehin vorhandene Daten für Zwecke der Strafverfolgung zuzugreifen, die zunächst zu Zwecken der Kommunikation und der Abrechnung erhoben worden sind. Eine lückenlose Überwachung der technisch vermittelten Kommunikation zur Gewinnung von Verdachtsmomenten unabhängig von einem Verdacht im Einzelfall wäre mit der Verfassung einer freiheitlichen Informationsgesellschaft unvereinbar.

[29] Hierauf hat das Europäische Parlament in seiner ECHELON-Entschließung hingewiesen, BR-Drs. 801/01, S. 4

[30] Zuletzt Antrag der Freistaaten Bayern und Thüringen, BR-Drs. 1014/01

Das Telekommunikationsgeheimnis ist von zentraler Bedeutung für die Informationsgesellschaft. Beschränkungen dürfen nur im unerlässlichen Umfang erfolgen.

Die kritische Evaluation der immer weiter um sich greifenden Überwachung der Telekommunikation und eine Bereinigung der gesetzlichen Überwachungstatbestände sind vordringlich.

Eine generelle Registrierung aller Bewegungen im Netz auf Vorrat und ohne konkreten Verdacht wäre verfassungswidrig.

1.5 Videoüberwachung an allen Ecken und Enden?

1.5.1 Technische Möglichkeiten

Die Beobachtung mit Videokameras hat in den letzten Jahren stark zugenommen; in Deutschland sollen sich gegenwärtig über eine halbe Million Videoüberwachungsanlagen im Einsatz befinden. Deren technische Möglichkeiten sind wesentlich umfangreicher, als man auf den ersten Blick vermuten könnte.

Die Videotechnik geht heute über das bloße Aufzeichnen von Bildmaterial weit hinaus. Systeme zur automatischen digitalen Gesichtserkennung und der Analyse von „normalem“ und „verdächtigem“ Verhalten sind bereits im Einsatz. Videokameras in Miniaturausführung können von jedermann erworben und unsichtbar installiert werden. So lassen sich beispielsweise Kameras mit allen erforderlichen Hilfsfunktionen zur Energieversorgung und Bildübertragung in Lampen, Rauchmeldern, Radios oder hinter Spiegeln und Bildern verstecken. Handys nach dem UMTS-Standard werden alsbald in der Lage sein, Bilder von jedem beliebigen Ort über Mobilfunk zu senden. Die Aufnahmen können mit Hilfe von Empfangseinrichtungen in normalen Fernsehgeräten betrachtet, mit Videorecordern oder DVD-Recordern aufgezeichnet oder direkt über das Internet weltweit veröffentlicht werden. Die Zahl der auf diesem Markt tätigen Unternehmen wächst ständig und häufig ist gerade die Unsichtbarkeit der Überwachungstechnik ein schlagkräftiger Werbeslogan.

Ein Videoüberwachungsvorgang kann aus technischer Sicht in die folgenden vier Phasen eingeteilt werden:

- die Bilderfassung,
- die Bildübertragung,
- die Bildanzeige und -überwachung,
- die Bildspeicherung und -auswertung.

Die Bilderfassung kann in unterschiedlicher Art und Weise erfolgen. Sie reicht von unbeweglichen Kameras mit unveränderbarem Objektiv, die ein fest definiertes Beobachtungsfeld aufnehmen, bis hin zu vollständig beweglichen, elektronisch steuerbaren Kameras mit leistungsfähigen Zoomobjektiven. Möglich sind je nach eingesetzter Technik detaillierte Personenabbildungen mit Porträtaufnahmen oder auch Übersichtsaufnahmen.

Lichtstarke Kameras mit Infrarottechnik oder Restlichtaufhellung (Nachtsichtkameras ermöglichen rund um die Uhr bei allen Witterungsverhältnissen hochwertige Aufnahmen). Die automatische Aufzeichnung lässt sich über Schaltuhren in ausgewählten Zeitfenstern realisieren oder von Bewegungsmeldern auslösen.

Die Bildübertragung erfolgt über Glasfaserkabel, ISDN-Leitungen, Funk- bzw. Richtfunkstrecken, über lokale Netze oder das Internet. So können praktisch beliebige Entfernungen überbrückt und die Anzeige, Überwachung und Speicherung der Bildaufnahmen weit entfernt vom Ort des Geschehens vorgenommen werden.

Abhängig vom Ziel der Überwachungsmaßnahmen wertet das Personal mit entsprechenden Reaktionsmöglichkeiten vor Ort die Bildübertragung aus oder es wird automatisch oder anlassbezogen aufgezeichnet und nur bei Bedarf genutzt.

Bei Maßnahmen mit Live-Überwachung lassen sich meist die Bilder mehrerer Kameras gleichzeitig auf einem Monitor darstellen. Mit Hilfe von Zoomfunktionen kann zwischen Übersichts-, Nah- und Detailaufnahmen gewechselt werden. Per Knopfdruck wird das Bild ausgedruckt oder eine Videosequenz zu Beweiszwecken aufgezeichnet. Um sicherzustellen, dass auch der Zeitraum unmittelbar vor einem Ereignis, die sog. Historie, zu Beweiszwecken zur Verfügung steht, werden alle Kamerabilder über einen Zeitraum von wenigen Minuten – wie bei einer Zeitlupensequenz bei der Fernsehübertragung eines Fußballspiels – gespeichert. Sie lassen sich nachträglich vergrößern, um Detailaufnahmen von Personen oder zu Sachschäden herzustellen.

Um eine wirksame Datenschutzkontrolle von Videoaufzeichnungen zu ermöglichen, muss rechnergestützt protokolliert werden, wer wann die Aufzeichnung ausgelöst hat. Zugleich muss technisch-organisatorisch sichergestellt werden, dass digitale Aufzeichnungen nicht manipuliert werden können, denn nur unter dieser Voraussetzung sind sie vor Gericht als Beweismittel verwertbar.

1.5.2 Videoüberwachung durch öffentliche Stellen außerhalb der Polizei

Seit der ersten Novellierung des Brandenburgischen Datenschutzgesetzes (BbgDSG) 1996 haben öffentliche Stellen auch außerhalb der Polizei die Befugnis, Videoüberwachung einzusetzen.

Nach § 33c Abs. 1 BbgDSG dürfen Behörden öffentlich zugängliche Räume durch Videokameras beobachten, wenn dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung des Hausrechts erforderlich ist. Eine öffentliche Stelle, die Videokameras einsetzen will, muss daher klären, ob der zu überwachende Bereich ein öffentlich zugänglicher Raum in diesem Sinne ist.

So plante beispielsweise eine Gemeinde, eine auf dem Bahnhofsvorplatz befindliche, von ihr betriebene Infosäule durch eine Videokamera beobachten zu lassen. Die Kamera sollte so installiert werden, dass auch öffentliches Straßenland in ihr Blickfeld geraten wäre. Von einem Raum kann aber nur dann die Rede sein, wenn es sich um einen für jedermann ohne weiteres erkennbar abgegrenzten Bereich handelt, an dem ein Hausrecht besteht. Öffentlich zugängliche Räume in diesem Sinne sind beispielsweise Rathäuser, öffentliche Verkehrsmittel oder Schwimmbäder, nicht jedoch der allgemein zugängliche Straßenraum. Dessen Videoüberwachung ist nur der Polizei unter den Voraussetzungen des Brandenburgischen Polizeigesetzes erlaubt. Die Videoüberwachung durch die Gemeinde selbst war hier nicht zulässig. Die Gemeinde hat daher nach unserer datenschutzrechtlichen Bewertung von ihrem Vorhaben Abstand genommen.

Plant eine öffentliche Stelle den Einsatz von Videoüberwachung, ist darüber hinaus stets zu prüfen, ob dieser Eingriff in das Recht auf informationelle Selbstbestimmung tatsächlich erforderlich ist, um ihre Aufgaben zu erfüllen bzw. das Hausrecht zu wahren. Die Videoüberwachung ist nur dann zulässig, wenn die Aufgaben ohne dieses Mittel nicht erfüllt werden können.

Auch dürfen durch die Videoüberwachung überwiegende schutzwürdige Interessen Betroffener nicht beeinträchtigt werden. Dies setzt zunächst voraus, dass die öffentliche Stelle nachvollziehbar ermittelt, welche schutzwürdigen Interessen von welchen Betroffenen bzw. Gruppen von Betroffenen durch die Videoüberwachung überhaupt beeinträchtigt werden können. Erst dann ist die öffentliche Stelle überhaupt in der Lage, ihr Interesse an der Videoüberwachung mit den schutzwürdigen Interessen der Betroffenen abzuwägen. Das Ergebnis dieser Abwägung hängt jeweils von den konkreten Umständen des Einzelfalls ab. Dabei ist insbesondere die Zahl unbeteiligter Betroffener, aber auch die konkrete von den Kameras beobachtete Lebenssituation zu berücksichtigen.

Ist über die bloße Beobachtung mit Videokameras auch die Aufzeichnung von Bildern geplant, müssen an die Prüfung der datenschutzrechtlichen Voraussetzungen noch höhere Anforderungen gestellt werden, weil die durch die Aufzeichnung gegebene Möglichkeit der Dokumentation und Speicherung der Bilder den Eingriff in die Persönlichkeitsrechte gegenüber der bloßen Beobachtung noch vertieft. Deshalb muss die Tatsache der Aufzeichnung dem Betroffenen erkennbar gemacht werden. Das gilt aber auch schon für die bloße Videobeobachtung. Diese hat grundsätzlich offen zu erfolgen. Öffentliche Stellen, die Videoüberwachung einschließlich Aufzeichnung durchführen, müssen durch gut sichtbare Schilder oder Aufkleber deutlich auf die Tatsache der Videoüberwachung hinweisen. Es reicht nicht aus, darauf zu verweisen, dass die Kamera sichtbar angebracht ist.

Diese Anforderungen hat beispielsweise das Landesamt für Bauen, Verkehr und Straßenwesen bei einer allerdings nur einmalig vorgenommenen Videoaufzeichnung im Zusammenhang mit einem Erörterungstermin zum Planfeststellungsverfahren für den Flughafen Berlin Brandenburg International nicht beachtet. Selbst wenn die dort vorgenommene Aufzeichnung tumultartiger Szenen ggf. zur Wahrnehmung des Hausrechts erforderlich gewesen sein sollte, so wurden weder schutzwürdige Interessen der Betroffenen geprüft, noch ist auf die Aufzeichnung hingewiesen worden. Das Landesamt für Bauen, Verkehr und Straßenwesen hatte diesen Fehler selbst erkannt und die Aufzeichnungen bereits vor unserem Tätigwerden gelöscht.

Bei der Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen müssen wegen des damit verbundenen erheblichen Eingriffs in die Persönlichkeitsrechte Betroffener die rechtlichen Voraussetzungen streng geprüft werden. In jedem Falle ist zu prüfen, ob nicht ebenso geeignete Mittel vorliegen, mit denen die durch die Videoüberwachung verfolgten Ziele auch mit einem geringeren Grundrechtseingriff erreicht werden können. Es ist zu beachten, dass die allgemeine Überwachung öffentlich zugänglicher Straßen und Plätze nur im Rahmen polizeilicher Tätigkeit erfolgen darf.

1.5.3 Videoüberwachung in öffentlichen Verkehrsmitteln und im Schülerverkehr

Bereits in unserem letzten Tätigkeitsbericht[31] haben wir ausführlich über Pilotprojekte zur Videoüberwachung in Bussen, die überwiegend oder ausschließlich zur Schülerbeförderung eingesetzt werden, berichtet. In Zusammenarbeit mit dem Ministerium für Bildung, Jugend und Sport, dem Landkreistag Brandenburg sowie Vertretern des Landkreises Ober-

[31] s. Tätigkeitsbericht 2000, A 6.3.1

havel und der Oberhavel Verkehrsgesellschaft haben wir inzwischen die datenschutzrechtlichen Anforderungen an eine zulässige Videoüberwachung im Schülerverkehr präzisieren können.

Beim Einsatz von Videoüberwachung in Bussen zur Schülerbeförderung ist es zunächst erforderlich, dass bereits vor dem Einsatz der mit der Videoüberwachung verfolgte Zweck klar umrissen werden muss. Darüber hinaus muss genau überlegt werden, ob und wenn ja wie aufgezeichnete Daten weiter genutzt werden dürfen, was wiederum entscheidend vom Zweck der Videoüberwachung abhängt. Dies gilt unabhängig davon, in welcher Rechtsform der Verkehrsbetrieb organisiert ist, da die Voraussetzungen für beide ähnlich sind. Nach Klärung der rechtlichen Zulässigkeit sind die technischen und organisatorischen Maßnahmen detailliert festzulegen, um ein Höchstmaß an Datensicherheit und eine möglichst datensparsame Gestaltung der Videoüberwachung zu ermöglichen.

Die in den Pilotprojekten verwendete sog. Blackboxlösung halten wir aus datenschutzrechtlicher Sicht für akzeptabel. Dabei handelt es sich um ein digitales Bildaufzeichnungssystem, dessen Bildmaterial mit einer speziellen Software am Bildschirm sichtbar gemacht und ausgewertet wird. Aus datenschutzrechtlicher Sicht ist allerdings wichtig, dass die Dauer der Aufzeichnung möglichst kurz ist. Nach den praktischen Erfahrungen im Landkreis Oberhavel halten wir eine Aufzeichnungsdauer von max. 72 Stunden nach Entstehen der Aufnahme für vertretbar.

Das Verkehrsunternehmen muss eine Reihe von technischen und organisatorischen Maßnahmen treffen. So sind diejenigen Beschäftigten, die Zugang zu den Aufzeichnungen haben, ausdrücklich zu benennen. Es ist festzulegen, welche dieser Personen die Aufzeichnungen an welche Stelle (Polizei, Staatsanwaltschaft, Gerichte, aber auch Schulen) weitergeben darf. Die Videoüberwachung muss offen erfolgen, d. h. jedes Fahrzeug ist mit entsprechenden Hinweisschildern oder Piktogrammen deutlich sichtbar zu kennzeichnen. Die verantwortliche Stelle muss einschließlich ihrer Anschrift erkennbar sein. Die Einzelheiten sind in einer Dienstanweisung des Verkehrsbetriebes zu regeln. Der Landkreistag Brandenburg hat zugesagt, hierzu für die Landkreise entsprechende Muster zu entwerfen. Soweit Beschäftigte des Verkehrsunternehmens von der Videoüberwachung betroffen sind (z. B. Busfahrer), muss eine Betriebs-/Dienstvereinbarung abgeschlossen werden.

Eine Besonderheit der Videoüberwachung im Schülerverkehr ist die mögliche Auswertung von Videoaufzeichnungen durch die Schulen. Hierzu plant das Ministerium für Bildung, Jugend und Sport ein Rundschreiben zu entwerfen, in welchem detailliert festgelegt ist, in welchen Fällen und zu welchen Zwecken Schulen Videoaufzeichnungen nutzen dürfen. Ein erster uns vorliegen-

der Entwurf eines solchen Rundschreibens stellte aus unserer Sicht bereits eine geeignete Grundlage für einen landesweit einheitlichen datenschutzgerechten Umgang mit Videoaufzeichnungen durch die Schulen dar.

Besonders ist hervorzuheben, dass Videoaufzeichnungen danach von den Schulen nur dann angefordert werden können, wenn es um ein nicht nur unerhebliches Fehlverhalten geht, bei dem wegen des unmittelbaren schulischen Bezugs Ordnungsmaßnahmen in Betracht kommen können. Ein solcher unmittelbarer schulischer Bezug liegt nur dann vor, wenn Handlungen von Schülerinnen und Schülern die Verkehrssicherheit gefährden. Verstöße gegen die personenbeförderungsrechtlichen Bestimmungen des Verkehrsunternehmens (z.B. „Schwarzfahren“) haben hingegen keinen unmittelbaren schulischen Bezug. Entsprechende Aufzeichnungen dürfen den Schulen deshalb nicht mitgeteilt werden. Des Weiteren sollen in den Rundschreiben einheitliche Regeln für die Aufbewahrung der Aufzeichnungen, für die Auswertung und Rückgabe und für den Umgang mit unaufgefordert zugesandten Videoaufzeichnungen geschaffen werden.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln ist zulässig. Sollen Videoaufzeichnungen durch die Schulen ausgewertet werden, ist dies nur bei erheblichem Fehlverhalten von Schülerinnen und Schülern erlaubt, das einen unmittelbaren schulischen Bezug aufweist.

1.5.4 Videoüberwachung öffentlich zugänglicher Straßen und Plätze durch die Polizei

Nachdem Ende des Jahres 2000 mit der Änderung des Brandenburgischen Polizeigesetzes in § 31 eine Rechtsgrundlage für die Videoüberwachung öffentlich zugänglicher Straßen und Plätze geschaffen worden war[32], gingen auf Anweisung des Innenministeriums die Polizeipräsidien auf die Suche nach videoüberwachungstauglichen Orten. Die Suche zog sich bis November 2001 hin, ehe schließlich Videokameras zur Überwachung eines großen öffentlichen Parkplatzes am Bahnhof Erkner installiert wurden und die erste Videoüberwachungsanlage in Brandenburg ihren Betrieb aufnahm. Nach einer 2-monatigen Anlaufphase haben wir begonnen, das zunächst auf sechs Monate befristete Pilotprojekt „Videoüberwachung Erkner“ zu überprüfen.

Voraussetzung für die offene Videoüberwachung einer Örtlichkeit sind gem. § 31 Abs. 3 Brandenburgisches Polizeigesetz (BbgPolG) Lageerkenntnisse über das dortige Kriminalitätsaufkommen, die erwarten lassen, dass auch in Zukunft dort Straftaten begangen werden. Die Videoüberwachung, die durch

[32] s. Tätigkeitsbericht 2000, A 4.1.1

Hinweisschilder bekannt zu machen ist, muss eine geeignete Maßnahme zur Verhinderung solcher Straftaten sein. Weiterhin hat die Polizei Kräfte bereitzuhalten, die sofort eingreifen können, wenn Personen dennoch Straftaten begehen. Die Vorschrift befugt grundsätzlich nur zur Beobachtung des Ortes. Bildaufzeichnungen dürfen erst gefertigt werden, wenn aufgrund des Verhaltens einer Person anzunehmen ist, dass sie eine Straftat begehen will. Aufbewahrt werden Bildaufzeichnungen und personenbezogene Daten nur, wenn ein Strafverfahren eingeleitet wird. Anderenfalls sind sie spätestens einen Monat nach der Aufzeichnung zu vernichten. Die Einhaltung dieser gesetzlichen Vorgaben ist bei der zuständigen Polizeidienststelle durch technische und organisatorische Verfahrensabläufe sicherzustellen.

Zunächst hat das Polizeipräsidium Frankfurt (Oder) in einer Konzeption sowohl die örtlichen Gegebenheiten als auch das Kriminalitätsaufkommen im Verlauf der vergangenen zwei Jahre bezogen auf Erkner sowie den zur Videoüberwachung vorgesehenen öffentlichen Parkplatz am Bahnhof und den Personalbedarf analysiert. Aus dem Lagebild ergibt sich, dass über den Zeitraum der vergangenen 18 Monate die Anzahl der Straftaten, die dort tagsüber zur Hauptbenutzungszeit des Parkplatzes begangen wurden, insgesamt zwar rückläufig, aber dennoch relativ hoch ist. Das gilt insbesondere für Fahrraddiebstähle sowie Diebstähle und Sachbeschädigungen an und aus den abgestellten Fahrzeugen. Da der Parkplatz vor allem von Pendlern aus dem Umland genutzt wird, die dort ihr Fahrzeug abstellen und mit dem Zug weiterfahren, ist der Zeitabstand zwischen Tatbegehung und Schadensfeststellung sowie Anzeige durch den Geschädigten fast immer so lang, dass Zeugen nicht mehr zu ermitteln sind und die Straftat nicht aufgeklärt werden kann. Aufgrund des Lagebilds und der örtlichen Gegebenheiten hielt das Polizeipräsidium Frankfurt (Oder) die offene Videoüberwachung des Parkplatzes für gerechtfertigt.

Die Besichtigung des Parkplatzes am Bahnhof ergab, dass dort zwei Kameras auf elektronisch steuerbaren Schwenk-/Neigeköpfen montiert sind, die mit einigen Ausnahmen den gesamten Parkplatz, insbesondere den überdachten Fahrradabstellplatz, erfassen können. Zwei große, relativ hoch oben angebrachte Schilder weisen in deutscher, englischer und polnischer Sprache auf die Videoüberwachung hin. Das ist bei drei Zufahrten und einer Treppe nicht ausreichend. Hinweisschilder sollten an allen Ein- und Ausgängen zu dem Parkplatz aufgestellt werden.

Die eigentliche Videoüberwachung findet an einem dazu in der Leitstelle der Polizeiwache Erkner eingerichteten Arbeitsplatz statt. Einer der beiden Diensthabenden verfolgt am Bildschirm die von den beiden Kameras übertragenen ständig wechselnden Übersichts- und Einzelaufnahmen.

In einer Dienstanweisung sind die Verfahrensabläufe und die zur Tätigkeit am Videoüberwachungsplatz autorisierten und zur Videoaufzeichnung berechtigten Mitarbeiter sowie ihre Vertreter aufgeführt. Die Kontrolle des Videoüberwachungsplatzes sowie die Speicherung der Videoaufzeichnungen, das Ausdrucken von Fahndungsbildern und das Löschen der Aufzeichnungen ist anderen Mitarbeitern zusätzlich zu den organisatorischen Funktionen vorbehalten, sodass Aufzeichnungen außerhalb der gesetzlichen Vorschriften durch die personelle Organisation verhindert werden. Insgesamt sind 29 Mitarbeiter der Polizeiwache für diesen Arbeitsplatz geschult.

Neben der personellen Organisation soll auch das sog. Vieraugenprinzip sicherstellen, dass keine unbefugten Bildaufzeichnungen vorgenommen werden können. Das Vieraugenprinzip gilt für den gesamten Aufzeichnungsvorgang einschließlich Speicherung der Aufzeichnung auf CD-ROM und Bildausdruck bzw. Löschung. Erst wenn sich zusätzlich zu dem Diensthabenden auch der Wachdienstführer am Videoüberwachungsarbeitsplatz eingeloggt hat, kann die Aufnahmefunktion gestartet werden. Dabei wird immer auch eine zurückliegende Zeitspanne von drei Minuten – und damit die sog. Historie[33] – erfasst. Ein gleichzeitig alarmiertes Einsatzfahrzeug, das im Stadtgebiet Erkner verfügbar ist, soll durch schnelles Eingreifen die Straftat entweder verhindern oder aber die Täter feststellen.

Über jede Videoaufzeichnung muss ein schriftliches Protokoll gefertigt werden, das Auskunft gibt über Aufnahmezeit, Grund, Feststellung des Sachverhalts, das Ergebnis der Prüfung, ob es sich um eine Straftat gehandelt hat, den Verbleib der Daten und die verantwortlichen Personen. Zusätzlich wird jede Aufzeichnungsphase rechnergestützt protokolliert. Wenn sich bei dem aufgezeichneten Ereignis der Verdacht einer Straftat bestätigt, wird die Bildsequenz auf CD-ROM gebrannt. Anderenfalls wird sie gelöscht. Die Auswertung der CD-ROM erfolgt nicht in der Polizeiwache selbst, sondern im Landeskriminalamt mit einer speziellen Software. Auf diese Weise soll sichergestellt werden, dass die Bildaufzeichnungen gegen Manipulationen gesichert als Beweismaterial in Strafverfahren vorgelegt werden können. Bei der ersten Prüfung wurde uns allerdings mitgeteilt, dass der Auswertungsplatz dort noch nicht eingerichtet worden ist, so dass die bis dahin bereits erstellten CD-ROMs noch in der Polizeiwache in verschlossenen Umschlägen aufbewahrt werden. Die Protokolle werden bei der Führungsstelle verschlossen abgelegt und spätestens nach einem Jahr vernichtet.

Soweit bei der Aufzeichnung auch Daten von Unbeteiligten angefallen sind, werden sie bei der Auswertung im Landeskriminalamt gelöscht. Bei der Besichtigung konnten wir uns überzeugen, dass die in der Dienstanweisung festgelegten Verfahrensregeln eingehalten wurden.

[33] s. oben A 1.3.4

Die Polizeiwache Erkner betreibt im Rahmen ihres Pilotbetriebs eine rege Öffentlichkeitsarbeit. Der Leiter der Polizeiwache hat versichert, dass der Betrieb der Videoüberwachung in der Leitstelle zu den üblichen Dienstzeiten besichtigt werden kann, wenn nicht gerade ein besonderes Ereignis stattfindet, das zur Aufzeichnung führt.

Zuverlässige Aussagen darüber, welchen Einfluss die Videoüberwachung auf die Kriminalitätsentwicklung am Bahnhof Erkner hat, lassen sich bisher in keiner Richtung machen, da die Kriminalitätszahlen nach Angaben der Polizei bedingt durch die Jahreszeit bisher ohnehin niedrig waren.

Die technisch-organisatorische Prüfung der Überwachungsanlage in Erkner ist noch nicht abgeschlossen. Kurz vor Ende des Berichtszeitraumes wurden außerdem polizeiliche Videoüberwachungsanlagen am Potsdamer Hauptbahnhof und in Rathenow in Betrieb genommen. Der Landesbeauftragte wird sie zu gegebener Zeit ebenfalls überprüfen.

Mit der vom Landtag vorgesehenen Evaluation der Videoüberwachungsmaßnahmen hat das Ministerium der Justiz die Fachhochschule der Polizei beauftragt.

Eine flächendeckende Einführung von Videoüberwachungsanlagen (z. B. auf allen Großparkplätzen) wäre vom Brandenburgischen Polizeigesetz nicht gedeckt; sie würde der Intention des Gesetzgebers eindeutig zuwiderlaufen.

Ungeachtet der Tatsache, dass die Videoüberwachung öffentlicher Straßen und Plätze eine bedenkliche Einschränkung des Rechts auf Unbeobachtetsein ist, haben wir bei der Besichtigung des Pilotprojekts Erkner festgestellt, dass diesem Recht durch technische und organisatorische Vorkehrungen im Rahmen des bei einer Videoüberwachung Möglichen weitestgehend Rechnung getragen wird. Eine flächendeckende Videoüberwachung z. B. aller Großparkplätze wäre nach dem Brandenburgischen Polizeigesetz nicht zulässig.

1.6 Elektronische Verwaltung (E-Government)

1.6.1 Neue Herausforderungen für den Datenschutz

Der Einsatz von Informations- und Kommunikationstechnologien in der öffentlichen Verwaltung diente bisher vor allem dazu, interne Verwaltungsabläufe zu rationalisieren. Nach dem Vorbild des elektronischen Geschäftsverkehrs (E-Government) gehen die öffentlichen Stellen sowohl auf Landes- als auch auf kommunaler Ebene zunehmend dazu

über, diese Technologien bei den Kontakten zwischen der Verwaltung einerseits und den Bürgern sowie der Wirtschaft andererseits zu nutzen. Die Verwaltung verfolgt das Ziel, durch Nutzung elektronischer Medien Verwaltungsabläufe weiter zu beschleunigen und zu vereinfachen, sie transparenter, bürgerfreundlich und besser erreichbar zu organisieren.

Die Nutzung elektronischer Medien beim Kontakt zwischen Bürger und Verwaltung ist nicht zuletzt auch eine Herausforderung für den Datenschutz sowohl in rechtlicher als auch in technischer und organisatorischer Hinsicht. Der Landesbeauftragte begleitet diesen Prozess auf unterschiedlichen Ebenen, um bei der schrittweisen Einführung der elektronischen Verwaltung darauf hinzuwirken, dass die Grundrechte auf Informationszugang und Datenschutz optimal gewährleistet werden. Hierzu arbeitet der Landesbeauftragte an einer vom Landesbeauftragten für den Datenschutz Niedersachsen geleiteten Arbeitsgruppe der Datenschutzkonferenz mit, die sich mit Fragen des Datenschutzes in der elektronischen Verwaltung beschäftigt. Ziel dieser Arbeitsgruppe ist es, eine Handlungsanleitung für die öffentliche Verwaltung zu entwerfen, die datenschutzrechtliche Anforderungen an die Projekte der elektronischen Verwaltung formuliert. Unabdingbare Voraussetzung für die Akzeptanz aber auch die Zulässigkeit von E-Government-Lösungen ist dabei, dass das bisherige Datenschutzniveau keinesfalls unterschritten werden darf. Wünschenswert ist im Gegenteil, Projekte der elektronischen Verwaltung dazu zu nutzen, den Einsatz datenschutzfreundlicher Technologien zu fördern und den Grundsatz von Datenvermeidung und Datensparsamkeit stärker zu berücksichtigen. Auch ist gerade in Brandenburg das Grundrecht auf Informationszugang bei der elektronischen Verwaltung sicherzustellen und dessen Durchsetzung durch Eröffnung neuer Zugangsmöglichkeiten zur Verwaltung zu erleichtern.

Darüber hinaus müssen Fragen bei der Sicherung der Zweckbindung, der Speicherung und Archivierung elektronischer Dokumente, der Einwilligung bzw. Zustimmung zur Nutzung des elektronischen Weges und zur Verarbeitung personenbezogener Daten auf diesem Weg, bei der Durchsetzung von Auskunfts- und Einsichtsrechten, bei der Berichtigung, Löschung und Sperrung von personenbezogenen Daten und nicht zuletzt bei der Gewährleistung der Datensicherheit gelöst werden.

Inzwischen existiert der Entwurf eines Konzeptes der Landesregierung für eine E-Government-Strategie. Bereits aus diesem Entwurf lässt sich entnehmen, dass die Landesregierung E-Government als Leitbild der Verwaltungsmodernisierung betrachtet. Gerade für ein Flächenland wie Brandenburg seien durch das Internet vielfältige Möglichkeiten gegeben, Personen und Behörden zeit- und ortsunabhängig zu erreichen. Nach den Vorstellungen der Landesregierung soll es bestimmte Leitprojekte zum E-Government geben.

Sie beabsichtigt, ein Kooperationsnetz aufzubauen, um die Umsetzung der E-Government-Strategie zu koordinieren.

Im weiteren Sinne zum E-Government ist auch das Projekt „Elektronischer Rechtsverkehr„ (ELREV) zu zählen, mit dem der Einsatz elektronischer Kommunikation bei Gerichten und Staatsanwaltschaften vorbereitet werden soll. Mit dem Ministerium der Justiz und für Europaangelegenheiten haben erste Gespräche über ein entsprechendes Pilotprojekt beim Finanzgericht Cottbus stattgefunden.

Mit der schrittweisen Einführung der elektronischen Verwaltung im Land Brandenburg ergeben sich zahlreiche neue datenschutzrechtliche Fragestellungen. Im Rahmen des E-Government ist dem effektiven Schutz der Persönlichkeitsrechte sowie dem Grundrecht auf Informationszugang ein hoher Wert beizumessen.

1.6.2 Melderegister online – die elektronische Melderegisterauskunft

Im Rahmen des von der Landesregierung und der Deutschen Telekom AG durchgeführten Wettbewerbs „Telekooperation für Brandenburg“ hat die Stadt Rathenow die Projektidee einer elektronischen Melderegisterauskunft entwickelt.

Ziel der Einführung der elektronischen Melderegisterauskunft ist es, Auskünfte vollständig über das Internet abzuwickeln. In einem ersten Schritt sollen die Polizei, das Finanzamt sowie ein Strom- und ein Gasversorgungsunternehmen Zugriff auf das Melderegister über das Internet haben. Es ist geplant, bestimmte Daten aus dem Melderegister auf einen außerhalb des Behördennetzes der Stadt befindlichen Server zu spiegeln und dieses sog. Informationsregister zyklisch zu aktualisieren. Der Zugriff soll nur mittels digitaler Signatur erfolgen.

Aus datenschutz- und melderechtlicher Sicht handelt es sich bei dem Vorhaben der Stadt Rathenow um einen automatisierten Abruf von Meldedaten. Dieser ist nach dem Brandenburgischen Meldegesetz in Verbindung mit der Meldedatenübermittlungsverordnung nur für ganz bestimmte Nutzer vorgesehen. Unter den vier Pilotpartnern der Stadt Rathenow gehört lediglich die Polizei zu den befugten Nutzern. Sowohl für das Finanzamt als auch für Strom- und Gasversorgungsunternehmen ist ein automatisierter Abruf von Meldedaten im Brandenburgischen Meldegesetz bisher nicht vorgesehen.

Mit der Umsetzung der geplanten Neufassung des Melderechtsrahmengesetzes des Bundes, die eine Anpassung des Brandenburgischen Melderechts nach sich ziehen wird, werden allerdings auch die übrigen drei Pilotpartner in

zulässiger Weise Meldedaten automatisiert über das Internet abrufen dürfen[34]. Melderegisterauskünfte könnten u. a. im Wege des automatisierten Abrufs über das Internet erteilt werden, wenn der Antrag in der vorgeschriebenen Form gestellt worden ist, der Antragsteller den Betroffenen mit bestimmten im Gesetz genannten Suchkriterien bezeichnet hat und die Identität des Betroffenen eindeutig festgestellt worden ist. Durch Nutzung der digitalen Signatur wird eindeutig die Identität des Abfragenden sichergestellt. Auch ist zu regeln, dass die Einwohnerinnen und Einwohner die Möglichkeit haben, dieser Form der Auskunftserteilung zu widersprechen. Dies müsste in der Stadt Rathenow ebenfalls veranlasst werden.

Eine elektronische Melderegisterauskunft ist nach dem Brandenburgischen Melderecht derzeit noch nicht zulässig. Im Rahmen des künftigen Melderechts müssen die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden und die Einwohnerinnen und Einwohner die Möglichkeit haben, dieser Form der Melderegisterauskunft zu widersprechen.

1.6.3 Autozulassung im Bürgerbüro – Projekt e-LoGo

Die Universität Potsdam führt derzeit das Projekt e-LoGo (electronic Local Government) durch, mit dem die elektronische Verwaltung auch in kleineren Ämtern und Gemeinden Einzug halten soll. Die Besonderheit an diesem Projekt besteht darin, dass die Universität hier das Konzept einer integrierten Verwaltung verfolgt. Der Bürger soll dabei kommunale Dienstleistungen möglichst dezentral in seinem Amt oder seiner amtsfreien Gemeinde aus einer Hand in Anspruch nehmen können, unabhängig davon, ob es sich um Dienstleistungen der Kreisverwaltung oder der Gemeindeverwaltung handelt. In Zusammenarbeit mit dem Straßenverkehrsamt des Landkreises Potsdam-Mittelmark soll dieses Konzept im Rahmen der Zulassung von Kraftfahrzeugen umgesetzt werden.

Die Zulassung von Kraftfahrzeugen ist die Aufgabe der Landkreise und kreisfreien Städte. Der Landkreis Potsdam-Mittelmark sowie die Universität Potsdam planen nunmehr, dass die Bürgerinnen und Bürger diese Dienstleistung der Kreisverwaltung auch im Bürgerbüro ihres Amtes oder ihrer amtsfreien Gemeinde in Anspruch nehmen können. Die Bürgerinnen und Bürger sollen es im sog. front-office-Bereich nur mit einem Ansprechpartner zu tun haben, während im sog. back-office-Bereich die bisherige Trennung von Kreis- und Gemeindeverwaltung beibehalten werden soll.

Geplant ist, dass die Bearbeiter im örtlichen Bürgerbüro sämtliche Amtshandlungen im Zusammenhang mit einer Kfz-Zulassung vornehmen können. Im

[34] s. A 4.3

Straßenverkehrsamt der Kreisverwaltung sollen lediglich Nacharbeiten erfolgen. Außerdem verbleibt der gesamte Aktenbestand sowie der elektronische Datenbestand auf dem Server der zentralen Zulassungsstelle in der Kreisverwaltung gespeichert. Für die Kommunen wird jeweils ein Zugang zum Server der Zulassungsstelle eingerichtet.

Datenschutzrechtlich ist problematisch, dass mit den Ämtern und amtsfreien Gemeinden nunmehr solche Stellen Zugriff auf personenbezogene Daten der Zulassungsstelle bekommen sollen, die bisher solche Daten zu ihrer Aufgabenerfüllung nicht benötigten. Dies ist nach der derzeitigen Rechtslage und Kompetenzverteilung nicht zulässig. Aus straßenverkehrsrechtlicher Sicht ist es daher erforderlich, die Verordnung zur Regelung der Zuständigkeiten insofern zu verändern, dass den Landkreisen die Befugnis eingeräumt wird, den Kommunen die Ausführung bestimmter Amtshandlungen im Zulassungsverfahren zu übertragen. Außerdem ist zu berücksichtigen, dass es sich bei dem geplanten Zugriff der Kommunen auf die Daten der Zulassungsstelle um ein automatisiertes Abrufverfahren i. S. v. § 9 des Brandenburgischen Datenschutzgesetzes handelt. Auch hierfür fehlt derzeit noch die erforderliche Rechtsgrundlage.

Schließlich wird es erforderlich sein, die nach dem Stand der Technik erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen. Diese sind derzeit noch offen und werden mit dem Landkreis Potsdam-Mittelmark sowie der Universität Potsdam diskutiert.

Die Universität Potsdam sowie der Landkreis Potsdam-Mittelmark prüfen zudem, inwieweit auch eine Zulassung von Kraftfahrzeugen durch Autohändler oder direkt durch die Bürgerinnen und Bürger über das Internet möglich ist. Hierfür sind neben datenschutzrechtlichen allerdings noch eine Reihe von straßenverkehrsrechtlichen Fragen offen.

Mit der Schaffung entsprechender Rechtsgrundlagen bestehen gegen die Einführung einer integrierten Kommunalverwaltung keine grundsätzlichen datenschutzrechtlichen Bedenken. Der Landesbeauftragte wird die Umsetzung dieser Vorhaben kritisch begleiten.

1.7 Genomanalysen am Menschen – nach welchen Regeln?

Die Fortschritte bei der Entschlüsselung des menschlichen Genoms bringen einerseits zusätzliche Diagnosemöglichkeiten und die Hoffnung auf die Therapie schwerer, bisher kaum heilbarer Krankheiten mit sich. Auf der anderen Seite müssen angesichts der sehr sensiblen Daten effektive Vorkehrungen zum Schutz des Rechtes auf informationelle Selbstbestimmung getroffen werden. Diese Problematik beschränkt sich

nicht nur auf den Umgang mit entsprechenden Proben und Daten bei Medizinern oder Forschern, sondern reicht bis zur Frage der Verwertung dieser Daten durch Versicherungen und Arbeitgeber.

Aufgrund der rasanten wissenschaftlichen Fortschritte bei der Entschlüsselung des menschlichen Genoms sah es die 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2000 als wichtig an, ihre erste Entschließung zur Genomanalyse und informationellen Selbstbestimmung aus dem Jahre 1989 zu bekräftigen. Wenig später trat die Enquetekommission des Bundestages „Recht und Ethik der modernen Medizin" an alle Datenschutzbeauftragten des Bundes und der Länder mit einem Fragenkatalog heran. Etwa in derselben Zeit bat das Ministerium für Arbeit, Soziales, Gesundheit und Frauen uns um Unterstützung bei der Erarbeitung von Eckpunkten zum Themenbereich „prädiktive genetische Testverfahren". Diese Bitte haben wir gerne erfüllt. Ebenso konnten wir unsere Überlegungen in das gemeinsame Antwortschreiben der Datenschutzbeauftragten an die Enquetekommission einbringen.

Die Arbeitsgemeinschaft „Genomanalyse" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitete im Berichtszeitraum einen Entwurf zur gesetzlichen Regelung genetischer Untersuchungen, den die Datenschutzkonferenz im Oktober 2001 zustimmend zur Kenntnis nahm[35].

Genetische Untersuchungen und die damit im Zusammenhang stehenden Datenverarbeitungen bedürfen danach grundsätzlich einer schriftlichen Einwilligungserklärung durch den Patienten. Bei dieser ist besonderer Wert auf eine Aufklärung der Betroffenen vorab zu legen. Bei Minderjährigen und nicht einsichtsfähigen Erwachsenen sollen bei genetischen Untersuchungen enge Grenzen gezogen werden. Auch das Recht auf Widerruf einer Einwilligungserklärung und die Folgen eines solchen Widerrufs galt es zu bedenken. Die Betroffenen sollen außerdem unentgeltlich Einsicht in und Auskunft über die Dokumentationen zu genetischen Untersuchungen erhalten.

Die Durchführung genetischer Untersuchungen ist nur solchen Personen oder Stellen zu überlassen, die dafür eine allgemeine Zulassung erhalten. Grundsätzlich sollen die Datenverarbeitungen und der Umgang mit den Proben streng zweckgebunden sein. Spezielle Regelungen trifft der Entwurf für pränatale Untersuchungen, Reihenuntersuchungen sowie prädiktive genetische Untersuchungen.

Bei der Unterrichtung über das Untersuchungsergebnis ist auch das Recht des Betroffenen auf Nichtwissen zu berücksichtigen. Es hat Auswirkungen auf die Rechte von Verwandten, für die die Information über bestimmte Erb-

[35] Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.3

anlagen ebenso relevant sein kann, wie für den Untersuchten. Ihr Recht auf Wissen bzw. Nichtwissen kann im Widerspruch zum Geheimhaltungs- oder Offenbarungswillen des Betroffenen stehen und ist mit seinen Interessen abzuwägen.

Betriebsärzte sollen jedoch Arbeitnehmer auf erhöhte Erkrankungs- und Unfallgefahren aufgrund bestimmter Genstrukturen hinweisen, zu geeigneten genetischen Untersuchungen beraten und zugelassene Ärzte für diese Untersuchungen benennen. Statt also durch Zwangsuntersuchungen solche erhöhten Risiken möglichst – aber doch nicht absolut sicher – auszuschließen, wird auf die Eigenverantwortung der Betroffenen und die allgemeinen Arbeitsschutzmaßnahmen gebaut.

Arbeitgebern soll es verboten sein, genetische Untersuchungen durchzuführen, zu veranlassen, sich Ergebnisse von genetischen Untersuchungen zu beschaffen oder diese auch nur entgegenzunehmen. Genetische Untersuchungen vor Abschluss eines Versicherungsvertrages sind i. d. R. ebenfalls verboten. Ein Verstoß gegen die Verbote soll in beiden Bereichen strafrechtliche Konsequenzen haben.

Im Versicherungsbereich werden ausnahmsweise Offenbarungspflichten bei der Vereinbarung besonders hoher Leistungssummen vorgesehen, wenn Anhaltspunkte dafür bestehen, dass der Versicherungsnehmer sich aufgrund des Ergebnisses einer genetischen Untersuchung zu dem Vertragsabschluss entschied, seinen Informationsvorsprung also über Gebühr zu seinem bzw. seiner Erben Vorteil nutzen will.

Für die Strafverfolgung gibt es bereits Gesetze, die DNA-Analysen unter bestimmten Voraussetzungen erlauben. Regelungsbedarf sahen wir aber auch bei genetischen Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb dieses Bereichs: Immer mehr Firmen wittern ein großes Geschäft bei Angeboten an Väter, die sich ihrer Vaterschaft nicht sicher sind. Durch einen Vergleich z. B. von Speichel- oder Haarproben des Kindes und des Mannes lässt sich dazu eine Aussage treffen. Werden jedoch das gesetzliche Vaterschaftsanfechtungsverfahren und die dabei vorgesehenen Untersuchungen zur Feststellung der Abstammung umgangen, so spricht einiges dafür, dass der Mann die Untersuchung ohne Wissen und – evtl. sogar gegen den – Willen der sorgeberechtigten Mutter und des Kindes durchführt.

Ein anderer Landesdatenschutzbeauftragter, den wir auf das Internetangebot einer Firma in seinem Zuständigkeitsbereich aufmerksam machten, hat heimliche genetische Vaterschaftstests als unzulässig beurteilt. Er hat festgestellt, dass, solange nicht die ausdrückliche Einwilligung der Sorgeberechtigten nachgewiesen ist, und auch darüber hinausgehende schutzwürdige Interes-

sen des Kindes nicht angemessen berücksichtigt sind, eine solche Datenverarbeitung gegen das Bundesdatenschutzgesetz verstößt. Die Testpraxis wurde deshalb datenschutzrechtlich beanstandet.

Unser Vorschlag im Gesetzentwurf zur Vermeidung heimlicher genetischer Abstammungstests sieht vor, dass die untersuchende Stelle selbst die Probe zu entnehmen hat. Zuvor ist eine schriftliche Einwilligungserklärung des Betroffenen und/oder des Sorgeberechtigten einzuholen, falls nicht eine gerichtliche oder behördliche Anordnung zu der Untersuchung verpflichtet. Verstöße gegen diese Voraussetzungen sollen auf Antrag strafrechtlich geahndet werden. Antragsberechtigt sind neben den Betroffenen stets die zuständigen Kontrollbehörden für den Datenschutz.

Im Forschungsbereich soll der Arbeit mit anonymisierten oder zumindest pseudonymisierten Daten der Vorrang eingeräumt werden.

Wir haben für unseren Gesetzesvorschlag eine Befristung auf zehn Jahre vorgesehen. Zwei Jahre vor diesem Termin sollen die Datenschutzbeauftragten dem Gesetzgeber einen Bericht über die Wirksamkeit der Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht vorlegen.

Welche Regelungen für die Zulässigkeit von Genomanalysen am Menschen und die damit zusammenhängenden Datenverarbeitungen getroffen werden, war der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein so wesentliches Anliegen, dass sie erstmals einen eigenen vollständigen Gesetzentwurf vorgelegt hat.

1.8 Von der Medikamentenchipkarte zur elektronischen Patientenakte

Vor dem Hintergrund des sog. Lipobay-Skandals, bei dem sich Wechselwirkungen zwischen Medikamenten als tödlich erwiesen, schlug das Bundesgesundheitsministerium vor, einen elektronischen Arzneimittelpass als Pflichtpass für alle Krankenversicherten einzuführen. Auf einer Chipkarte sollten lückenlos alle verordneten Medikamente dokumentiert werden. Inzwischen wird daran gedacht, die Chipkarte im Rahmen einer elektronischen Patientenakte zu nutzen, in der eine Gesundheitsdatensammlung über jeden Krankenversicherten entsteht. Das Ziel dürfte die Umwandlung der freiwilligen Patientenchipkarte in einen Pflichtpass sein.

Die Chipkarte bringt nur die scheinbare Sicherheit, dass alle wesentlichen Daten elektronisch erfasst sind. Sie kann keine Auskunft darüber geben, ob der Patient verordnete Medikamente überhaupt eingenommen hat, ob er rezeptfreie Arzneimittel konsumiert oder Alkohol trinkt. Fehl- und Doppelunter-

suchungen sowie gefährliche Wechselwirkungen zwischen Medikamenten lassen sich auch dann vermeiden, wenn Ärzte sowohl die Anamnese als auch die Aufklärung der Patienten über bekannte Nebenwirkungen und Wechselwirkungen von Medikamenten ernst nehmen.

Unzutreffend ist außerdem auch die vom Ministerium zur Unterstützung seiner Pläne geäußerte Auffassung, eine Medikamentenchipkarte sei besonders datenschutzfreundlich, weil sie die Speicherung der sensiblen Gesundheitsdaten in der ausschließlichen Verfügungsmacht des Patienten (auf der Chipkarte) ermögliche. Die Daten können so aber wesentlich einfacher verloren gehen als eine Dokumentation in einer Arztpraxis. Die Chipkarte könnte außerdem – im Gegensatz zur Patientenakte beim Arzt – jederzeit beschlagnahmt werden.

Ein Patient könnte zudem leicht unter Druck geraten, seine Chipkarte Stellen, wie z. B. dem Arbeitgeber, vorlegen zu sollen. Die Datenschutzbeauftragten des Bundes und der Länder haben daher stets betont, dass der Einsatz von Chipkarten freiwillig zu sein hat[36]. Es muss stets die Möglichkeit bestehen, unbeeinflusst über den Einsatz und die Verwendung der Karte zu entscheiden.

Es bleibt abzuwarten, welche konkreten Pläne das Bundesgesundheitsministerium letztlich im Rahmen einer Gesundheitsreform hat. Wir werden uns jedoch weiterhin für die Freiwilligkeit einer Patientenchipkarte oder auch einer elektronischen Patientenakte einsetzen.

2 Technisch-organisatorische Entwicklungen

2.1 Elektronische Signatur – Praktikable Lösungen in Sicht?

Die sichere und rechtsverbindliche Kommunikation mit der öffentlichen Verwaltung im Internet erfordert das flächendeckende Angebot der elektronischen Signatur. Welche rechtlichen und technischen Voraussetzungen sind dazu nötig?

Im novellierten Signaturgesetz (SigG)[37] und in der Signaturverordnung (SigV)[38] werden die Rahmenbedingungen der elektronischen Signatur festgeschrieben. Die rechtlichen Voraussetzungen sind damit weitestgehend gegeben. Soll die eigenhändige Unterschrift durch die elektronische Form er-

[36] Entschließung vom 26.10.2001, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.3
[37] vom 16.5.2001, BGBl. I S. 876
[38] vom 16.11.2001, BGBl. I S. 3074

setzt werden, so muss das Verwaltungsverfahrensrecht entsprechend angepasst werden. Die entsprechenden Vorarbeiten für eine einheitliche Rechtsänderung in Bund und Ländern sind noch nicht abgeschlossen.

Aber auch in technisch-organisatorischer Hinsicht ist ein koordiniertes Vorgehen im Land die Grundvoraussetzung für die rasche Einführung der elektronischen Signatur. Im Berichtszeitraum wurde daher im Landesbetrieb für Datenverarbeitung und Statistik (LDS) eine Arbeitsgruppe Elektronische Signaturen ins Leben gerufen, die sich mit den rechtlichen Voraussetzungen und der zu schaffenden Infrastruktur bei der Einführung von Signaturen auf Basis einheitlicher Standards beschäftigt.

Derzeit sind die Signaturanwendungskomponenten akkreditierter Zertifizierungsdienstleister noch nicht aufeinander abgestimmt. Das bedeutet, dass jede E-Government-Anwendung die Komponenten aller Zertifizierungsstellen enthalten muss, um eine freie Wahl des Zertifizierungsdienstleisters zu ermöglichen. Dieses Verfahren ist in der Praxis jedoch sehr aufwändig. Mit Hilfe des Interoperabilitätsstandards „ISIS-MTT“ (Industrial Signature Interoperability Specification/Standard MailTrusT) soll daher eine einheitliche Lösung geschaffen werden. Die Arbeitsgruppe geht davon aus, dass im Laufe des Jahres 2002 entsprechende Produkte zur Verfügung stehen werden und empfiehlt daher beim Einsatz von qualifizierten (akkreditierten) Signaturen den Standard „ISIS-MTT“ zu berücksichtigen.

Selbst dann wird sich die gegenwärtig noch nicht anwendungsreife qualifizierte Signatur angesichts der schwierigen rechtlichen und technischen Fragen erst nach einer längeren Übergangszeit durchsetzen. Entscheidend ist, dass die öffentliche Verwaltung in dem Bestreben, die elektronische Signatur möglichst bald allgemein verfügbar zu machen, keine Abstriche am Sicherheitsniveau zulassen sollte. Das Beispiel des privaten schweizerischen Zertifizierungsdiensteanbieters Swisskey, der im Berichtszeitraum in Konkurs fiel und für den Zusammenbruch der gesamten öffentlichen Schlüsselinfrastruktur in der Schweiz sorgte, macht überdies deutlich, dass der Staat die Infrastruktur-Verantwortung nicht vollständig auf Private abwälzen darf. Die öffentliche Verwaltung in Brandenburg sollte ausschließlich mit akkreditierten Zertifizierungsdiensteanbietern kooperieren, bei denen im Konkursfall die Regulierungsbehörde nach § 15 SigG die Dokumentation der Zertifikate übernehmen muss.

Der flächendeckende Einsatz der qualifizierten elektronischen Signatur ist die Voraussetzung für alle E-Government-Projekte. Der einheitliche Standard „ISIS-MTT“ soll zukünftig die Interoperabilität der Signaturkomponenten der verschiedenen Zertifizierungsdienstleister sicherstellen.

Der Staat darf sich seiner Verantwortung für eine sichere öffentliche Schlüsselinfrastruktur nicht entziehen.

2.2 Sicherheit in Funknetzen

Im LAN (Local Area Network)-Bereich der öffentlichen Verwaltung wurden in den letzten Jahren primär kabelgebundene Lösungen eingesetzt. In letzter Zeit ist in Universitäten, Kommunen und Krankenhäusern zu beobachten, dass vorhandene LANs durch kabellose Netzwerke ergänzt werden.

Der Vorteil von Funknetzen liegt auf der Hand. Die aufwändige Kabelverlegung entfällt. In denkmalgeschützten Gebäuden sind sie die einzige Möglichkeit eine Netzinfrastruktur zu errichten. Bei der Installation von Funknetzen sind jedoch eine Reihe von Sicherheitsaspekten zu berücksichtigen, um ein unbefugtes Eindringen in diese Netze zu verhindern.

Funk-LAN-Systeme nach dem WLAN (Wireless Local Area Network)-Standard IEEE (Institute of Electrical and Electronics Engineers) 802.11b sind derzeit am weitesten verbreitet. Sie arbeiten im ISM(Industrial, Science, Medical)-Band zwischen 2,4 und 2,4835 GHz. Möglich sind Übertragungsgeschwindigkeiten bis zu 11 MBit/s. In der Praxis werden Netto-Datenraten von ca. 5 MBit/s erreicht. Die zur Verfügung stehende Bandbreite wird auf die Anzahl der aktiven Nutzer aufgeteilt. Funk-LAN-Systeme nach dem Standard IEEE 802.11a arbeiten mit 5 GHz und einer Datenrate bis zu 54 MBit/s. Produkte, die dem Standard IEEE 802.11a entsprechen, sollen in Kürze verfügbar sein.

Zum Anschluss eines mobilen Rechners (z. B. Notebook, Laptop) an das Funk-Netz muss dieser mit einer WLAN-Card ausgestattet werden. Der Zugang der Funk-Clients zum drahtgebundenen LAN erfolgt über Access Points (AP).

Ein Access Point kann in verschiedenen Modi betrieben werden. Access Points können als Funk-Brücken arbeiten und damit z. B. drahtgebundene LANs miteinander verbinden. Der Infrastruktur-Modus ermöglicht den Funk-Clients den Zugang zum drahtgebundenen LAN. Werden mehrere Access Points in einem Funk-Netz verwendet, so ist auch ein Roaming zwischen den Access Point-Zellen möglich. Ein Access Point versorgt einen Radius von ungefähr 30 Metern. Durch Verwendung von Parabolantennen können Entfernungen bis zu 5 km erreicht werden. Aus Sicherheitsgründen sollten Passwörter für die Administration von Access Points vergeben werden.

Die Funknetzkennung SSID (Service Set Identifier) muss bekannt sein, um sich in einem Funknetz anzumelden. Die SSID sollte netzwerk-spezifisch festgelegt werden. Es können dann nur die Clients zugreifen, denen die SSID bekannt ist. Die Sicherheit der SSID bieten jedoch nur einen geringen Schutz, da einige WLAN-Adapter-Cards im Stande sind, die SSID aus den Access Points auszulesen.

Zur Erhöhung der Sicherheit können die im Funknetz zugelassenen MAC(Media Access Control)-Adressen der WLAN-Cards der Clients im Access Point eingetragen werden. Dadurch wird erreicht, dass nur die zugelassenen Clients einen Zugriff zum Funknetz erhalten. Bei Verlust der WLAN-Card kann jedoch unter Umständen ein unberechtigter Nutzer in das Funknetz eindringen.

Die im WLAN-Standard IEEE 802.11 enthaltene Sicherheitskomponente Wired Equivalent Privacy (WEP) für Funk-Netze hat sich in den letzten Jahren als unsicher herausgestellt. Der hierbei verwendete Verschlüsselungsalgorithmus RC4 entspricht nicht mehr den heutigen Anforderungen an sichere kryptographische Verfahren. Sollen personenbezogene Daten in einem Funk-Netz übertragen werden, so ist die Verschlüsselung des Netzverkehrs unter Verwendung von VPN(Virtual Private Network)–Techniken, z. B. IPSec (IP Security) unabdingbar. Auch sollten Funknetze von kabelgebundenen Netzen durch eine Firewall abgeschottet werden.

Einbruchsversuche in Funk-Netze können nicht festgestellt und auch schwer verhindert werden. Bei der Übertragung von personenbezogenen Daten ist deshalb die Realisierung zusätzlicher Sicherheitsmaßnahmen unabdingbar.

2.3 Externe Zugänge zum Landesverwaltungsnetz

In unserem letzten Tätigkeitsbericht forderten wir die Fachnetzbetreiber auf zu überprüfen, ob in ihren Netzen externe, ungesicherte Netzzugänge betrieben werden. Der Landesbetrieb für Datenverarbeitung und Statistik (LDS) führte dazu im September 2001 bei ca. 250 an das Fachnetz Allgemeine Verwaltung angeschlossenen Daten verarbeitenden Stellen eine Umfrage durch, um alle externen Netzzugänge zu erfassen.

Nach dem bisherigen Stand der Umfrage betreiben eine Reihe von Daten verarbeitenden Stellen externe, ungesicherte Netzzugänge. Der LDS ist stets bemüht, die zentralen Zugänge zum Landesverwaltungsnetz nach dem aktuellen Stand der Technik abzusichern. So werden u. a. externe Zugänge (Internet, TESTA-Netz, ISDN-Zugänge) durch Firewallsysteme abgeschottet. Die Sicherheit im Landesverwaltungsnetz kann aber nur gewährleistet werden, wenn alle angeschlossenen Stellen ihre externen Zugänge schützen.

Schon bei der Existenz eines einzigen ungesicherten Zugangs zum Landesverwaltungsnetz (LVN) ist die Sicherheit des gesamten Netzes in Frage gestellt. Die betroffenen Stellen sollten schnellstmöglich diese externen Zugänge vom LVN trennen. Nach Auswertung der Umfrage mit dem LDS werden wir kurzfristig Kontrollen gem. § 26 BbgDSG in den Daten verarbeitenden Stellen durchführen, die externe, ungesicherte Zugänge auch weiterhin betreiben.

Eine Umfrage des LDS ergab, dass einige an das LVN angeschlossene Daten verarbeitende Stellen externe, ungesicherte Zugänge betreiben. Die betroffenen Stellen sollten diese Zugänge schnellstmöglich vom LVN trennen und erst nach Erstellung und Umsetzung eines IT-Sicherheitskonzeptes wieder in Betrieb nehmen.

2.4 „Aktive Elemente“ – klingt ganz positiv

Ein Großteil der Mitarbeiter der Landes- und Kommunalverwaltungen können mittlerweile von ihrem Arbeitsplatz aus auf das Internet als zunehmend unverzichtbare Informationsquelle zugreifen. In einem IT-Sicherheitskonzept wurden technisch-organisatorische Maßnahmen beschrieben, die geeignet sind, das Landesverwaltungsnetz vor Angriffen aus dem Internet zu schützen. Der Landesbetrieb für Datenverarbeitung und Statistik (LDS) hat dieses Konzept konsequent umgesetzt und passt es ständig den neuen Erfordernissen an.

Selbst durch bloßes Surfen im Internet bestehen eine Reihe von Risiken, die durch Nutzung sog. aktiver Inhalte (u. a. Java, JavaScript, ActiveX) hervorgerufen werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl bereits im Jahr 1999, auf die Nutzung solcher aktiver Inhalte zu verzichten und appellierte an die Betreiber von WWW-Servern Alternativangebote bereitzustellen, die ohne aktive Inhalte dargestellt werden können.

Die Arbeitsgruppe „Aktive Elemente“ des Interministeriellen Ausschusses für Informationstechnik (IMA-IT) hat Richtlinien zu diesem Thema erarbeitet:

1. Die Nutzung aktiver Inhalte (z. B. Java, JavaScript, ActiveX) ist sowohl beim Zugriff auf das Internet als auch im Landesverwaltungsnetz mit erheblichen Sicherheitsrisiken verbunden. Bei Einsatz bzw. Nutzung von aktiven Inhalten ist im besonderen Maße zwischen Notwendigkeit und Risiken abzuwägen.

2. Innerhalb des Landesverwaltungsnetzes sind aktive Inhalte nur im unbedingt erforderlichen Maße zu verwenden.

3. Bei Nutzung des Internet sind als aktive Inhalte nur Java und JavaScript (nach Vorliegen bestimmter Sicherheitsvoraussetzungen) zulässig. Andere aktive Inhalte werden, je nach technischer Möglichkeit (z. B. ActiveX), am zentralen Internetzugang gefiltert.

4. Entsprechende dezentrale Sicherheitsmaßnahmen sind von den am Landesverwaltungsnetz angeschlossenen Behörden zu realisieren, um weitere unzulässige aktive Inhalte bei Internetnutzung zu unterbinden. Ebenfalls ist die Nutzung zulässiger aktiver Inhalte im Landesverwaltungsnetz und ggf. Internetnutzung abzusichern.

5. Empfohlene dezentrale Sicherheitsmaßnahmen können aus der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ entnommen werden. (http://www.lda.brandenburg.de/empfehl/oh_inter/oh_int.htm)

Durch die Verwendung aktiver Inhalte (z. B. Java, JavaScript, ActiveX) entstehen eine Reihe von Gefährdungen bei der Nutzung des Internet. In einer Arbeitsgruppe des IMA-IT wurden daher Richtlinien erarbeitet, die den Einsatz dieser aktiven Inhalte beschränken.

2.5 Hinweise zur Nutzung des Internet

Der Anschluss eines Arbeitsplatzcomputers (APC) an das Internet ist mit einer Vielzahl von Risiken verbunden. Die folgenden Maßnahmen können zur Minimierung des Restrisikos beitragen:

- Vertrauliche Informationen sollten nur verschlüsselt über das Internet übertragen werden (s. http://www.pgpi.com).

- Es sollten jeweils die aktuellen Versionen der Browser verwendet werden, da erkannte Fehler relativ schnell beseitigt werden.

- Die Browser sollten möglichst restriktiv konfiguriert werden (Abschalten von Java, Script-Sprachen, ActiveX usw.[39]).

- Die Warnmeldungen der Browser sollten eingeschaltet werden.

- Durch Nutzung von Anonymisierungsdiensten kann die Erstellung von Nutzerprofilen über „Surfgewohnheiten“ vermieden werden.

[39] s. dazu oben A 2.4

- Vor dem „Surfen“ im Internet sollten alle nicht benötigten Anwendungen und Dienste beendet werden, um einen eventuellen Angriff zu erschweren.

- Sensible Daten sollten nur verschlüsselt auf dem Arbeitsplatzcomputer abgelegt werden (z. B. Dateiverschlüsselung).

- Personal-Firewall- und Intrusion Detection Systeme

sollten ebenso eingesetzt werden wie Anti-Viren-Programme.

Der Internetnutzer sollte sich regelmäßig über sicherheitsrelevante Ereignisse informieren (z. B. http://www.cert.dfn.de).

Der beste Schutz ist die Verwendung eines separaten Arbeitsplatzcomputers, mit dem ausschließlich im Internet gearbeitet wird und auf dem keine personenbezogenen Daten gespeichert werden.

Durch Umsetzung von technisch-organisatorischen Maßnahmen können die Risiken, die beim Anschluss eines Arbeitsplatzcomputers an das Internet bestehen, auf ein Minimum reduziert werden. Einen absoluten Schutz wird man jedoch niemals erreichen.

3 Telekommunikation und Medien

3.1 Multi-Mediadienste

3.1.1 Datenschutz in einer neuen Medienordnung

Am 21. November 2001 ist über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG) in Kraft getreten[40]. Bestandteil dieses Gesetzes ist eine umfassende Änderung des Teledienstedatenschutzgesetzes (TDDSG). Gleichzeitig soll das Medien- und Telekommunikationsrecht in Bund und Ländern unter dem Stichwort „Neue Medienordnung“ neu geregelt und vereinfacht werden.

Ziel der Novellierung war es, unter Beibehaltung des hohen Datenschutzniveaus die Systematik des Gesetzes klarer zu gestalten und Erfahrungen, die bei der praktischen Anwendung des Gesetzes gemacht worden waren, zu berücksichtigen. Die weitgehende Angleichung an die Telekommunikations-Datenschutzverordnung[41] sollte ein möglichst einheitliches materielles Daten-

[40] BGBl. I S. 3721

[41] s. dazu Tätigkeitsbericht 2000, A 3.1

schutzrecht bei allen modernen Informations- und Kommunikationsdiensten schaffen.

Die Neufassung stellt nunmehr klar, dass das Teledienstedatenschutzgesetz nicht im Dienst- und Arbeitsverhältnis gilt, soweit die Nutzung von Telediensten ausschließlich zu beruflichen oder dienstlichen Zwecken erfolgt. Ebenso gelten die Bestimmungen nicht bei solchen Diensten, die ausschließlich Arbeits- oder Geschäftsprozesse steuern. Aufrechterhalten wurde die strenge Zweckbindung der bei der Nutzung von Telediensten erhobenen Daten. So können nach wie vor die bei der Nutzung des Internet entstehenden personenbezogen Daten weiterhin nur aufgrund einer Einwilligung für Werbe- und Marketingzwecke verarbeitet werden. Wie bisher dürfen Nutzungsprofile nur unter Verwendung von Pseudonymen erstellt werden. Der Nutzer hat zusätzlich dagegen ein Widerspruchsrecht. Auch der Grundsatz der Datenvermeidung und Datensparsamkeit wird berücksichtigt. Die Diensteanbieter sind nach wie vor verpflichtet, die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder pseudonym zu ermöglichen.

Kritisiert wurde von den Datenschutzbeauftragten, dass Abrechnungsdaten, die zur Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote verarbeitet werden, nunmehr sechs Monate nach Versendung der Rechnung gespeichert werden dürfen. Gegen die Auffassung der Sicherheitsbehörden konnten wir uns hier ebenso wenig wie im Telekommunikationsbereich mit der Forderung verkürzter Speicherfristen durchsetzen.

Um wie bisher ein einheitliches Datenschutzniveau bei der Nutzung von Multimediadiensten herzustellen, muss der für einen Teilbereich geltende Mediendienste-Staatsvertrag so schnell wie möglich dem neuen Teledienstedatenschutzgesetz angepasst werden. Dies soll in Kürze geschehen.

Bund und Länder streben darüber hinaus eine umfassendere Neugestaltung des Multimediarechts unter dem Stichwort einer neuen Medienordnung an. Die uns bisher bekannt gewordenen Vorschläge beschränken sich allerdings darauf, den Ländern umfangreichere Befugnisse beim Jugendschutz im Multimediabereich (vor allem im Internet) zu übertragen. Auf der anderen Seite ist eine Reihe von Ländern bereit, Kompetenzen im Online-Datenschutz an den Bund abzugeben.

Die neue Medienordnung darf sich nicht auf eine Neuverteilung von Kompetenzen beschränken. Die Zersplitterung des Online-Datenschutzes führt zu einer Vielzahl von Abgrenzungsproblemen, die durch die technische Entwicklung und die Konvergenz der Medien weiter zunehmen werden. So wird das Internet inzwischen für klassische Telekommunikationsdienste oder das Fernsehkabel für den Internetzugang genutzt. In Folge dessen lässt sich eine

Reihe von Angeboten nur noch unter großen Schwierigkeiten als Telekommunikations-, Tele-, Medien- oder Rundfunkdienst einordnen. Wir halten es deshalb für erforderlich, zu einem einheitlichen Datenschutzrecht für alle Dienste der elektronischen Kommunikation zu kommen. Dieser Ansatz wird auf europäischer Ebene durch den neuesten Richtlinien-Entwurf der Europäischen Union zum Schutz der Privatsphäre in der elektronischen Kommunikation bereits verfolgt.

Die Datenschutzbeauftragten von Bund und Ländern regen darüber hinaus an, das Fernmeldegeheimnis in Art. 10 des Grundgesetzes zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiterzuentwickeln.

Hierzu hat die 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung zur neuen Medienordnung verabschiedet[42].

Die Neufassung des Teledienstedatenschutzgesetzes behält das bisherige hohe Datenschutzniveau bei der Nutzung von Telediensten weitgehend bei. Die Landesregierung sollte sich für ein einheitliches Datenschutzrecht auf hohem Niveau für die gesamte elektronische Kommunikation einsetzen. Das derzeit bestehende Fernmeldegeheimnis sollte zu einem Mediennutzungs- und Kommunikationsgeheimnis entwickelt werden.

3.1.2 Chef surft mit – dienstliche und private Nutzung von E-Mail und Internet am Arbeitsplatz

Immer mehr Behörden gewähren ihren Mitarbeiterinnen und Mitarbeitern Zugang zu E-Mail und Internet am Arbeitsplatz. Die Nutzung elektronischer Medien vom Arbeitsplatz aus wirft sowohl bei der ausschließlich dienstlichen, aber auch bei der ggf. erlaubten privaten Nutzung eine Reihe neuer datenschutzrechtlicher Fragen auf.

Um den zulässigen Umfang von Protokollierung und Inhaltskontrolle bei der Nutzung von Internet und E-Mail festzustellen, kommt es darauf an, ob die Behörde ihren Bediensteten nur die dienstliche Nutzung dieser Dienste oder auch deren private Nutzung erlaubt. Die überwiegende Zahl der obersten Landesbehörden in Brandenburg hat die private Nutzung von E-Mail und Internet verboten. Viele Ministerien haben dabei das Muster für eine Dienstvereinbarung zur Nutzung des Internet aus dem Handbuch für Informationstechnik des Ministeriums des Innern als Grundlage genommen.

Hat die öffentliche Stelle die private Nutzung untersagt, so hat der Dienstherr bzw. Arbeitgeber das Recht zu prüfen, ob die Nutzung durch die Beschäftig-

[42] s. Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.3

ten wirklich nur dienstlich motiviert ist. Allerdings ist eine automatisierte Vollkontrolle nicht erlaubt. Diese ist vielmehr nur bei begründeten Anlässen ausnahmsweise nach einem in einer Dienstvereinbarung festzulegenden Verfahren zulässig, das den Beschäftigten auch bekannt ist. Unbeschränkt möglich (und empfehlenswert) sind hingegen automatisierte Virenchecks.

Da dienstliche E-Mails grundsätzlich mit normalem dienstlichen Postverkehr gleichzusetzen sind, kann ein Vorgesetzter verfügen, dass ihm jede E-Mail seiner Mitarbeiter vorgelegt wird.

Inwieweit Zugriffe auf das Internet protokolliert werden, richtet sich in erster Linie nach § 29 des Brandenburgischen Datenschutzgesetzes (BbgDSG). Es ist dringend anzuraten, Art und Umfang der Protokollierung in einer Dienstvereinbarung festzulegen. Um von vornherein das private Surfen im Internet einzuschränken, bieten sich Nutzungssperren von Diensten oder Webseiten (z. B. Positiv- bzw. Negativlisten oder Filter) an.

Erlaubt eine Behörde ihren Mitarbeiterinnen und Mitarbeitern unbeschränkt die private Nutzung von Internet oder E-Mail, so hat dies weit reichende Folgen. Die öffentliche Stelle muss sich dabei darüber im Klaren sein, dass sie dadurch zu einem Diensteanbieter im Sinne des Multimedia- bzw. Telekommunikationsrechts wird. Der Dienstherr bzw. Arbeitgeber ist gegenüber den Beschäftigten verpflichtet, das Fernmeldegeheimnis zu wahren. Aus datenschutzrechtlicher Sicht hat die Behörde dabei die Vorschriften der Telekommunikations-Datenschutzverordnung, des Teledienstedatenschutzgesetzes sowie des Mediendienste-Staatsvertrages zu beachten. Abweichungen von diesen Vorschriften zu Lasten der Beschäftigten sind auch durch eine Dienstvereinbarung nicht zulässig. Eine detaillierte Protokollierung oder Inhaltskontrolle der privaten Nutzung ist auch mit Einwilligung der Mitarbeiterinnen und Mitarbeiter nicht zulässig, da es in einem Dienst- oder Arbeitsverhältnis zum einen an der erforderlichen Freiwilligkeit fehlt. Zum anderen ist insbesondere beim E-Mail-Verkehr auch das Fernmeldegeheimnis des privaten Kommunikationspartners betroffen. So ist es dem Dienstherrn bzw. Arbeitgeber nicht erlaubt, erkennbar private E-Mails zur Kenntnis zu nehmen. Auch die private Nutzung sowie das Vorgehen bei Missbrauch sollte durch Dienstvereinbarung unter Beteiligung des Personalrats geregelt werden.

Private E-Mails sind wie private schriftliche Post zu behandeln. Das heißt, dass eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis gegeben werden müssen. Eine Kontrolle des Inhalts von E-Mails ist unzulässig. Keine Bedenken bestehen, wenn aus Gründen der Datensicherheit Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthal-

ten. Die Bediensteten sind darüber zu unterrichten. Besteht der Verdacht strafbarer Handlungen bei der Nutzung der elektronischen Post, bleibt dem Dienstherrn oder Arbeitgeber nur die Möglichkeit, die Staatsanwaltschaft einzuschalten.

Weiterhin ist es bei privater E-Mail Nutzung erforderlich, diese möglichst auf technischer Ebene von der dienstlichen Nutzung zu trennen. Anderenfalls muss bei jeder dienstlichen E-Mail davon ausgegangen werden, dass es sich auch um eine private E-Mail handeln könnte, sodass auch dienstliche E-Mails nicht kontrolliert werden dürften. Wir empfehlen, für die Beschäftigten entweder separate E-Mail-Adressen für die private Nutzung einzurichten oder – für den Fall, dass das private Nutzen des Internet erlaubt ist – sie an einen kostenlosen Web-Mail-Dienst zu verweisen und die private Nutzung des dienstlichen E-Mail-Anschlusses zu untersagen.

Wird auch die private Nutzung des Internet erlaubt, darf nur aus Gründen der Datensicherheit oder zu Zwecken der Abrechnung protokolliert werden. Deshalb ist auch hier eine Trennung der dienstlichen von der privaten Nutzung auf technischer Ebene zu ermöglichen. Es bietet sich an, für die private Nutzung einen Einzelplatzrechner zur Verfügung zu stellen.

Bietet eine öffentliche Stelle ihren Bediensteten die dienstliche und/oder private Nutzung von E-Mail und Internet an, hat sie eine Reihe von datenschutzrechtlichen Anforderungen zu beachten. Art und Umfang von Protokollierung und Kontrolle der Nutzung dieser Dienste sind in einer Dienstvereinbarung unter Beteiligung des Personalrates festzulegen. Nähere Informationen zum Thema „Datenschutz bei der Nutzung von Internet und Intranet“ sind unserem Internetangebot zu entnehmen[43].

3.1.3 Sicheres Bezahlen im Internet

Zunehmend erfolgt die Verlagerung von Geschäftsprozessen in das Internet. Ob der Konsum von Waren und Dienstleistungen im Internet in Anspruch genommen wird, hängt in entscheidendem Maße davon ab, inwieweit dort auch eine Bezahlung möglich ist. Gleiches gilt bei Internet-Projekten der öffentlichen Verwaltung[44], wenn bei ihnen Gebühren ohne Medienbruch über das Internet bezahlt werden sollen.

Die bisher gängigen Möglichkeiten des bargeldlosen Zahlungsverkehrs lassen sich nur teilweise ins Internet übertragen. Vor allem aber fehlt es bisher

[43] http://www.lda.brandenburg.de/material/oh_int.htm
[44] s. oben A 1.4

an der Akzeptanz durch die Bürgerinnen und Bürger, denen eine Zahlung über das Internet nicht sicher genug ist.

Viele befürchten zudem, dass bei der Zahlung im Internet eine Vielzahl von personenbezogenen Daten entsteht, die von den an Zahlungsvorgängen beteiligten Stellen beispielsweise zur Erstellung umfassender Nutzerprofile verarbeitet wird. Das Misstrauen, das Schicksal einmal ins Netz gegebener personenbezogener Daten nicht mehr kontrollieren zu können, ist weit verbreitet.

Auf der anderen Seite zeigt sich ein erhebliches Interesse, den Bürgerinnen und Bürgern akzeptable, sichere und dennoch einfach zu handhabende Zahlungslösungen für das Internet anzubieten. Der Gesetzgeber hat 2001 mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) nunmehr ausdrücklich die Daten verarbeitenden Stellen dazu verpflichtet, das Ziel von Datensparsamkeit und Datenvermeidung anzustreben. Das ist vor allem durch Anonymisierung und Pseudonymisierung zu erreichen. Die gleiche Verpflichtung besteht bereits seit 1997 für die Anbieter von Multimedia-Diensten und seit 1998 für die Verwaltung in Brandenburg. Damit stellt auch der Gesetzgeber klar, dass der beste Datenschutz dort herrscht, wo personenbezogene Daten gar nicht erst entstehen.

Zahlungsverfahren im Internet beschränken sich nicht nur auf die Geschäftswelt, also auf die Beziehung zwischen Verbrauchern und Unternehmen (Business to Consumer B2C). Im Rahmen des E-Government werden sie auch zwischen Bürgerinnen und Bürgern sowie der Wirtschaft einerseits und der Verwaltung andererseits in den Bereichen „Business to Administration (B2A)“ als auch „Citizen to Administration (C2A)“ zunehmend Anwendung finden.

Um einen Überblick zu gewinnen, inwieweit die auf dem Markt befindlichen oder geplanten Zahlungsverfahren im Internet den datenschutzrechtlichen Forderungen Rechnung tragen, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und dem Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern im Februar 2001 sieben Anbieter zu einer Präsentationsveranstaltung eingeladen, um ihre Lösungen für die Zahlung von Waren und Dienstleistungen im Internet vorzustellen.

Es hat sich gezeigt, dass ein hohes Interesse an Fragen des Datenschutzes und der Datensicherheit besteht, weil beides für die Akzeptanz eines Verfahrens entscheidend ist. Die Anbieter begriffen dies weniger als Behinderung, sondern vielmehr als Marktvorteil.

Bei allen vorgestellten Verfahren sind unterschiedliche Möglichkeiten der anonymen oder pseudonymen Nutzung vorgesehen. Einerseits kommt es darauf an, ob der Nutzer gegenüber dem Anbieter bzw. dem Emittenten anonym bzw. pseudonym agieren kann. Mindestens ebenso wichtig ist andererseits, ob dies – ähnlich wie bei den üblichen Bar-Geschäften des täglichen Lebens – auch gegenüber dem Händler (bzw. der öffentlichen Stelle), deren Dienstleistung bezahlt werden soll, möglich ist.

Es hat sich gezeigt, dass ein anonymes oder zumindest pseudonymes Auftreten gegenüber dem Zahlungsdienstleister nicht bei allen Verfahren möglich ist. Insbesondere bei den Lösungen, die auf einer Zahlung mit Kreditkarte beruhen, lässt sich eine vollständige Anonymität gegenüber dem Emittenten nicht herstellen. Es befinden sich aber auch Verfahren auf dem Markt, die eine vollständig anonyme Zahlung gegenüber dem Anbieter mittels Guthabenkarte ermöglichen.

Ebenso wichtig sind Aspekte der Datensicherheit. So ist der Einsatz zum Teil starker Verschlüsselungsverfahren bei der Übertragung personenbezogener Daten weitgehend selbstverständlich.

Weiterhin ist es für die Nutzer nicht immer einfach, die einzelnen Schritte der Verarbeitung seiner personenbezogenen Daten nachzuvollziehen. Manche Verfahren sind so komplex, dass sie kaum breitere Akzeptanz finden dürften.

Öffentliche Stellen, die die Bezahlung ihrer Dienstleitungen über das Internet ermöglichen wollen, können inzwischen auf eine Reihe von Verfahren zurückgreifen, die den Grundsatz von Datenvermeidung und Datensparsamkeit gut berücksichtigen und ein hohes Maß an Datensicherheit aufweisen.

3.2 Datenschutz beim Ostdeutschen Rundfunk Brandenburg

3.2.1 Daten der Gebührenzahler gut geschützt?

Aufgrund unserer Befugnis, die Einhaltung datenschutzrechtlicher Bestimmungen beim Ostdeutschen Rundfunk Brandenburg (ORB) außerhalb des journalistisch-publizistischen Bereichs kontrollieren zu können, haben wir mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bei der gemeinsamen Rundfunkgebührenstelle von ORB und Sender Freies Berlin (SFB) geprüft, inwieweit der Datenschutz bei der Erhebung der Rundfunkgebühren gewährleistet ist.

Die gemeinsame Rundfunkgebührenstelle verarbeitet sowohl personenbezogene Daten über Rundfunkteilnehmer als auch solche der Rundfunkbe-

auftragten. Die Rundfunkbeauftragten sind freie Mitarbeiter von ORB bzw. SFB, die die Rundfunkanstalten bei der Ermittlung von nicht angemeldeten Rundfunkteilnehmern im Außendienst unterstützen. Wie alle übrigen öffentlich-rechtlichen Rundfunkanstalten haben auch ORB und SFB die Gebühreneinzugszentrale in Köln (GEZ) mit dem Einzug der Rundfunkgebühren beauftragt. Deshalb findet der überwiegende Teil der Datenverarbeitung hinsichtlich der Hörer und Fernsehzuschauer dort statt. Die Rundfunkgebührenstelle bearbeitet lediglich besondere Einzelfälle im Zusammenhang mit dem Einzug der Rundfunkgebühren. Sie versendet Bescheide, führt Widerspruchsverfahren durch und bearbeitet Beschwerden der Rundfunkteilnehmer. Soweit nicht eine besondere Zuständigkeit der Sozialämter besteht, entscheidet die Rundfunkgebührenstelle auch über die Befreiungen von der Rundfunkgebühr.

Die Prüfung hat ergeben, dass die datenschutzrechtlichen Bestimmungen in der gemeinsamen Gebührenstelle weitgehend eingehalten werden. Folgende Mängel wurden allerdings festgestellt:

Möchte ein Rundfunkteilnehmer aus sozialen Gründen von der Rundfunkgebühr befreit werden, so muss er dies bei seinem zuständigen Sozialamt beantragen. Zwar ist nach der Rundfunkgebührenbefreiungsverordnung vorgesehen, dass der ORB selbst auf Vorschlag des Sozialamtes über die Befreiung von der Rundfunkgebühr entscheidet. Faktisch befindet das jeweilige Sozialamt eigenständig über den Antrag auf Befreiung. Dennoch übermitteln die Sozialämter regelmäßig die einzelnen Gründe für die Befreiung von der Rundfunkgebühr an die GEZ. Für eine solche regelmäßige Übermittlung dieser sehr sensiblen personenbezogenen Daten sehen wir aufgrund dieser Praxis keine Erforderlichkeit. Diese ist daher nur in begründeten Einzelfällen zulässig.

Die Tätigkeit der Rundfunkbeauftragten wird trotz der Tatsache, dass diese freie Mitarbeiter sind, vom ORB als Datenverarbeitung im Auftrag angesehen. Dies entspricht dem Rundfunkgebührenstaatsvertrag. Wir haben dem ORB empfohlen, die vertraglichen Vereinbarungen mit den Rundfunkbeauftragten zu ergänzen. Nach dem Brandenburgischen Datenschutzgesetz ist es bei einer Datenverarbeitung im Auftrag erforderlich, die Art und Weise der Verarbeitung personenbezogener Daten einschließlich der zu treffenden technisch-organisatorischen Maßnahmen und ergänzender Weisungen detailliert und verbindlich schriftlich festzulegen. Dabei muss der Charakter der Datenverarbeitung im Auftrag als untergeordnete Hilfstätigkeit ohne eigene Entscheidungsbefugnisse deutlich hervortreten. Dies war bisher nicht in ausreichender Weise geschehen. Den Rundfunkbeauftragten gegenüber muss verbindlich festgelegt werden, wann sie berechtigt sind, Auskünfte von Betroffenen zu verlangen. Schließlich haben wir dem ORB empfohlen, sog. Teilnehmer-

datenkarten, die der Rundfunkbeauftragte zur Erfüllung seiner Aufgaben benutzt, ohne Angabe der Kontoverbindung einzuführen.

Technisch ist es dem ORB derzeit möglich, auf die Teilnehmerdaten von rd. 30 Millionen Haushalten in Deutschland zuzugreifen. Zwar kann nach dem Rundfunkgebührenstaatsvertrag eine Rundfunkanstalt im Einzelfall personenbezogene Daten von Rundfunkteilnehmern auch an andere Rundfunkanstalten im Rahmen eines automatisierten Abrufverfahrens übermitteln, wenn dies zur Aufgabenerfüllung einer der beiden Anstalten erforderlich ist. Allerdings halten wir es nicht für erforderlich, dass eine Rundfunkanstalt jeweils auf den gesamten Datenkatalog der Rundfunkteilnehmer aus dem Einzugsbereich anderer Rundfunkanstalten zugreifen kann. Wir haben dem ORB daher empfohlen, sich für die Beschränkung des Datenkatalogs, auf den regelmäßig zugegriffen werden kann, einzusetzen.

Der ORB hat zu erkennen gegeben, dass er eine Reihe unserer Empfehlungen umsetzen wird.

Die Verarbeitung von personenbezogenen Daten der Rundfunkteilnehmer durch den Ostdeutschen Rundfunk Brandenburg entspricht ganz überwiegend den datenschutzrechtlichen Bestimmungen. Zur Verbesserung des Datenschutzes waren lediglich kleinere Empfehlungen erforderlich.

3.2.2 „Haben Sie wirklich keinen Fernseher?“ – Zum Zweiten

Bereits 1999[45] haben wir darüber berichtet, in welchem Umfang Rundfunkteilnehmerinnen und Rundfunkteilnehmer, die lediglich ein Radio angemeldet haben, dem ORB bzw. der Gebühreneinzugszentrale (GEZ) gegenüber Auskünfte erteilen müssen. Der ORB hält an seiner Auffassung fest, dass jeder Radiobesitzer verpflichtet sei, dem ORB mitzuteilen, dass er kein Fernsehgerät hat.

Die Auffassung des ORB läuft darauf hinaus, diejenigen, die ihm als „Nur-Hörer“ bekannt werden, schlechter zu stellen als diejenigen, die sich bei der GEZ überhaupt nicht angemeldet haben. Letztere müssen auch nach Auffassung des ORB nicht mitteilen, dass sie keine Rundfunkgeräte besitzen.

Bei den durch jährliche Mailing-Aktionen angeschriebenen „Nur-Hörfunkteilnehmern“ wird insbesondere durch das wiederholte Nachfragen der Eindruck erweckt, es ließen sich aus der Anmeldung eines Radios tatsächliche Anhaltspunkte für ein nicht angemeldetes Fernsehgerät herleiten. Es besteht

[45] s. Tätigkeitsbericht 1999, A 3.4.2

keine Pflicht zur Negativauskunft, nur weil jemand als Besitzer eines Radios Rundfunkteilnehmer im Sinne des Rundfunkgebührenstaatsvertrages ist.

Wir haben dem ORB mehrfach empfohlen, die Bürgerinnen und Bürger darauf hinzuweisen, dass die Angabe, keinen Fernseher zu besitzen, von den angeschriebenen Rundfunkteilnehmerinnen und -teilnehmern nur auf freiwilliger Basis erlangt werden kann. Dennoch verwendet der ORB das bemängelte Anschreiben weiter und erweckt so bei den Befragten den unrichtigen Eindruck, dass sie dazu verpflichtet seien. Da ein solches Verhalten nicht hingenommen werden kann, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht dies gegenüber dem ORB als Auftraggeber der GEZ nunmehr förmlich beanstandet.

Hat jemand ein Radio bei der vom ORB beauftragten GEZ angemeldet, so ist er nicht verpflichtet mitzuteilen, dass er keinen Fernseher besitzt. Die Landesregierung wird gebeten, sich bei der ab dem Jahr 2004 geplanten Neuregelung der Rundfunkfinanzierung für eine unmissverständliche Formulierung von Auskunftspflichten im Rundfunkgebührenstaatsvertrag einzusetzen.

3.3 Freiwillige Selbstkontrolle der Presse – Chance oder Risiko?

Das neue Bundesdatenschutzgesetz (BDSG) verpflichtet in § 41 Abs. 1 die Länder dazu, in ihrer Gesetzgebung die Verarbeitung personenbezogener Daten durch die Presse zu ausschließlich eigenen journalistisch-redaktionellen oder literarischen Zwecken zu regeln. Es müssen zumindest Vorschriften zum Datengeheimnis, zu den technischen und organisatorischen Maßnahmen sowie zum Schadensersatz vorhanden sein. Außerdem können entsprechend § 38 a BDSG Verhaltensregeln zur praktischen Umsetzung datenschutzrechtlicher Bestimmungen geschaffen werden.

Der Deutsche Presserat – ein Gremium zur freiwilligen Selbstkontrolle der Presse hinsichtlich der Einhaltung presserechtlicher Grundsätze – hat sich der Aufgabe angenommen, die Vorschrift des § 38 a BDSG umzusetzen. Dazu hat er seine Satzung dahingehend geändert, dass zu seinen Aufgaben nunmehr auch die Selbstregulierung im Bereich des Redaktionsdatenschutzes gehört. Ein neuer Beschwerdeausschuss wurde eingerichtet, der für die Bearbeitung von Beschwerden in diesem Bereich zuständig ist.

Inzwischen hat der Deutsche Presserat auch allgemeine Datenschutzleitlinien in den Pressekodex übernommen. Diese Leitlinien enthalten Regeln zur Richtigstellung falscher Berichterstattung sowie deren Dokumentation, zur Auskunft über die der Berichterstattung zugrunde liegenden personenbezogenen

Daten, zur Löschung und Archivierung personenbezogener Daten sowie zum Umfang zulässiger Datenübermittlungen. Der neue Pressekodex wurde im November 2001 offiziell dem Bundespräsidenten überreicht.

Problematisch ist bei diesem Versuch einer Selbstregulierung, dass die Trägervereine des Deutschen Presserates nur einen Teil der Zeitungs- und Zeitschriftenverlage repräsentieren. Fraglich ist daher, ob auch Verlage, die nicht Mitglied dieser Trägervereine sind, durch den Deutschen Presserat über § 38a BDSG verpflichtet werden können. Sollte eine nennenswerte Zahl von Presseunternehmen nicht gebunden werden können, besteht die Gefahr, dass die Europäische Datenschutzrichtlinie nicht ausreichend umgesetzt wird und die Selbstkontrolle bei vielen Verlagen nicht greift.

Unabhängig vom Gelingen der Selbstregulierung ist es erforderlich, dass das Brandenburgische Landesrecht den Vorgaben von § 41 Abs. 1 BDSG angepasst wird. Nur so kann ein einheitliches Datenschutzrecht für alle Presseunternehmen sowie eine ausreichende Umsetzung der Europäischen Datenschutzrichtlinie im Pressebereich gewährleistet werden. Ein entsprechender Entwurf der Staatskanzlei ist uns inzwischen zugegangen.

Die Landesregierung sollte eine Anpassung des Brandenburgischen Presse- und Datenschutzrechts an § 41 Abs. 1 BDSG sowie an die EG-Datenschutzrichtlinie anstreben.

4 Inneres

4.1 Polizei

4.1.1 Datenexport vor Weltwirtschaftskonferenzen

Im Berichtszeitraum haben sich mehrere Personen an uns gewandt, weil das Bundeskriminalamt personenbezogene Daten über sie an die Polizeien der ausländischen Konferenzorte übermittelt hatte. Bei einem Betroffenen hatte das zur Folge, dass er zwar nach den Kontrollen an der Grenze seine Reise zum Veranstaltungsort fortsetzen konnte, kurz vor Erreichen des Zieles aber angehalten, in Gewahrsam genommen und 48 Stunden später nach Deutschland abgeschoben wurde.

Die Prüfung des Sachverhalts beim zuständigen Polizeipräsidium ergab, dass gegen ihn wegen Nötigung und Sachbeschädigung ermittelt worden war. Dieses Strafverfahren endete jedoch mit einem gerichtlichen Freispruch, sodass das Polizeipräsidium die im Zusammenhang mit dem Ermittlungsverfahren im Polizeilichen Auskunftssystem Straftaten (PASS) und im Kriminalaktennachweis (KAN) gespeicherten Daten gelöscht und die zu dem Peten-

ten geführte Kriminalakte vernichtet hat. Weiterhin hat es auch die Löschung der zu dem Betroffenen im bundesweiten Informationssystem der Polizei (INPOL) gespeicherten Daten beim Bundeskriminalamt veranlasst. Das Bundeskriminalamt löschte jedoch nur das Land Brandenburg als ursprünglichen Datenbesitzer. Der Datensatz selbst blieb als vom Bundeskriminalamt betriebene Speicherung erhalten. Bei den in Rede stehenden Daten handelt es sich um die in der bundesweiten Datei „Erkennungsdienst“ gespeicherten erkennungsdienstlichen Unterlagen, die im Zusammenhang mit dem o. g. Ermittlungsverfahren von dem Betroffenen erhoben worden waren. Das Bundeskriminalamt begründet die Weiterspeicherung erkennungsdienstlicher Unterlagen trotz Löschung durch das für die erkennungsdienstliche Behandlung verantwortliche Bundesland mit der für diese Datei geltenden grundsätzlichen Aussonderungsprüffrist von fünf Jahren. Dies ist jedoch nicht zulässig. Wir haben den Bundesbeauftragten für den Datenschutz gebeten, die Angelegenheit des Betroffenen zuständigkeitshalber weiter zu verfolgen. Unterdessen hat das Bundeskriminalamt ihm mitgeteilt, dass die in Rede stehenden Daten gelöscht worden seien und ihm Schadensersatz für die erlittene Unbill zustehe.

Dessen ungeachtet wirkt die ursprünglich nichtvollzogene Löschung aber weiter. Das zuständige Polizeipräsidium sieht sich aufgrund der Abschiebung, über die es von der dortigen Polizei informiert worden ist, veranlasst, mit dem Petenten vor jedem Weltwirtschaftstreffen eine sog. Gefährderansprache zu führen, in deren Verlauf der Petent darauf hingewiesen wird, dass er besser nicht zu den Konferenzorten fahren solle.

Für diese Gefährderansprache und die Einschränkung der Freizügigkeit gibt es keine Rechtsgrundlage, weil der Betroffene sich bislang straffrei geführt hat. Ob und inwieweit das Polizeipräsidium dem Rechnung tragen wird, ist noch offen.

Das Bundeskriminalamt ist unter Beachtung des Verhältnismäßigkeits gem. § 14 Abs. 1 Bundeskriminalamtsgesetz (BKAG) grundsätzlich befugt, Daten ins Ausland zu übermitteln. Jedoch handelte es sich bei dem übermittelten Sachverhalt nicht um konkret nachgewiesene Tatvorwürfe, sondern um einen mehrere Jahre zurückliegenden Verdachtsfall. Fest steht, dass der Verfahrensstand nicht vor der Datenübermittlung bei dem zuständigen Polizeipräsidium abgefragt worden ist.

Weiterhin hat es auch gegen § 32 Abs. 2 i. V. m. Abs. 8 BKAG verstoßen, demgemäss übermittelte Daten zu löschen sind, wenn die übermittelnde Stelle das Bundeskriminalamt über die Löschung informiert. Nach dem Freispruch hat das zuständige Polizeipräsidium die Löschung veranlasst. Damit war eine Weiterspeicherung unzulässig.

Der Fall macht deutlich, wie wichtig eine regelmäßige Überprüfung von Datenspeicherungen in polizeilichen Datenbeständen des Bundes und der Länder und die strikte Einhaltung von Löschungsverpflichtungen durch die Polizei insbesondere vor einer Datenübermittlung ins Ausland sind. Aus einem laxen Umgang mit personenbezogenen Daten können nicht nur dem Betroffenen schwere Nachteile entstehen, sondern auch den jeweiligen staatlichen Stellen finanzieller Schaden durch Schadensersatzleistungen.

4.1.2 Die Dateien „LIMO“, „REMO“ und „AUMO“ beim Bundeskriminalamt

Die Dateien „Gewalttäter rechts – REMO“, „Gewalttäter links – LIMO“ und „Straftäter politisch motivierter Ausländerkriminalität – AUMO“ sollen der Bekämpfung politisch motivierter Gewalttaten dienen. Als Verbunddateien werden sie jedoch erst im Rahmen von INPOL-neu realisiert. Bis dahin wird die Verarbeitung der dort zu erfassenden Daten als Anlass-/Zweckkombination in der INPOL-Personenfahndungsdatei und als „Personengebundener Hinweis“ (PHW) in den INPOL-Dateien „Personenfahndung“, „Erkennungsdienst“ und „Kriminalaktennachweis“ geführt. Obwohl die in Rede stehenden Erfassungen bereits seit geraumer Zeit betrieben werden, hat das Bundesministerium des Innern erst jetzt das sog. Zustimmungsverfahren nach § 34 Abs. 2 Bundeskriminalamtgesetz (BKAG) eingeleitet, um die für INPOL-Dateien erforderliche Zustimmung der Bundesländer einzuholen. Das Brandenburgische Ministerium des Innern hat uns die Errichtungsanordnungen zur Stellungnahme übersandt.

Rechtsgrundlage für die Speicherung der Daten ist insbesondere § 8 BKAG. Demgemäss dürfen personenbezogene Daten von Beschuldigten und – so erforderlich – andere zur Identifizierung geeignete Merkmale verarbeitet werden. Weitere personenbezogene Daten wie die Anlass-/Zweckkombination und PHW's dürfen von Beschuldigten und Tatverdächtigen nur verarbeitet werden, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass der Betroffene in Zukunft erneut straffällig wird (Negativprognose).

Zwar enthalten die Errichtungsanordnungen einen Katalog von Straftaten und eine Auflistung sonstiger Tatbestände, in deren Zusammenhang personenbezogene Daten in den Dateien erfasst werden sollen, es fehlt jedoch an Kriterien für eine Negativprognose als grundlegende Voraussetzung für die Verarbeitung eines personenbezogenen Datums in der Datei. Maßgeblich muss dabei sein, dass die Straftat, auf die sich der Verdacht bezieht und wegen der Grund zu der Annahme besteht, dass der Betroffene auch zukünftig strafrechtlich in Erscheinung treten wird, in einem ursächlichen Zusammenhang

mit seiner politischen Orientierung steht. Die Anhaltspunkte müssen zudem auf eine bestimmte politische Motivation hindeuten. Neben dem Straftatenkatalog und der Auflistung einschlägiger Ereignisse, bei denen die in Rede stehenden Gewalttäter auftreten können, sollten die Errichtungsanordnungen daher auch eine Zusammenstellung von Anhaltspunkten enthalten, um so sicherzustellen, dass nur personenbezogene Daten von Betroffenen mit entsprechender politischer Motivation eingestellt werden.

Es dürfen nur personenbezogene Daten im Zusammenhang mit Straftaten von überregionaler Bedeutung in die Dateien aufgenommen werden. Die Zentralstellenfunktion des Bundeskriminalamtes zur Unterstützung der Polizeien des Bundes und der Länder ist auf die Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung beschränkt. Es kann also keineswegs so sein, dass insbesondere Straftaten aus rechtsorientierten, politisch motivierten Beweggründen grundsätzlich für die Datenverarbeitung relevant sind. Gerade rechtsex-tremistische Aktivitäten von Einzeltätern bzw. von losen Gruppierungen beschränken sich meist auf das engere lokale Umfeld der Täter. Sie dürften mangels überregionaler Bedeutung auch nicht in die Datei „REMO“ aufgenommen werden.

Zur Festlegung von Prüffristen, Speicherungsdauer und Veränderungen sowohl in den Dateien als auch der Anlass-/Zweckkombination und der PHW's verweisen die Errichtungsanordnungen auf § 32 BKAG. Die Aussonderungsprüffrist wird für Erwachsene und Jugendliche grundsätzlich auf fünf Jahre, für Kinder auf zwei Jahre und für sonstige Personen auf drei Jahre festgesetzt. Zu den PHW's ist jedoch festgelegt, dass die Aussonderungsprüffristen bei Erwachsenen zehn, bei Jugendlichen fünf und bei Kindern zwei Jahre nicht überschreiten dürfen. Regelmäßige Prüffristen in kürzeren Zeitabständen bis zum Ablauf der Aussonderungsprüffrist sind nicht vorgesehen.

In vielen Einzelfällen dürfte das unverhältnismäßig sein. Insbesondere die nach § 8 Abs. 2 BKAG zu stellende Prognose, dass der Betroffene künftig erneut wegen einer politisch motivierten Straftat straffällig werden wird, erfordert eine Überprüfung dieser Motivation in kurzen Zeitabständen. Das gilt gerade auch für den Personenkreis der Verdächtigen, bei denen die Gefahr besteht, dass ihre Daten für längere Zeit ungeprüft gespeichert bleiben, weil die Begründetheit des Verdachts – anders als bei Beschuldigten – nicht nach den Vorschriften der StPO von der Staatsanwaltschaft bzw. einem Gericht beurteilt wird. Bei diesem Personenkreis kann eine Speicherung von bis zu 10 Jahren insbesondere mit Hinblick auf die eventuell dem Betroffenen erwachsenden Konsequenzen[46] nicht hingenommen werden. Insbesondere muss in den Errichtungsanordnungen vorgesehen werden, dass auch die für eine Datenspeicherung verantwortlichen Länderpolizeien auf der Grundlage ihrer

[46] s. unten A 4.1.7

Vorschriften bei ihrer Einzelfallbearbeitung Datenlöschungen veranlassen können, denen das Bundeskriminalamt folgen muss.

In die Dateien sollen neben Beschuldigten, Verdächtigen und rechtskräftig verurteilten Personen auch solche Personen aufgenommen werde, gegen die lediglich Personalienfeststellungen, Platzverweise und Ingewahrsamnahmen zur Verhinderung anlassbezogener Straftaten angeordnet wurden, unter der Voraussetzung, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen könnten. Die Speicherung personenbezogener Daten lediglich aufgrund von Erkenntnissen aus präventiv-polizeilichen Maßnahmen, die nicht automatisch in ein strafrechtliches Gerichtsverfahren münden, ist datenschutzrechtlich sehr problematisch.

Die notwendigen Konkretisierungen der Tatsachen, die die Annahme rechtfertigen, dass der Betroffene zukünftig im Zusammenhang mit politisch motivierten Straftaten von erheblicher Bedeutung straffällig werden könnte (Negativprognose), müssen in den Errichtungsanordnungen ergänzt werden. Die Prognose darf sich nur auf solche Straftaten beziehen; Personalienfeststellung, Platzverweise und vorbeugende Ingewahrsamnahme rechtfertigen nicht die Einstellung in eine bundesweite Datei.

4.1.3 Trotz Freispruch: Veröffentlichung und anhaltende Speicherung des Vorwurfs der Vergewaltigung

In mehreren Zeitungsberichten über eine erneute Flucht aus dem Maßregelvollzug wurde dem zuständigen Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF) vorgeworfen, es habe die von dem Entflohenen ausgehende Gefährdung der Öffentlichkeit bagatellisiert. Das zuständige Polizeipräsidium hatte im Zuge der Öffentlichkeitsfahndung den Namen sowie eine Personenbeschreibung des Betroffenen und die Tatsache mitgeteilt, dass dieser wegen gefährlicher Körperverletzung im Maßregelvollzug untergebracht und wegen weiterer Straftaten polizeilich in Erscheinung getreten sei. Nach seiner Wiederergreifung veröffentlichte das Innenministerium eine Pressemitteilung, aus der erstmals hervorging, dass er mit 27 Delikten, „unter anderem einer Vergewaltigung", im „Polizeilichen Auskunftssystem Straftaten" (PASS) registriert sei. Die Zeitungen griffen diese Pressemitteilung auf und stellten die Datenspeicherungen einschließlich der Vergewaltigung als Taten dar, die der Entwichene begangen habe. Obwohl das Verfahren wegen des Tatvorwurfs der Vergewaltigung mit einem Freispruch des Betroffenen abgeschlossen worden war, lehnt die Polizei die Löschung dieses Tatvorwurfs mit der Begründung ab, dass weiterhin ein Restverdacht bestehe.

Aus dem Sachverhalt ergaben sich Mängelfeststellungen bezüglich der Pressearbeit des Innenministeriums und der Datenverarbeitung von Polizei und Staatsanwaltschaft.

Auch wenn in der Pressemitteilung des Ministeriums des Innern der Name des Betroffenen nicht genannt wird, sind die aufgeführten Sachverhalte ausreichend personenbezogen. Das Polizeipräsidium hatte nämlich am Vortag im Zuge der Öffentlichkeitsfahndung nach dem Betroffenen Name und Alter sowie eine Personenbeschreibung veröffentlicht. In der Presse waren diese Angaben beschränkt auf die Initialen des Nachnamens wiedergegeben worden.

Als Rechtsgrundlage ist § 16 i.V.m. § 13 Abs. 2 Satz 1 Buchst. d Brandenburgisches Datenschutzgesetz (BbgDSG) heranzuziehen, weil eine Pressemitteilung – soweit sie personenbezogene Daten enthält – datenschutzrechtlich einer Übermittlung an den nicht öffentlichen Bereich gleichkommt. Danach sind Übermittlungen zulässig, wenn sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich sind. Weiterhin ist § 5 Abs.1 Landespressegesetz (BbgPG) insoweit zu berücksichtigen, als die übermittelten Informationen der Presse zur Erfüllung ihrer öffentlichen Aufgaben dienen müssen. Daraus ergeben sich Anforderungen bezüglich Wahrheitsgehalt, Vollständigkeit und Eindeutigkeit, da die Presse bei ihrer Berichterstattung auf wahre Auskünfte, die den tatsächlichen Sachverhalt eindeutig wiedergeben, angewiesen ist. Die Behörden müssen sich daher vergewissern, dass die mitzuteilenden Sachverhalte die Wirklichkeit wiederspiegeln. Schließlich müssen gem. § 5 Abs. 2 BbgPG der Presse Auskünfte verweigert werden, wenn damit ein schutzwürdiges privates Interesse verletzt würde. Dieser Grundsatz ist auch bei Presseerklärungen zu berücksichtigen.

Bei ihrer Pressearbeit haben die öffentlichen Stellen zum einen eine Prüfungspflicht bezüglich der Richtigkeit und Vollständigkeit der Information und zum anderen die Verpflichtung, zwischen dem Informationsinteresse der Öffentlichkeit und dem Grundrechtsschutz eines eventuell Betroffenen sorgfältig abzuwägen. Zu beidem ist die Behörde um so mehr verpflichtet, wenn sie mit eigenen Pressemitteilungen unaufgefordert an die Öffentlichkeit tritt und personenbezogene Sachverhalte von sich aus veröffentlicht.

Durch die Pressemitteilung der Polizei waren der Öffentlichkeit neben den o.g. näheren Angaben zur Person nur die Sachverhalte über den Betroffenen bekannt gegeben worden, die erforderlich waren, um vor der von dem Entwichenen ausgehenden Gefährdung der öffentlichen Sicherheit zu warnen. Der Tatvorwurf der Vergewaltigung war nicht auf gesicherte Erkenntnisse zu stützen, daher ist er auch nicht aufgenommen worden. Die Veröffentlichung von

Namen, Alter und Personenbeschreibung ist gem. § 131 Abs. 4 Strafprozessordnung (StPO) zulässig, wenn wegen einer Straftat von erheblicher Bedeutung eine Öffentlichkeitsfahndung unerlässlich ist. Diese Voraussetzungen waren im Hinblick auf die dem Betroffenen zur Last gelegten Delikte und dem Ablauf vorausgegangener Entfernungen des Betroffenen aus dem Maßregelvollzug erfüllt. Der Betroffene musste die mit der Übermittlung an den nicht öffentlichen Bereich in Form der Pressemitteilung des Polizeipräsidiums einschließlich der Medienberichterstattung verbundenen tiefen Eingriffe in seine Persönlichkeitsrechte im überwiegenden Allgemeininteresse hinnehmen. Dies galt nur so lange, wie er noch flüchtig war.

Bei seiner Pressemitteilung nach der Ergreifung hat das Ministerium des Innern die sich aus den Vorschriften des Brandenburgischen Datenschutzgesetzes sowie des Pressegesetzes herzuleitenden Grundsätze nicht beachtet. So hat es den Tatvorwurf der Vergewaltigung ohne vorherige Verifizierung veröffentlicht, obwohl der Datensatz in PASS, nur den Tatvorwurf aus 1995 enthält, nicht aber den Verfahrensausgang des Ermittlungsverfahrens. Es ist seit Jahren bekannt, dass bei einer im Datensatz fehlenden Mitteilung über den Verfahrensausgang die Richtigkeit der Datenspeicherung in PASS und in anderen kriminalpolizeilichen Sammlungen nicht zweifelsfrei gegeben ist. Das Ministerium hätte erkennen müssen, dass zum Schutz der Persönlichkeitsrechte des Betroffenen weitere Tatsachenfeststellungen geboten waren. Es wäre verpflichtet gewesen, zunächst bei den zuständigen Stellen, z. B. bei der Staatsanwaltschaft, nachzufragen, ob dem Betroffenen die fragliche Vergewaltigung nachgewiesen worden war. Gerade bei Tatvorwürfen aus dem Bereich der Sexualdelikte ist besondere Sorgfalt geboten, da zum einen die Öffentlichkeit besonderes sensibel auf solche Veröffentlichungen reagiert, zum anderen der Makel des Sexualverbrechers besonders schwer auf dem Betroffenen lastet. Die Veröffentlichung eines solchen Deliktes kann daher im Rahmen der Öffentlichkeitsfahndung nach einem entwichenen Straftäter nur in Frage kommen, wenn der Betroffene deswegen rechtskräftig verurteilt worden ist.

Des Weiteren hat das Ministerium nicht abgewogen, ob und inwieweit nach der Wiederergreifung des Flüchtigen durch seine Pressemitteilung das Interesse des Betroffenen an der Geheimhaltung der Informationen verletzt würde. Das wäre aber nach § 5 Abs. 2 Nr. 3 BbgPG erforderlich gewesen. Da nun von dem Flüchtigen keine Gefährdung der Öffentlichkeit mehr ausgehen konnte, lässt sich folglich auch kein Anspruch auf die Kenntnis der Tatvorwürfe zum Schutz der Öffentlichkeit mehr herleiten.

Nicht hinnehmbar ist auch die fortdauernde Datenspeicherung des Vorwurfs der Vergewaltigung bei der Polizei. Soweit diese die Meinung vertritt, dass im vorliegenden Fall die nach § 170 Abs. 2 StPO bereits eingestellten Ermitt-

lungsverfahren zu dem Betroffenen nicht gelöscht werden müssen, ist dies zwar grundsätzlich auf Grund der Vielzahl der ihm zur Last gelegten Straftaten gerechtfertigt. Insbesondere unter dem Aspekt des fortdauernden Tatverdachts ist eine weitergehende Speicherung dieser Tatvorwürfe datenschutzrechtlich nicht zu bemängeln. Wird aber der Betroffene wegen eines Tatvorwurfs freigesprochen, so ist eine weitere Speicherung dieses Vorwurfs unzulässig. Mit dem Freispruch ist das Verfahren abgeschlossen. Mit Rechtskraft des Urteils tritt Bindungswirkung und Strafklageverbrauch ein. Anders als bei einer Einstellung nach § 170 Abs. 2 StPO kann die Staatsanwaltschaft das Ermittlungsverfahren hier nicht jederzeit wieder aufnehmen. Selbst wenn sich nach Rechtskraft eines Urteils der Tatvorwurf bestätigen sollte, wäre eine Verurteilung wegen des Strafklageverbrauches unmöglich. Dieser Grundsatz muss sich auch in der Datenverarbeitung der Polizei wiederspiegeln. Es ist daher nicht zulässig, dass trotz eines freisprechenden Urteils, welches in Rechtskraft erwachsen ist, mit dem Argument eines „Resttatverdachts“ diese Daten weiter aufbewahrt werden. Damit blieben die Entscheidung des Gerichts und die daraus resultierenden strafprozessualen Grundsätze völlig unbeachtet.

Letztendlich ist auch zu bemängeln, dass in den kriminalpolizeilichen Sammlungen des Polizeipräsidiums noch weitere Verfahren des Betroffenen ohne den Abschlussvermerk der Staatsanwaltschaft geführt werden. Gem. § 482 Abs. 2 StPO ist die Staatsanwaltschaft verpflichtet, die Polizeibehörde über den Ausgang des Verfahrens zu unterrichten und die Entscheidungsformel, die entscheidende Stelle sowie Datum und Art der Entscheidung mitzuteilen, damit bei der Polizei die erforderlichen Konsequenzen bezüglich der Datenverarbeitung gezogen werden können. Die unterbliebene Mitteilung und die daraus resultierende falsche Aktenführung hat unter anderem zu dem diskriminierenden Vorwurf gegen den Betroffenen geführt.

Die Behörden müssen bei Ihrer Presse- bzw. Öffentlichkeitsarbeit prüfen, ob die veröffentlichten Daten der Wahrheit entsprechen, wenn der Sachverhalt Unklarheiten aufweist. Bei der Abwägung des öffentlichen Informationsinteresses gegen das Geheimhaltungsinteresse des Betroffenen ist der jeweilige Verfahrensstand festzustellen und in die Ermessensentscheidung einzubeziehen.

Daten aus einem rechtskräftigen, freisprechenden Urteil sind nicht mit Daten aus einer Einstellung gem. § 170 Abs. 2 StPO gleichzusetzen und somit stets zu löschen.

Um Fehlinformationen zu vermeiden und eine aktuelle Aktenführung zu gewährleisten, muss die Staatsanwaltschaft die Polizei gem. § 482 StPO regelmäßig und umfassend informieren.

4.2 Verfassungsschutz

Im Berichtszeitraum hat der Landtag das überfällige Gesetz zur Regelung von Sicherheitsüberprüfungen verabschiedet[47]. Überprüft werden Personen, die eine sicherheitsrelevante Tätigkeit übernehmen sollen. Das Überprüfungsverfahren, an dem die Verfassungsschutzbehörde lediglich mitwirkt, wird von der Dienststelle veranlasst.

Mit dem Sicherheitsüberprüfungsgesetz ist eine wesentliche Rechtslücke für sensible Personaldaten geschlossen worden, auf die der Landesbeauftragte wiederholt hingewiesen hat[48]. Er hat im Gesetzgebungsverfahren eine Reihe von Änderungen vorgeschlagen, die nur zum Teil Eingang in das Gesetz gefunden haben. Noch weitergehend als im Brandenburgischen Verfassungsschutzgesetz sind hier die Kontrollbefugnisse des Landesbeauftragten eingeschränkt worden. Dem Landesbeauftragten persönlich wird die Auskunft verweigert, wenn die zuständige Aufsichts- oder Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Bundeslandes gefährdet würde. Im Verfassungsschutzgesetz steht ihm in Person in solchen Fällen ein Auskunftsrecht zu. Das gilt auch bei Personen, denen im Rahmen einer Sicherheitsüberprüfung Vertraulichkeit zugesichert worden ist, für den Fall, dass diese sich an den Landesbeauftragten wenden.

Damit ist der Landesbeauftragte in solchen Fällen daran gehindert, entsprechend der Landesverfassung darauf zu dringen, dass das Grundrecht auf Datenschutz gewahrt wird. Dem Betroffenen bleibt nur der Weg vor die Gerichte. Auch das Einsichtsrecht der Betroffenen in die zu ihrer Person geführten Si-

[47] GVBl. I 2001 S. 126

[48] vgl. zuletzt Tätigkeitsbericht 2000, A 4.2

cherheitsakten oder Sicherheitsüberprüfungsakten ist stärker eingeschränkt, als die Landesverfassung es vorsieht.

Der Landesbeauftragte hatte zudem mit Unterstützung des Landesrechnungshofes angeregt, Personen, die vom Landtag in ein öffentliches Amts- oder Dienstverhältnis gewählt worden sind, als Geheimnisträger kraft Amtes zu qualifizieren. Sie sollten nur auf eigenen Antrag einer Sicherheitsüberprüfung unterzogen werden. Grundsätzliche Erwägungen lassen es als fragwürdig erscheinen, dass die Exekutive die Möglichkeit erhält, unabhängige Amtsträger zu überprüfen, nachdem das Parlament sie zur Kontrolle der Regierung gewählt hat. Der Gesetzgeber ist diesem Einwand jedoch nicht gefolgt.

Mit dem In-Kraft-Treten des Brandenburgischen Sicherheitsüberprüfungsgesetzes wird eine Lücke im Schutz sensibler Personaldaten geschlossen.

Allerdings schränkt das Gesetz das Akteneinsichtsrecht der Betroffenen und die Kontrollbefugnis des Landesbeauftragten in diesem Bereich stark ein.

4.3 Meldewesen

Enttäuschende Novellierung des Melderechts

Bereits in unserem letzten Tätigkeitsbericht haben wir über Pläne der Bundesregierung berichtet, mit einem Dritten Änderungsgesetz zum Melderechtsrahmengesetz (MRRG) das Melderecht an die modernen Informations- und Kommunikationstechnologien anzupassen[49]. Inzwischen hat die Bundesregierung einen entsprechenden Gesetzentwurf beschlossen, zu dem der Bundesrat Stellung genommen hat. Eine Beschlussfassung des Deutschen Bundestages steht derzeit noch aus.

Die bisher umfassendste Änderung des Melderechts hat einen eher enttäuschenden vorläufigen Abschluss gefunden. Ziel der Gesetzesänderung war es, das Melderecht im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen. Diese Absicht der Bundesregierung wurde von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt[50].

Erfreulicherweise hat die Bundesregierung davon Abstand genommen, eine gemeinsame Nutzung der Melderegister unterschiedlicher Meldebehörden zuzulassen. Auch sind die Meldebehörden nunmehr verpflichtet, sich gegen-

[49] s. Tätigkeitsbericht 2000, A 4.4.1

[50] s. Entschließung der 61. Konferenz, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.1

seitig über bestehende Auskunftssperren (vgl. § 32 a Brandenburgisches Meldegesetz – BbgMeldeG) zu unterrichten. Für die Erteilung von einfachen Melderegisterauskünften über das Internet wurde zumindest die datenschutzrechtliche Minimalforderung umgesetzt, dem Betroffenen ein Widerspruchsrecht einzuräumen.

Zahlreiche Forderungen der Datenschutzbeauftragten sind von der Bundesregierung jedoch nicht berücksichtigt worden. So wird die Meldepflicht deutscher Gäste in Hotels und Pensionen entgegen ursprünglichen Plänen nicht abgeschafft. Für die Übermittlung von Meldedaten über das Internet[51] innerhalb des öffentlichen Bereichs wird immer noch keine fortgeschrittene elektronische Signatur im Sinne des Signaturgesetzes verlangt. Im Gegensatz zu ersten Entwürfen wird die Nutzung des Melderegisters für politische Zwecke weiterhin nicht an die Einwilligung der Betroffenen gebunden (z. B. Parteienwerbung). Daher müssen auch in Zukunft Einwohnerinnen und Einwohner bei Wahlen und Abstimmungen der Übermittlung ihrer Meldedaten zu Zwecken der Wahlwerbung ausdrücklich widersprechen. Dies ist insofern besonders bedauerlich, als unsere praktische Erfahrung in der Zusammenarbeit mit den Meldebehörden des Landes gezeigt hat, dass seit der Neugestaltung der Meldescheine im Jahre 1999 die Zahl der Widersprüche bei Neuanmeldungen deutlich zunimmt, da im Gegensatz zur früheren Rechtslage der Meldeschein ein eigenes Feld zur Einlegung solcher Widersprüche vorsieht.

Die Erteilung einer erweiterten Melderegisterauskunft, bei der außer Namen und Anschrift noch eine Reihe weiterer Daten herausgegeben werden darf, ist weiterhin nur an das berechtigte Interesse des Antragstellers gebunden. Dies stellt keine wirksame Einschränkung der Melderegisterauskunft dar und berücksichtigt das Recht auf informationelle Selbstbestimmung nicht in angemessener Weise. Sachgerecht wäre es vielmehr gewesen, die Darlegung eines rechtlichen Interesses zu verlangen. Datenschutzrechtlich bedenklich ist zudem, dass der Entwurf kein Recht auf Einsicht in die in Akten gespeicherten personenbezogenen Daten vorsieht.

Die bevorstehende Novellierung des Melderechtsrahmengesetzes hat aus datenschutzrechtlicher Sicht das Ziel einer umfassenden Modernisierung des Melderechts verfehlt. Wir fordern die Landesregierung auf, alle bei einem Rahmengesetz möglichen Spielräume zu nutzen, um über das Melderechtsrahmengesetz hinaus datenschutzrechtliche Verbesserungen im Brandenburgischen Meldegesetz vorzusehen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht bietet dafür seine Unterstützung an.

[51] s. dazu oben A 1.5.2

4.4 Personaldaten

4.4.1 Öffentlicher Dienst auf dem Prüfstand – Organisationsuntersuchung durch eine Unternehmensberatung

Eine Unternehmensberatung wurde damit beauftragt, ein Gutachten über Optimierungspotentiale der brandenburgischen Straßenbauverwaltung anzufertigen. Im Zuge der Erstellung des Gutachtens sollten auch mittels Interviews und Fragebögen Personaldaten der Beschäftigten erhoben werden.

Bei einer externen Organisationsuntersuchung durch Private handelt es sich um eine Datenverarbeitung im Auftrag i. S. v. § 11 Brandenburgisches Datenschutzgesetz (BbgDSG). Dies setzt voraus, dass die Verantwortung für die Organisationsuntersuchung bei der auftraggebenden Stelle verbleibt und die Unternehmensberatung lediglich untergeordnete Hilfsaufgaben bei der Verarbeitung personenbezogener Daten durchführt. Sofern eine private Auftragnehmerin selbständig und eigenverantwortlich eine Organisationsuntersuchung vornehmen würde, handelte es sich nicht mehr um eine Datenverarbeitung im Auftrag, sondern um eine sog. Funktionsübertragung. Diese bedürfte neben einer besonderen gesetzlichen Ermächtigung aus datenschutzrechtlicher Sicht einer Befugnis zur Übermittlung personenbezogener Daten an eine private Auftragnehmerin. Gemäß § 29 Abs. 1 Satz 2 BbgDSG ist die Übermittlung von Personaldaten an Private nur unter sehr strengen Voraussetzungen zulässig. Es ist daher dringend davon abzuraten, private Unternehmen selbständig und eigenverantwortlich Organisationsuntersuchungen durchführen zu lassen.

Wird die Beauftragung nach den o. g. Grundsätzen als Datenverarbeitung im Auftrag organisiert, bestehen dagegen keine grundsätzlichen datenschutzrechtlichen Bedenken. Wichtig ist, dass die Anforderungen von § 11 BbgDSG eingehalten werden. Dazu gehören neben einer Reihe formaler Anforderungen, wie z. B. der Meldepflichten gegenüber den verschiedenen Aufsichtsbehörden, auch bestimmte inhaltliche Anforderungen. Insbesondere hat sich die Auftragnehmerin hinsichtlich der Verarbeitung personenbezogener Daten den Weisungen des Auftraggebers zu unterwerfen. Darüber hinaus muss schriftlich detailliert festgelegt werden, was genau Gegenstand und Umfang der Datenverarbeitung ist, welche technischen und organisatorischen Maßnahmen von der Auftragnehmerin zu treffen sind und ob und ggf. welche Unterauftragsverhältnisse zulässig sind.

Auch hier ist darauf zu achten, dass der Verarbeitung von Personaldaten enge Grenzen gesetzt sind. Da es in der Regel darum geht, Defizite in der Arbeits- und Verwaltungsorganisation aufzudecken, kommt es auf einen kon-

kreten Personenbezug zu einzelnen Bediensteten in den meisten Fällen nicht an. Sollte die Verarbeitung von Personaldaten in Einzelfällen notwendig sein, so ist bei der Auswertung dafür Sorge zu tragen, dass die Personaldaten so früh wie möglich so zusammengefasst werden und ein Personenbezug nicht mehr ohne Weiteres herstellbar ist. Ausgeschlossen ist die Nutzung der durch Organisationsuntersuchungen gewonnenen Personaldaten für Verhaltens- und Leistungskontrollen.

Die Stabsstelle für Verwaltungsmodernisierung hat bei der Beauftragung den datenschutzrechtlichen Fragen bedauerlicherweise zunächst keine große Bedeutung zugemessen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist über das Vorhaben erst auf Veranlassung des betroffenen Ministeriums für Stadtentwicklung, Wohnen und Verkehr informiert worden. Eine eingehende datenschutzrechtliche Bewertung des Vorhabens konnte u. a. schon deshalb bisher nicht vorgenommen werden, weil die Auftraggeberin – die Stabsstelle für Verwaltungsmodernisierung in der Staatskanzlei – keine ausreichenden Unterlagen vorgelegt hat.

Bei der Beauftragung nicht öffentlicher Stellen mit Organisationsuntersuchungen handelt es sich um eine Datenverarbeitung im Auftrag. Es ist darauf zu achten, dass personenbezogene Daten der Bediensteten nur verarbeitet werden, wenn dies zur Durchführung des Auftrages unerlässlich ist. Von einer Funktionsübertragung im Sinne einer selbständigen und eigenverantwortlichen Durchführung von Organisationsuntersuchungen durch Private ist mangels Rechtsgrundlage Abstand zu nehmen.

4.4.2 Leistung zählt – Prämien, Zulagen und leistungsabhängiger Aufstieg im öffentlichen Dienst

Um den Beamtinnen und Beamten des Landes Brandenburg eine leistungsgerechtere Besoldung zu gewähren, hat die Landesregierung nach bundesrechtlichen Vorgaben zwei Verordnungen verabschiedet, mit denen leistungsbezogene Elemente eingeführt werden. Bei der Erarbeitung von Durchführungshinweisen durch das Ministerium der Finanzen wurden wir einbezogen.

In beiden Verordnungen ist geregelt, dass nur 10% der Beamten der Besoldungsordnung A unter bestimmten weiteren formellen Voraussetzungen begünstigt werden können. Da überwiegend der Dienstvorgesetzte über die Gewährung von leistungsbezogenen Bezügebestandteilen zu entscheiden hat, benötigt dieser zur Feststellung der formellen Voraussetzungen eine Reihe von Personaldaten, die regelmäßig nur der Zentralen Bezügestelle des Landes Brandenburg (ZBB) zur Verfügung stehen. Es ist daher vorgesehen, dass die ZBB den obersten Landesbehörden jeweils umfangreiche Listen zur

Verfügung stellt, die eine Reihe von personenbezogenen Daten, wie z. B. Name, Vorname, Personalnummer, Besoldungsgruppe oder Lebensaltersstufe, enthalten. Diese Daten können nach § 29 Abs. 1 Satz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) im Rahmen des § 61 Landesbeamtengesetz (LBG) an die Ministerien übermittelt werden, da sie für deren Entscheidung erforderlich sind.

Das Ministerium der Finanzen hat unsere Vorschläge vollständig umgesetzt. So sind die Listen den jeweils zuständigen Personalreferaten als vertrauliche Personalsache zuzusenden. Außerdem haben die Personalreferate die Liste nach den jeweiligen Vergabebereichen aufzuteilen und die so entstandenen Teillisten nur den Vergabeberechtigten als vertrauliche Personalsache zu übergeben. Schließlich war eine Vorgabe zur Vernichtung der Listen aufzunehmen. Sie sind spätestens mit Ablauf des jeweils laufenden Jahres zu löschen, da zum 1. Januar des Folgejahres den obersten Landesbehörden neue Listen zugehen.

Das Ministerium der Finanzen hat bei seinen Durchführungshinweisen zur Vergabe von leistungsbezogenen Bezügebestandteilen die besonderen Anforderungen des Personaldatenschutzes berücksichtigt.

4.4.3 Führung von Personalakten mit Folgen

Anlässlich der Beschwerde einer Beamtin haben wir bei einer Landesbehörde deren Personalakte aus datenschutzrechtlicher Sicht geprüft und dabei zahlreiche, z. T. erhebliche Mängel festgestellt.

Wie in diesem konkreten Fall haben Personalakten häufig kein Inhaltsverzeichnis und sind entweder gar nicht oder nur lückenhaft paginiert. In einem Inhaltsverzeichnis sind insbesondere alle vorhandenen Teil- und Nebenakten aufzuführen, um jederzeit Vollständigkeit und Inhalt der Personalakte gerade in Streitfällen dokumentieren zu können. Dem gleichen Zweck dient die Paginierung der Personalakte. Dabei sollten die jeweiligen Teile der Personalakte (beispielsweise Bewerbungsunterlagen, eigentliche Grundakte, Krankmeldungen, Disziplinarvorgänge usw.) jeweils getrennt paginiert werden, um unterschiedliche Löschungsfristen ohne Änderung der Paginierung berücksichtigen zu können.

Gemäß § 60 Landesbeamtengesetz (LBG) besteht ein uneingeschränktes Recht, in die Personalakte einzusehen. Weder bedarf die Einsicht in die Personalakte einer Genehmigung noch ist die Häufigkeit der Inanspruchnahme dieses Rechts beschränkt. Deshalb ist es nicht erforderlich und damit unzulässig, einen Vermerk oder ein Protokoll über eine durchgeführte Einsicht an-

zufertigen und zur Personalakte zu nehmen. Anderenfalls könnte der Eindruck vermittelt werden, der Bedienstete sei ein Querulant.

In der von uns geprüften Personalakte befanden sich aber auch zahlreiche Dokumente, die für die betreffende Beamtin sehr nachteilig waren, ohne dass sich feststellen ließ, ob sie diese Dokumente zur Kenntnis erhalten hat. Andererseits enthielt die Personalakte Äußerungen der Beamtin zu derartigen Dokumenten, die jedoch selbst in der Akte nicht zu finden waren. Vor diesem Hintergrund weisen wir darauf hin, dass Beamte nach § 59 Satz 1 LBG zu Beschwerden, Behauptungen und Bewertungen mit nachteiligem Charakter zu hören sind, bevor diese in die Personalakte aufgenommen werden. Die Tatsache der Anhörung ist zu protokollieren. Unprotokollierte Dokumente müssen aus der Personalakte entfernt werden. Ebenso ist es selbstverständlich, dass Gegenäußerungen von Beamten nur dann gem. § 59 Satz 2 LBG zur Personalakte zu nehmen sind, wenn das damit in untrennbarem Zusammenhang stehende Dokument zulässigerweise dort abgelegt wurde.

Bevor beispielsweise Schriftverkehr mit einer Rechtsvertretung in die Personalakte aufgenommen wird, ist eingehend zu prüfen, ob dieser in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis i. S. v. § 57 Abs. 1 Satz 2 LBG steht. Falls dies nicht der Fall ist, ist eine gesonderte Sachakte zu führen. Weder die Erklärung zur Kostenübernahme noch Informationen über die Gewerkschaftszugehörigkeit gehören in die Personalakte.

Die betreffende Landesbehörde hat unsere Hinweise umgesetzt.

Angesichts zahlreicher Unsicherheiten beim Führen von Personalakten halten wir es nach wie vor dringend für erforderlich, dass das Ministerium des Innern eine einheitliche Verwaltungsvorschrift hierzu erlässt, um eine möglichst einheitliche datenschutzgerechte Personalaktenführung in der Verwaltung sicherzustellen.

4.4.4 Einsicht in Personalakten auch durch kommunale Rechnungsprüfer

Bisher haben wir die Auffassung vertreten, dass dem Landesrechnungshof (LRH) ein Recht zur Einsichtnahme in Personalakten zustehe, während Prüfer kommunaler Rechnungsprüfungsämter dazu nicht befugt seien. Aufgrund einer Anfrage des Rechnungsprüfungsamtes einer kreisfreien Stadt haben wir unseren Standpunkt überprüft.

Ebenso wie für den LRH gelten auch für die Tätigkeit des Rechnungsprüfungsamtes die Bestimmungen des Datenschutzrechts. Das bedeutet, dass das Rechnungsprüfungsamt nur dann personenbezogene Daten für seine

Tätigkeit erheben und weiterverarbeiten darf, wenn deren Kenntnis für die Erfüllung seiner Aufgaben nach §§ 113, 114 Gemeindeordnung (GO) erforderlich ist. Danach hat ein Rechnungsprüfungsamt u. a. die Aufgaben, Kassenvorgänge und Belege oder die Jahresrechnung der Kommune zu prüfen. Dabei hat es gem. §§ 12 ff. Brandenburgisches Datenschutzgesetz (BbgDSG) die Befugnis, personenbezogene Daten zu verarbeiten.

Nach der Gemeindeordnung ist das Rechnungsprüfungsamt bei der sachlichen Beurteilung der Prüfungsvorgänge unabhängig und an Weisungen nicht gebunden. Um diese Unabhängigkeit nicht zu gefährden und keinen Einfluss auf die Prüftätigkeit des Rechnungsprüfungsamtes zuzulassen, bestimmt es selbst, welche personenbezogenen Daten es zur Erfüllung seiner Aufgaben benötigt. Dies kann die Verwaltung oder die Gemeindevertretung grundsätzlich weder verweigern noch auf seine Berechtigung überprüfen.

Das Recht des Rechnungsprüfungsamtes, sich alle Unterlagen vorlegen zu lassen, bezieht sich auch auf Personalakten. Dem steht auch das Landesbeamtengesetz nicht entgegen. Entscheidend ist, dass die Rechnungsprüfung im Datenschutzrecht privilegiert wird. § 13 Abs. 3 BbgDSG legt fest, dass rechtmäßig erhobene personenbezogene Daten immer auch zum Zwecke der Rechnungsprüfung verarbeitet werden dürfen, ohne dass damit eine Änderung der Zweckbestimmung dieser Daten verbunden ist. Zwischen der Rechnungsprüfung durch den Landesrechnungshof und der durch ein kommunales Rechnungsprüfungsamt besteht datenschutzrechtlich kein Unterschied. Aus § 13 Abs. 3 BbgDSG folgt, dass die Rechnungsprüfung Bestandteil der personalwirtschaftlichen Aufgaben des Dienstherrn oder Arbeitgebers ist. Die Befugnis des Rechnungsprüfungsamtes, Einsicht in Personalakten zu nehmen, ergibt sich deshalb aus der gleichen Vorschrift, nach der das Personalamt selbst die Personalakten bearbeiten darf (§ 57 LBG). Eine Einwilligung des Bediensteten ist nicht erforderlich, da das Rechnungsprüfungsamt kein Dritter ist.

Nehmen Prüfer des Rechnungsprüfungsamtes Einsicht in Personalunterlagen, müssen sie sich strikt auf den erforderlichen Umfang beschränken und in jedem Einzelfall sorgfältig prüfen, ob der konkrete Personenbezug zur Erfüllung des Prüfauftrags unabdingbar ist. Von der Einsichtnahme dürfen nur zahlungsrelevante Unterlagen umfasst sein. Dies betrifft insbesondere die geführten Besoldungs- und Vergütungsunterlagen einschließlich der bezügerelevanten Nachweise z. B. über Kinder oder die Beschäftigungsverhältnisse der Ehegatten. Die Einsichtsrechte des Rechnungsprüfungsamtes können sich sogar auf Bewerbungsunterlagen und Zeugnisse erstrecken.

Das Amt sollte grundsätzlich nicht in vertrauliche Unterlagen einsehen, die in der Regel für Zahlungen nicht relevant sind. Dazu gehören z. B. Disziplinar-

sachen, Beurteilungen, Gesundheitszeugnisse oder Mitteilungen der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR. Dies gilt insbesondere dann, wenn diese Unterlagen entweder als Teilakte geführt oder zumindest getrennt gegliedert werden

Prüfer kommunaler Rechnungsprüfungsämter haben ebenso wie solche des Landesrechnungshofes ein Recht auf Einsicht in Personalakten. Sie sind dabei verpflichtet, die Kenntnisnahme personenbezogener Daten auf das für die Prüfung unabdingbare Maß zu beschränken.

4.4.5 Darf der behördliche Datenschutzbeauftragte den Personalrat kontrollieren?

Ein behördlicher Datenschutzbeauftragter hat die Verarbeitung personenbezogener Daten des Personalrats kontrolliert. Ihm wurde vorgeworfen, von seinen Kontrollbefugnissen nicht in der gebotenen, unabhängigen Weise Gebrauch gemacht zu haben. Dies begründete der Personalrat damit, dass der Datenschutzbeauftragte sich vor allem für Mitarbeiterbeschwerden über den Amtsleiter interessiert hatte. Der Personalrat befürchtete, in Zukunft keine vertrauliche Beratung und Unterstützung der Beschäftigten mehr leisten zu können.

Sowohl der Personalrat als auch der behördliche Datenschutzbeauftragte haben ihre Aufgaben unabhängig von den Weisungen der Dienststelle zu erfüllen. Die Unabhängigkeit des Personalrats bedeutet nicht, dass dieser beliebig personenbezogene Daten der Beschäftigten verarbeiten darf.

Das Bundesarbeitsgericht hat entschieden[52], dass sich die Kontrollbefugnisse eines betrieblichen Datenschutzbeauftragten nicht auf die Unterlagen des Betriebsrates erstrecken, es sei denn, dass es dazu eine ausdrückliche Regelung gäbe. Das Bundesdatenschutzgesetz enthält insoweit eine Lücke. Brandenburg hat dagegen in § 94 Abs. 1 Personalvertretungsgesetz (PersVG) auch den Personalrat unter die „uneingeschränkte“ Kontrolle des behördlichen Datenschutzbeauftragten gestellt. Dieser ist zu besonderer Verschwiegenheit verpflichtet und muss nach § 7 a Brandenburgisches Datenschutzgesetz (BbgDSG) die ihm bekannt werdenden personenbezogenen Daten auch gegenüber der Leitung der Dienststelle vertraulich behandeln. Der Personalrat wiederum hat ein Mitbestimmungsrecht bei der Bestellung und Abberufung des behördlichen Datenschutzbeauftragten (§ 66 Nr. 6 PersVG). Damit hat Brandenburg schon früh ein Konzept der internen Datenschutzkontrolle verwirklicht, wie es jetzt im Zuge der Modernisierung des Datenschutzrechts für die öffentliche Verwaltung insgesamt und für die Privatwirtschaft vorge-

[52] s. Beschluss v. 11.11.1997, Recht der Datenverarbeitung 1998, S. 64

schlagen worden ist[53]. Dennoch können auch hier Interessenkollisionen zwischen dem Personalrat als Arbeitnehmervertretung und dem behördlichen Datenschutzbeauftragten als unabhängige, aber doch der Leitung nahe stehende Stelle auftreten. Aufgabe des Personalrates ist in erster Linie, die Interessen der Arbeitnehmer zu vertreten, während der behördliche Datenschutzbeauftragte auch die Arbeitnehmervertretung zu kontrollieren hat. Eine Auflösung dieses Interessenkonflikts wird angesichts der unterschiedlichen rechtlichen Grundlagen nicht dahingehend möglich sein, dass einer der beiden Funktionen stets der Vorrang einzuräumen ist. Im Konfliktfall sollte daher von der in § 94 Abs. 2 PersVG vorgesehenen Anrufung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht durch den Personalrat Gebrauch gemacht werden. Die Kontrollrechte des Landesbeauftragten sind unbestritten und umfassen die gesamte Dienststelle einschließlich des Personalrats. Aufgrund seiner besonderen Stellung besteht keine Gefahr einer Interessenkollision.

Auch die Datenverarbeitung des Personalrats ist den Vorschriften des Brandenburgischen Datenschutzgesetzes unterworfen. Der Personalrat hat ein Mitbestimmungsrecht bei der Bestellung des behördlichen Datenschutzbeauftragten. Bei unauflösbaren Konflikten zwischen Personalrat und behördlichem Datenschutzbeauftragten sollte der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht eingeschaltet werden.

4.4.6 Das Personalinformationssystem PERIS und die Stellenbörse

Die Koordinierungsstelle für Personalmanagement der Landesregierung (KPM) hat eine Stellenbörse eingerichtet. Dieser sind Stellen von Landesbediensteten zu melden, die in Folge der Verwaltungsmodernisierung künftig wegfallen. Auch können sich dort Beschäftigte melden, die eine berufliche Veränderung im eigenen Interesse anstreben. Ziel ist die Weitervermittlung der Betroffenen innerhalb der Landesverwaltung. Welche datenschutzrechtlichen Anforderungen hat die Stellenbörse zu beachten?

Zur Datenverarbeitung nutzt die KPM das automatisierte Personalinformationssystem PERIS, das bereits in anderen Bereichen der Landesverwaltung im Einsatz ist. Allerdings wurde das bisherige Verfahren zur Nutzung von PERIS durch die KPM modifiziert. Es handelt sich um eine ressortübergreifende Personaldatenverarbeitung, die in dieser Form rechtlich nicht geregelt ist. Aufgrund dieser Änderungen haben wir empfohlen, ein Sicherheitskonzept für den Einsatz von PERIS bei der Stellenbörse zu entwickeln. Dabei ist zu berücksichtigen, dass der PERIS-Server entweder in einem speziell gesi-

[53] Roßnagel/Pfitzmann/Garstka, Gutachten zur Modernisierung des Datenschutzrechts, S. 203

cherten Raum der KPM oder des Landesbetriebs für Datenverarbeitung und Statistik (LDS) unterzubringen ist. Im letzten Fall ist die Übertragung der Daten mit starken kryptographischen Verfahren komplett zu verschlüsseln, um sie gegen so genannte Man-in-the-Middle-Attacken zu schützen. Mit dieser Methode hatte die Stiftung Warentest die nur teilweise verschlüsselte elektronische Steuererklärung (ELSTER) erfolgreich angegriffen[54].

Die Beantwortung eines Fragebogens durch die Beschäftigten sowie die Verarbeitung ihrer Daten durch die Stellenbörse kann nur auf freiwilliger Basis erfolgen. Der Erhebungsbogen „Personalprofil für die Vermittlung durch die Koordinierungsstelle für Personalmanagement“ berücksichtigt dies, indem das Einverständnis durch Unterschrift ausdrücklich zu erklären ist.

Die KPM hat bereits eine sinnvolle Muster-Dienstvereinbarung über den Einsatz von PERIS in der Stellenbörse entwickelt. Dadurch wird die ressortübergreifende Datenverarbeitung transparent gestaltet. Möglichen Befürchtungen der Beschäftigten, es würden sämtliche in der Landesverwaltung vorhandenen Personaldaten zusammengeführt, kann durch die Muster-Dienstvereinbarung ebenfalls wirksam begegnet werden.

Die Verarbeitung von Personaldaten durch die Stellenbörse kann ausschließlich auf freiwilliger Basis erfolgen. Der Einsatz des Personalinformationssystems PERIS sollte durch ein spezielles Sicherheitskonzept begleitet werden.

4.5 Statistik: Kontrollen bei örtlichen Erhebungsstellen für die Agrarstatistik

Bei Kontrollen in einigen Erhebungsstellen für die Agrarstatistik hatten wir insbesondere zu prüfen, ob diese in datenschutzgerechter Weise von der übrigen Verwaltung abgeschottet sind.

Örtliche Erhebungsstellen sind nach § 12 Abs. 2 Brandenburgisches Statistikgesetz für die Dauer der Bearbeitung von statistischen personenbezogenen Einzelangaben räumlich, organisatorisch und personell von anderen Stellen der Verwaltung zu trennen.

Eine Erhebungsstelle für die Agrarstatistik muss sowohl für die Verwaltung als auch für die auskunftspflichtigen Landwirte deutlich als Statistikstelle erkennbar sein. Dazu ist eine eindeutige Kennzeichnung der Räume erforderlich.

[54] s. Tätigkeitsbericht 2000, A 12.3; Die von der Stiftung Warentest festgestellte Sicherheitslücke wurde zwischenzeitlich geschlossen.

Sofern PC zur Datenerfassung genutzt werden, sind diese vom Behördennetz unbedingt zu trennen. Dem trugen die kontrollierten Stellen durch die Nutzung von Einzelplatz-PC ausreichend Rechnung. Für die sichere Aufbewahrung sensibler Unterlagen fehlte jedoch in einigen Stellen ein geeigneter Stahlschrank oder Datensafe.

Nur in wenigen Fällen wurden die Beschäftigten der Erhebungsstellen schriftlich zur Wahrung des Statistikgeheimnisses verpflichtet, wie dies nach § 3 Abs. 2 der Verordnung über die Durchführung des Agrarstatistikgesetzes (AgrStatG-DVO) notwendig ist. Die Abschottung von den übrigen Teilen der Verwaltung sollte auch durch eine Dienstanweisung geregelt werden.

Nach § 3 Abs. 2 AgrStatG-DVO dürfen die in den Erhebungsstellen Beschäftigten ihre Kenntnisse über auskunftspflichtige Landwirte nicht für andere Zwecke verwenden. Nähme ein solcher Beschäftigter beispielsweise nach Abschluss der Agrarstatistik-Erhebung gleichzeitig Aufgaben der EU-Agrarförderung wahr, wäre es praktisch unmöglich, von ihm zu fordern, sein Wissen aus der Statistik dabei auszublenden. Statistikbeschäftigte sollten also keine Aufgaben wahrnehmen, die eine Nähe zur Agrarstatistik aufweisen.

Statistische Erhebungen dienen der Vorratshaltung von Daten, die in der übrigen Verwaltung unzulässig ist. Daher sind Erhebungsstellen für die Agrarstatistik räumlich, organisatorisch und personell von anderen Stellen der Verwaltung zu trennen.

4.6 Kommunalrecht

4.6.1 Fernsehübertragung aus dem Kommunalparlament

Ein Journalist des städtischen Fernsehsenders postierte sich während einer Sitzung der Stadtverordnetenversammlung mit seiner Kamera in unmittelbarer Nähe einzelner Stadtverordneter. Dadurch wurden während einer emotional geführten Debatte abfällige leise Bemerkungen von einzelnen Abgeordneten über anwesende Bürger aufgezeichnet und an die Öffentlichkeit gebracht. Der Vorsitzende der Stadtverordnetenversammlung bat uns, allgemein zum Umgang mit Medien bei den Sitzungen der Stadtverordnetenversammlung aus datenschutzrechtlicher Sicht Stellung zu nehmen.

In der § 49 Abs. 2 Gemeindeordnung (GO) ist geregelt, dass die Sitzungen kommunaler Vertretungen auf Tonband aufgezeichnet werden können, um die Niederschrift zu erstellen. Voraussetzung dafür ist, dass alle Mitglieder der Gemeindevertretung vor der Sitzung zugestimmt haben. Die Aufzeichnungen müssen nach der darauffolgenden Sitzung gelöscht werden.

Die gleiche Vorschrift lässt auch Ton- und Bildaufzeichnungen öffentlicher Sitzungen durch die Presse und das Fernsehen zu. Dabei bedarf es ebenso der vorherigen Zustimmung aller Abgeordneten; eine Pflicht, die Aufnahmen zu löschen, besteht jedoch nicht.

Tonband- und Fernsehaufzeichnungen durch Journalisten sind während der Sitzungen kommunaler Vertretungskörperschaften nur mit Einwilligung aller Abgeordneten zulässig.

4.6.2 Korruptionsbekämpfung im rechtsfreien Raum?

Eine Stadtverordnetenversammlung beabsichtigte, einen ehrenamtlichen Anti-Korruptionsbeauftragten einzusetzen. Dieser sollte Bediensteter der Stadtverwaltung sein sowie die Bürgerinnen und Bürger bei der Vorbeugung und Bekämpfung von Korruption beraten. Für ihn waren dabei umfassende Rechte vorgesehen.

Ein Anti-Korruptionsbeauftragter kann nicht durch bloßen Beschluss der Gemeindevertretung (bzw. der Stadtverordnetenversammlung) bestellt werden. Nach § 25 Abs. 4 Gemeindeordnung (GO) muss dies sowie seine konkreten Rechte und Pflichten in der Hauptsatzung vorgesehen werden. Insbesondere sollte in der Hauptsatzung geregelt werden, ob der Anti-Korruptionsbeauftragte befugt werden soll, an nicht öffentlichen Sitzungen teilzunehmen, denn dieses Recht steht ihm nicht ohne Weiteres zu. Zudem ist er in der Regel darauf angewiesen, u. U. auch personenbezogene Informationen zu erheben und weiter zu verarbeiten. Dabei müssen selbstverständlich die datenschutzrechtlichen Bestimmungen beachtet werden. Es ist nicht zulässig, dass der Anti-Korruptionsbeauftragte ohne Zustimmung des betroffenen Beschäftigten Einsicht in dessen Personalakten nimmt.

Die Korruptionsbekämpfung sollte sich nicht allein auf die Bestellung von Anti-Korruptionsbeauftragten beschränken. Der vorliegende Fall macht deutlich, wie wichtig das seit 1998 in Brandenburg geltende Jedermannsrecht auf Akteneinsicht im Hinblick darauf ist, die Rechtmäßigkeit der Verwaltung zu prüfen bzw. diese zu rechtmäßigem Verwaltungshandeln anzuhalten. Aus unserer Sicht ist eine transparente Verwaltung erheblich weniger anfällig gegenüber Korruptionspraktiken als eine Verwaltung, die das Recht auf Informationszugang nicht in ausreichender Weise umsetzt.

Beabsichtigt eine Kommune einen Anti-Korruptionsbeauftragten einzusetzen, so müssen dessen Befugnisse sich im Rahmen der datenschutzrechtlichen Bestimmungen, vor allem der Vorschriften des Personaldatenschutzes, bewegen und in der Hauptsatzung festgelegt werden. Eine transparente Verwaltung ist die beste Korruptionsprävention.

4.7 Sonstiges/Verwaltungsrecht

4.7.1 Grundstückseigentümer im Internet

Seit einigen Jahren wird das Liegenschaftskataster weitgehend in elektronischer Form geführt. In dieser Form stehen einerseits das automatisierte Liegenschaftsbuch (ALB) sowie andererseits die automatisierte Liegenschaftskarte (ALK) zur Verfügung, auf die jetzt der zentrale, landesweite Zugriff eingerichtet werden soll.

Der Landesbetrieb „Landesvermessung und Geobasisinformation Brandenburg“ (LGB) sowie das Ministerium des Innern haben zu diesem Zweck das Verfahren ALBonline entwickelt, mit dem bestimmte institutionelle Nutzer des Liegenschaftskatasters die Möglichkeit erhalten sollen, auf die im ALB gespeicherten Daten über das Internet zugreifen zu können. Dabei ist nicht vorgesehen, das ALB für die Allgemeinheit zu öffnen und in das Internet einzustellen. Dies wäre nach dem Vermessungs- und Liegenschaftsgesetz (VermLiegG) auch nicht zulässig, da die im ALB gespeicherten personenbezogenen Eigentümerdaten nur bei einem berechtigten Interesse herausgegeben werden dürfen. Der Landesbetrieb beabsichtigt daher, nur denjenigen Nutzern einen Zugriff auf das ALB zu eröffnen, die gesetzlich befugt sind, das ALB automatisiert abzurufen. Dazu gehören beispielsweise die öffentlich bestellten Vermessungsingenieure, Notare, aber auch die Ämter und Gemeinden des Landes.

Nach § 2 Liegenschaftskataster-Datenübermittlungsverordnung (LiKaDÜV) i. V. m. § 10 des Brandenburgischen Datenschutzgesetzes (BbgDSG) sind eine Reihe von technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen. Der Landesbetrieb hat zu diesem Zweck eine Rechnerarchitektur entwickelt, die die angemessenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik im Wesentlichen berücksichtigt. Die bei den Kataster- und Vermessungsämtern gespeicherten ALB-Daten werden täglich über das Landesverwaltungsnetz und eine Firewall auf einen Datenbankserver im Landesbetrieb überspielt, wodurch die Aktualität des Liegenschaftsbuches gewährleistet wird.

Der Nutzer von ALBonline muss zunächst schriftlich die Zulassung zum Online-Verfahren beantragen. Mit Bewilligung des Antrages wird ihm eine Nut-

zerkennung sowie ein Passwort zugeteilt. Der Zugang zum Webserver des Landesbetriebes ist nur über eine Firewall möglich. Die Daten einschließlich Nutzerkennung und Passwort werden mit dem Verfahren 3DES und einer Schlüssellänge von 156 Bit verschlüsselt. Webserver und Datenbankserver sind gegen unbefugte Zugriffe noch einmal besonders gesichert. Die Kommunikation erfolgt ausschließlich in HTML über das Protokoll http. Aktive Inhalte (Java-Applets, ActiveX) werden nicht verwendet. Die Nutzerführung erfolgt über temporäre Cookies, die nach Ende der Sitzung gelöscht werden. Es erfolgt ein lesender Zugriff auf die Datenbank des ALB, deren Veränderung ist nicht möglich.

Zur Zeit werden zwischen dem Landesbetrieb und dem LDA Brandenburg noch einige Detailfragen geklärt, damit ALBonline seinen Echtbetrieb aufnehmen kann. Die Zusammenarbeit mit dem Ministerium des Innern sowie dem Landesbetrieb in dieser Angelegenheit war sehr konstruktiv.

Das vom Landesbetrieb eingeführte Verfahren ALBonline, mit dem autorisierte Nutzer auf Liegenschaftsdaten über das Internet zugreifen können, genügt den Datenschutzanforderungen sowohl aus rechtlicher als auch aus technischer und organisatorischer Sicht.

4.7.2 Wie war im Amt es doch vordem mit Formularen so bequem!

Ein Notar sandte uns einen „Fragebogen für bebaute Grundstücke“, den die Partei eines Grundstückskaufvertrages vom Gutachterausschuss für Grundstückswerte eines Landkreises mit der Bitte um Beantwortung erhalten hatte. Das Anschreiben des Ausschusses enthielt lediglich einen Hinweis darauf, dass die erbetenen Daten auf Grund einer gesetzlichen Verpflichtung vertraulich behandelt würden. Der Notar hatte Zweifel an der Rechtmäßigkeit dieses Vorgehens.

Die Zweifel waren berechtigt. Notare und andere beurkundende Stellen sind zwar nach dem Baugesetzbuch (§ 195 Abs. 1) verpflichtet, den Gutachterausschüssen Abschriften der beurkundeten Grundstückskaufverträge zur Führung der Kaufpreissammlung zu übersenden. Die Kaufpreissammlung dient zur Ermittlung durchschnittlicher Grundstückswerte. Darüber hinaus räumt das Baugesetzbuch den Gutachterausschüssen das Recht ein, den Parteien des Kaufvertrages zusätzliche Fragen zu stellen, soweit der Kaufvertrag im Einzelfall hierfür nicht ausreicht. Die Gutachterausschüsse haben zwei Möglichkeiten, von dieser gesetzlichen Befugnis Gebrauch zu machen: Entweder sie schicken immer dann, wenn sie einen Kaufvertrag erhalten, einheitliche Fragebögen zur Erhebung zusätzlicher Informationen für die Wertermittlung des betreffenden Grundstücks an die Vertragsparteien, wobei sie ausdrücklich auf die Freiwilligkeit der Erhebung hinweisen, da der Fragebo-

gen auch in den Fällen versandt wird, in denen sich alle erforderlichen Informationen bereits dem Kaufvertrag entnehmen lassen; oder der Ausschuss stellt nur in den Einzelfällen ergänzende Fragen (was auch in formularmäßiger Form möglich ist), in denen der Kaufvertrag geprüft worden ist und zusätzliche Informationen zur Wertermittlung benötigt werden. Eine pauschale Befragung der Parteien von Grundstückskaufverträgen ohne Hinweis auf die Rechtsgrundlage (falls im Einzelfall eine Pflicht zur Beantwortung besteht) oder auf die Freiwilligkeit ist dagegen unzulässig. Der Gutachterausschuss, den wir hierauf hingewiesen und dem wir eine konkrete Formulierung zur Ergänzung seines Fragebogenformulars vorgeschlagen hatten, änderte sein Formular und übernahm unseren Vorschlag.

Demgegenüber vertritt das Ministerium des Innern als Rechtsaufsichtsbehörde die Auffassung, dass das ursprüngliche Formular (ohne Hinweis auf die Freiwilligkeit der Beantwortung) rechtmäßig gewesen sei. Es hat die Gutachterausschüsse für Grundstückswerte des Landes aufgefordert, zu der bisherigen Praxis zurückzukehren.

Das widerspricht jedoch dem bei der Durchführung des Baugesetzbuches anzuwendenden Brandenburgischen Datenschutzgesetz. Dieses sieht in § 12 vor, dass bei der Erhebung personenbezogener Daten auf Grund einer Rechtsvorschrift, also mit Auskunftspflicht, auf die zugrunde liegende Rechtsvorschrift hingewiesen werden muss. Falls es sich um freiwillige Angaben handelt, ist auf die Freiwilligkeit hinzuweisen. Im Übrigen verkennt das Innenministerium aber auch die gestufte Informationserhebung, wie sie bei der Führung der Kaufpreissammlung vorgeschrieben ist. In erster Linie werden die Abschriften der Grundstückskaufverträge zur Wertermittlung herangezogen; zu ihrer Vorlage sind die beurkundenden Stellen in jedem Fall verpflichtet. Ergänzende Informationen kann der Gutachterausschuss nur im Einzelfall erheben und die dann bestehende Auskunftspflicht auch zwangsweise durchsetzen, wenn der Kaufvertrag nicht alle erforderlichen Informationen enthält. Das Innenministerium, das wir auf diese Rechtslage hingewiesen haben, hat hierauf nicht reagiert und uns auch trotz unserer entsprechenden Bitte einen angekündigten geänderten Hinweis auf die Rechtsgrundlage im Fragebogen nicht zugänglich gemacht.

Die Gutachterausschüsse für Grundstückswerte können die Parteien von Grundstückskaufverträgen generell auf freiwilliger Basis um die Beantwortung ergänzender Fragen zur Bewertung des Grundstücks auf einem Fragebogen bitten, wobei sie auf die Freiwilligkeit der Datenerhebung hinweisen müssen. Eine Pflicht zur Beantwortung ergänzender Fragen besteht nur dann, wenn der Kaufvertrag im Einzelfall zur Wertermittlung nicht ausreicht. Eine pauschale Versendung von Fragebögen ohne Hinweis auf die Freiwilligkeit oder die Rechtsgrundlage für eine Auskunftspflicht im Einzelfall ist zu beanstanden.

4.7.3 Datenschutz auch nach dem Tod – neues Bestattungsrecht

Bis zum Ende des Jahres 2001 galt im Land Brandenburg auf dem Gebiet des Leichen-, Bestattungs- und Friedhofswesens das Recht der ehemaligen DDR fort. Durch das Brandenburgische Bestattungsgesetz[55] wird dieses Rechtsgebiet neu geregelt.

Die Regelungen zum Umgang mit Toten- und Sektionsscheinen sind aus datenschutzrechtlicher Sicht insgesamt zufriedenstellend. Die Scheine werden grundsätzlich 30 Jahre bei dem für den Sterbeort zuständigen Gesundheitsamt aufbewahrt. Die Möglichkeit, in diese Scheine Einsicht zu nehmen oder in Kopie zu erhalten, besteht nunmehr dann, wenn der Antragsteller ein berechtigtes Interesse glaubhaft machen kann und schutzwürdige Belange des Verstorbenen oder seiner Angehörigen nicht beeinträchtigt werden. Ebenso räumt das Gesetz die Möglichkeit ein, die Angaben auf den Toten- und Sektionsscheinen für wissenschaftliche Forschungsvorhaben zu nutzen. Bestimmte Einzelheiten zum Umgang mit diesen Scheinen müssen in einer Rechtsverordnung geregelt werden, die das zuständige Ministerium für Arbeit, Soziales, Gesundheit und Frauen zeitnah erlassen sollte.

Der Entwurf des Ministeriums des Innern für eine Bestattungsdatenschutzverordnung sieht darüber hinaus eine konkrete Regelung zum Umgang mit personenbezogenen Daten durch Träger von Bestattungseinrichtungen wie Friedhöfen oder Krematorien vor. Daten Verstorbener werden mit personenbezogenen Daten lebender Personen gleichgestellt. Das Bestattungsrecht unterscheidet nicht danach, ob es sich um staatliche, kirchliche oder private Träger von Bestattungseinrichtungen handelt. Der Entwurf der Bestattungsdatenschutzverordnung beschränkt die zulässige Verarbeitung von personenbezogenen Daten durch Träger von Bestattungseinrichtungen auf einen Katalog bestimmter, ausdrücklich im Entwurf genannter erforderlicher Daten. Dabei wird in sachgerechter Weise nach den Daten Verstorbener, bestat-

[55] Gesetz über das Leichen-, Bestattungs- und Friedhofswesen im Land Brandenburg (BbgBestG) v. 10.11.2001, GVBl. I. S. 226

tungspflichtiger Personen, gewerblich Tätiger und sonstiger Nutzer unterschieden. Die in den Entwurf aufgenommene Vorschrift zur Berichtigung, Löschung und Sperrung von Daten bietet einen angemessenen Ausgleich zwischen den Persönlichkeitsrechten der Betroffenen einerseits und den wissenschaftlichen, historischen aber auch berechtigten persönlichen Interessen vor allem an den Daten verstorbener Personen.

Mit dem neuen Brandenburgischen Bestattungsgesetz wurden in Brandenburg auch klare Vorgaben zum Umgang mit personenbezogenen Daten Verstorbener und ihrer Angehöriger auf gesetzlicher Ebene geschaffen. Diese sollten möglichst bald durch die notwendigen Rechtsverordnungen ergänzt werden.

5 Justiz und Europaangelegenheiten

5.1 EUROJUST – die zukünftige europäische Staatsanwaltschaft

Der Europäische Rat hat 1999 beschlossen, eine staatsanwaltschaftliche Zentralstelle mit dem Namen EUROJUST einzurichten, die vor allem der Bekämpfung der schweren organisierten Kriminalität dienen soll, indem sie die Koordinierung der nationalen Staatsanwaltschaften erleichtert und die Erledigung von Rechtshilfeersuchen vereinfacht. Seit dem 1. März 2001 hat eine vorläufige Stelle zur Zusammenarbeit unter der Bezeichnung Pro-EUROJUST im Vorgriff auf EUROJUST ihre Arbeit aufgenommen.

Da die Aufgabenstellung von EUROJUST voraussichtlich dazu führen wird, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern – in Zukunft – auch über Opfer und Zeugen sammeln soll, bedarf es als Rechtsgrundlage einer der europäischen Polizeibehörde EUROPOL vergleichbaren Konvention. Diese muss von den Parlamenten der Mitgliedsstaaten ratifiziert werden, um die tiefgreifenden Grundrechtseingriffe durch EUROJUST zu legitimieren und für einen ausreichenden Rechtsschutz zu sorgen.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST haben die Datenschutzbeauftragten des Bundes und der Länder die Aufnahme umfassender Datenschutzvorschriften[56] über

[56] vgl. „Entschließung der 62. Datenschutzkonferenz des Bundes und der Länder vom 24.-26.10.2001 in Münster“ in: Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.3

- den Informationsaustausch mit Partnern und Drittstaaten,
- den Umfang der zu verarbeitenden Daten,
- den Ermittlungsindex als Vorgangsverwaltung,
- das Auskunftsrecht,
- die Änderung, Berichtigung und Löschung,
- Speicherungsfristen,
- die Datensicherheit,
- eine gemeinsame Kontrollinstanz und
- den Rechtsschutz für die Betroffenen

in die Konvention gefordert.

Außerdem muss zum einen der Zugriff des deutschen EUROJUST-Mitgliedes auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister in Deutschland auf eine eindeutige gesetzliche Grundlage gestellt werden. Zum anderen muss sie für EUROJUST ein Auskunftsrecht über strafrechtliche Ermittlungsverfahren in Deutschland etablieren. Ohne diese Rechtsgrundlage könnten die Ermittlungsbehörden der Bundesrepublik Deutschland nach § 474 Strafprozessordnung (StPO) derartigen Auskunftsersuchen nicht stattgeben.

Gegenwärtig bereitet der Europäische Rat einen Beschluss über die Einrichtung von EUROJUST[57] vor, der auch gewisse datenschutzrechtliche Regelungen enthalten soll. Der Abschluss einer Konvention ist bisher nicht vorgesehen.

EUROJUST sollte auf der Basis einer Konvention zwischen den Mitgliedstaaten eingerichtet werden, die einen ebenso hohen Datenschutzstandard vorsieht wie die EUROPOL-Konvention.

[57] Entwurf eines Ratsbeschlusses vom 19.10.2001, 12727/1/01 REV 1

5.2 Rückwirkende Erfassung von DNA-Analysen

5.2.1 Überprüfung der staatsanwaltschaftlichen Praxis

Seit 1999 werden Beschuldigte und Verurteilte sowie ihnen gleichgestellte Personen, deren Strafverfahren wegen einer Straftat von erheblicher Bedeutung, wie z. B. Sexualdelikte oder Körperverletzung, abgeschlossen sind, zur Abgabe einer Speichelprobe aufgefordert. Die daraus erstellten DNA-Identifizierungsmuster werden an das Bundeskriminalamt (BKA) übermittelt und in die dort geführte DNA-Analysedatei eingestellt, mit der bei zukünftigen Straftaten die Täter schneller identifiziert werden sollen. Wir haben die entsprechenden Unterlagen einer Staatsanwaltschaft überprüft.

Maßstab unserer Prüfung war das DNA-Identitätsfeststellungsgesetz, mit dem die Strafprozessordnung um grundrechtssichernde Regelungen für dieses Verfahren ergänzt worden ist. Gem. § 81 e i. V. m. § 81 a StPO ist im anhängigen Strafverfahren die Entnahme von Körperzellen eines Beschuldigten bzw. Dritten und deren molekulargenetische Untersuchung zur Identifizierung oder zum Ausschluss von Spurenverursachern zulässig. Die Körperzellen sind nach Abschluss der Auswertung unverzüglich zu vernichten. DNA-Identifizierungsmuster von Beschuldigten und Verurteilten sowie ihnen gleichgestellten Personen dürfen erhoben und in der DNA-Analysedatei beim BKA gespeichert werden. Eine richterliche Anordnung ist sowohl für die Entnahme von Körperzellen und die anschließende molekulargenetische Untersuchung für die Zwecke eines anhängigen Strafverfahrens, als auch für Zwecke der Identitätsfeststellung Verurteilter in künftigen Strafverfahren und die Aufbewahrung der verformelten Ergebnisse erforderlich. Voraussetzungen für die Maßnahme sind zum einen, dass dem Betroffenen eine Straftat von erheblicher Bedeutung zur Last gelegt wurde, und zum anderen die Negativprognose, bei der das Gericht wegen der Art oder Ausführung der Tat, aufgrund der Persönlichkeit des Täters oder anhand sonstiger Erkenntnisse feststellt, dass er erneut straffällig werden wird.

In einigen Ermittlungsakten fanden sich noch Kurzberichte bzw. Protokolle über die Speichelprobeentnahme, die von den Betroffenen unterschrieben waren und auf denen sie bestätigten, dass sie sich der Maßnahmen freiwillig unterzogen hätten. Den Unterlagen war nicht zu entnehmen, ob die Betroffenen vorher über die Tragweite ihrer Einwilligung bzw. über die Grenzen der Freiwilligkeit aufgeklärt worden waren. In einem Runderlass zur Durchführung

der DNA-Analyse[58] ist eine Einwilligung des Betroffenen nur hinsichtlich der Form der Entnahme von Körperzellen durch Mundhöhlenabstrich vorgesehen. Im Fall seiner Verweigerung des Mundhöhlenabstrichs wird eine Blutprobe entnommen. Die molekulargenetische Untersuchung und die Einstellung in die Analysedatei bedürfen in jedem Fall einer richterlichen Anordnung.

Dabei ist es jedoch erforderlich, dass der Betroffene zuvor über den gesamten Ablauf der Maßnahme informiert und auf seine Rechte in einem Merkblatt hingewiesen werden sollte, das ihm zusammen mit der Ladung zur Speichelprobenentnahme zugestellt wird. Die vorgefundenen Kurzberichte bzw. Protokolle ließen dies nicht immer erkennen.

In einigen Fällen war zweifelhaft, ob die zuständigen Staatsanwälte die Erforderlichkeit einer DNA-Analyse ausreichend geprüft hatten, da die Unterlagen Hinweise enthielten, dass bereits früher eine DNA-Analyse durchgeführt worden war bzw. aber zumindest Körperzellen durch Mundhöhlenabstrich entnommen worden waren. In beiden Fällen ist dessen ungeachtet die Maßnahme durchgeführt worden.

Obwohl der o. g. Runderlass festlegt, dass die Polizei die Staatsanwaltschaft bei der nach § 81 g Abs. 1 StPO zu treffenden Prognoseentscheidung und bei der Abfassung von Anträgen auf richterliche Anordnung unterstützen soll, fanden sich in den geprüften Unterlagen dafür nur in Ausnahmefällen entsprechende Belege dafür. Die Heranziehung polizeilicher Erkenntnisse wäre aber insbesondere bei denjenigen Betroffenen erforderlich, bei denen Tat, Verurteilung und Freiheitsstrafe mehrere Jahre zurückliegen und die sich seit längerem wieder auf freiem Fuß befinden oder in Fällen, in denen die Strafe zu Bewährung ausgesetzt wurde und die Bewährungsfrist vor längerer Zeit abgelaufen bzw. die Reststrafe erlassen worden war. Insbesondere bei der Beurteilung der Wiederholungsgefahr dürfte die Feststellung, ob der Betroffene nach Verbüßung der Haftstrafe oder Ablauf der Bewährungszeit polizeilich einschlägig oder überhaupt wieder in Erscheinung getreten ist, ausschlaggebend sein.

In mehreren geprüften Fällen fanden sich problematische Ermessensentscheidungen der Staatsanwälte, bei denen die Entscheidung, einen richterlichen Beschluss zu beantragen, weder aufgrund der Taten noch aufgrund der Persönlichkeit der Täter oder der bekannten Sachverhalte nachzuvollziehen war. So wurde in einem Fall die Therapie, der sich der Betroffene auf Wunsch des Opfers unterzogen hat, zu seinem Nachteil ausgelegt und damit die von

[58] Runderlass des Ministeriums der Justiz und für Europaangelegenheiten, des Ministeriums des Innern und des Ministeriums für Arbeit, Soziales, Gesundheit und Frauen vom 20.12.2000 Umsetzung des DNA-Identitätsfeststellungsgesetzes@, Justizministerialblatt für das Land Brandenburg, S. 18 ff.

dem Betroffenen ausgehende Wiederholungsgefahr begründet. In einem anderen Fall hat der Staatsanwalt den Antrag auf einen richterlichen Beschluss zur Durchführung der DNA-Analyse nur mit der Tat als einer Straftat von erheblicher Bedeutung begründet, ohne die seitherige straffreie Lebensführung des Betroffenen zu berücksichtigen. Hier hat allerdings das Amtsgericht den Antrag mit ausführlicher Würdigung des seit der Tat straffreien Lebens des Betroffenen abgelehnt.

Wir haben die Auffassung vertreten, das sich bei Sachverhalten, wie eine lang zurückliegende Tat und Bewährungsstrafe oder Aussetzen der Reststrafe verbunden mit seitheriger straffreier Lebensführung im Allgemeinen keine Wiederholungsgefahr begründen lässt, sodass die Staatsanwaltschaft keinen Antrag zur retrograden Erfassung stellen sollte.

Für die Entnahme von Körperzellen zum Zweck der Identitätsfeststellung in künftigen Strafverfahren ist gem. § 1 g Abs. 3 StPO ein Beschluss des zuständigen Amtsgerichts erforderlich, der eine Negativprognose über den Betroffenen voraussetzt. Der anordnende Richter muss feststellen, ob der Betroffene aufgrund seiner Persönlichkeit bzw. wegen der Art oder Ausführung der Tat mit hoher Wahrscheinlichkeit erneut als Straftäter in Erscheinung treten wird. Die erforderlichen Erkenntnisse kann er nur aus der Begründung des Antrags zu einer DNA-Analyse sowie aus den Straf- und Vollstreckungsakten oder ggf. Bewährungsheften gewinnen. Das Bundesverfassungsgericht hat dazu ausgeführt[59], dass vorher eine zureichende Sachaufklärung durch die Beiziehung der o. g. Unterlagen und durch zeitnahe Auskünfte aus dem Bundeszentralregister erforderlich ist und dass in den Entscheidungsgründen die bedeutsamen Umstände abgewogen werden müssen. Des Weiteren muss die Entscheidung sich auf einen Einzelfall beziehen. Die bloße Wiedergabe des Gesetzeswortlautes reicht keinesfalls aus. Auch das Verfassungsgericht des Landes Brandenburg hat die Gerichte in einem Beschluss vom November 2001[60] zu Sorgfalt und Sensibilität bei der Anordnung von DNA-Analysen aufgefordert.

In mehreren Fällen waren Zweifel angebracht, ob die amtsgerichtlichen Beschlüsse diesen Vorgaben des Bundesverfassungsgerichts entsprachen, denn sie beschränkten sich auf die Wiedergabe des Gesetzeswortlauts und der kurzen Ausführungen des beantragenden Staatsanwaltes zur Art der begangenen Straftat und der Persönlichkeit des Betroffenen. Auch wenn der Landesbeauftragte die richterliche Tätigkeit nicht zu überprüfen hat, weist er darauf hin, dass selbst in einem Verfahren, in dem wie bei der retrograden Durchführung von DNA-Analysen große Fallzahlen zu bewältigen sind, Grundrechtseingriffe nicht nur formelhaft und ohne eigene Abwägung be-

59. BVerfG 2 BvR 1741/99 v. 14.12.2000

60 Beschluss v. 15.11.2001 – VfGBbg 49/01, 49/01 EA -, Justizministerialblatt v. 15.1.2002, S. 11f.

gründet werden dürfen. Die Staatsanwaltschaft sollte die Abwägung des Gerichts unterstützen, indem sie für eine Beiziehung der Verfahrensakten sorgt.

Insgesamt haben wir in den geprüften Unterlagen keine datenschutzrechtlichen Verstöße festgestellt. Die Bestimmungen der §§ 81 f Abs. 1 und 81 g Abs. 1 StPO waren insoweit eingehalten worden. Ungeachtet dessen kann eine abschließende datenschutzrechtliche Beurteilung noch nicht vorgenommen werden, weil einzelne in den Unterlagen festgestellte Sachverhalte oder Verfahrensabläufe noch geklärt werden müssen.

Die Staatsanwaltschaft muss in jedem Einzelfall prüfen, ob Grund zu der Annahme besteht, dass der verurteile Straftäter erneut eine Straftat von erheblicher Bedeutung begehen wird und deshalb sein genetischer Fingerabdruck zu speichern ist. Das Amtsgericht hat über den Antrag der Staatsanwaltschaft nach eigener Abwägung zu entscheiden.

5.2.2 „PROREDDI“

Im Berichtszeitraum hat der Generalstaatsanwalt eine Errichtungsanordnung für die von ihm betriebene Datei „Programm zur Realisierung des DNA-Identitätsfeststellungsgesetzes – PROREDDI“ vorgelegt. Sie dient der rückwirkenden Erfassung der von DNA-Identitätsmustern verurteilter Straftäter in der beim Bundeskriminalamt geführten DNA-Analysedatei. Die rückwirkende Erfassung der sog. Altfälle setzt voraus, dass die zuständigen Staatsanwaltschaften die personenbezogenen Daten der Verurteilten aus in Frage kommenden Strafverfahren sowie die diesbezüglichen Verfahrensdaten aus dem Bundeszentralregister erhält.

Gegen den Betrieb der Datei als solcher bestehen keine datenschutzrechtlichen Bedenken. Dies gilt jedoch nicht für die Errichtungsanordnung. Insbesondere haben wir bemängelt, dass in der Errichtungsanordnung lediglich die Rechtsvorschrift und die dortigen Voraussetzungen aufgezählt werden, ohne dass anhand des Zwecks der Datei die Einzelheiten festgelegt werden. So fehlen beispielsweise Fristen, nach deren Ablauf die Erforderlichkeit der Datenspeicherungen geprüft werden müssen sowie eine maximale Speicherungsdauer.

Nach Weiterleitung des DNA-Analyseergebnisses über das Landes- an das Bundeskriminalamt oder nach der Ablehnung, eine DNA-Analyse durchzuführen, besteht kein Erfordernis zur weiteren Speicherung des gesamten Datensatzes in der Datei PROREDDI mehr. Es genügt vielmehr, wenn die Staats-

anwaltschaft ihre Maßnahmen in dem Einzelfall im Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV)[61] dokumentiert.

Mit der bloßen Verweisung auf die Rechtsvorschriften wird zum einen sowohl der Zweck von Errichtungsanordnungen als auch die Regelung der Strafprozessordnung verkannt. In ihr hat der Bundesgesetzgeber allgemeine Parameter zur Datenverarbeitung aufgestellt, innerhalb derer sich die Datenverarbeitung bei den Staatsanwaltschaften zu bewegen hat. Den Anforderungen bezüglich Regelungstiefe und -detailliertheit an eine bestimmte Datei im Einzelfall können sie gerade nicht genügen. Das sollen die in § 490 StPO für jede Datei vorgeschriebenen Errichtungsanordnungen leisten.

Die Errichtungsanordnung PROREDDI, die dazu lediglich auf die einschlägigen Vorschriften zur Datenverarbeitung für Zwecke künftiger Strafverfahren oder für Zwecke der Vorgangsverwaltung verweist, leistet das nicht.

Die Errichtungsanordnung trifft keine eindeutige Festlegung für die Zeit nach Abschluss der rückwirkende Erfassung der aus dem Bundeszentralregister übermittelten Altfälle. Wenn die DNA-Identifizierungsmuster der dazu in Frage kommenden Betroffenen in der DNA-Analysedatei eingestellt worden sind, hat die Datei ihren Zweck erfüllt und ist somit aufzulösen.

Aus der Errichtungsanordnung muss ersichtlich sein, welche Daten dort auf welche Weise wie lange und zu welchen Zwecken verarbeitet und unter welchen Voraussetzungen an welche Empfänger übermittelt werden dürfen. In der Errichtungsanordnung „PROREDDI“ muss zudem noch festgelegt werden, dass die Datei nach Abschluss der rückwirkenden Erfassung der Altfälle aufgelöst wird.

5.3 „MESTA“

Das von Brandenburg zusammen mit den Bundesländern Hamburg, Hessen, Schleswig-Holstein und Nordrhein-Westfalen betriebene Entwicklungsprojekt „Mehrländer-Staatsanwaltschaft-Automation (MESTA)“ ist unterdessen in den Echtbetrieb gegangen und steht allen Staatsanwaltschaften des Landes zur Verfügung. Der Generalstaatsanwalt hat uns den Entwurf einer Errichtungsanordnung mit der Bitte um datenschutzrechtliche Prüfung übersandt.

Das Verfahrensregister MESTA soll als einheitlicher Datenbestand über brandenburgische staatsanwaltschaftliche Ermittlungsverfahren bei der Generalstaatsanwaltschaft des Landes geführt werden, auf den alle Staatsan-

[61] s. unten A 5.3

waltschaften uneingeschränkt Zugriff haben. Damit ist der Eingriff in die Grundrechte der Betroffenen wesentlich tiefer als bei der datenschutzfreundlicheren, nicht umgesetzten dezentralen Lösung bei den einzelnen Staatsanwaltschaften mit nach Erforderlichkeitskriterien festgelegten Zugriffsrechten anderer Dienststellen. Die Erforderlichkeit einer zentralen Datei auf Landesebene ist nicht zwingend gegeben, da das bundesweite Zentrales Staatsanwaltschaftliches Verfahrensregister bereits denselben Datenbestand mit einer grundsätzlichen Speicherungsdauer von zwei Jahren zur Verfügung stellt.

Die Errichtungsanordnung enthält selbst bei den wesentlichen Datenverarbeitungsschritten keine auf den Zweck der Datei „MESTA“ und die dort zu verarbeitenden Daten ausgerichteten Regelungen. Vielmehr wird lediglich auf die Datenverarbeitungsvorschriften der Strafprozessordnung verwiesen.

Zudem scheint die Verweisungssystematik auch grundsätzlich weder sach- noch datenschutzgerecht. Bei einer Zentraldatei wie MESTA kommt es insbesondere auf eine möglichst einheitliche Anwendung der Datenverarbeitungsregelungen in der Praxis an, damit für alle Nutzer die Datenverarbeitung transparent und der Datenbestand aussagefähig ist. Ein Datenbestand, in dem gewichtige Sachverhalte ebenso behandelt worden sind wie Bagatellsachen, der mit vielen inaktuellen Datensätzen aus Altvorgängen befrachtet ist und bei dem die Qualität der Daten nicht durch stringente Verarbeitungsregelungen gesichert ist, erfüllt die Erwartungen der Anwender an Aussagefähigkeit und Transparenz der Datenverarbeitung nicht.

Insgesamt haben wir kritisiert, dass die vorliegende Errichtungsanordnung mit ihren umfänglichen Anlagen grundsätzlich wenig transparent und in vielen Punkten unzulänglich ist. Wir haben eine Überarbeitung empfohlen.

5.4 Heiratsabsichten – datenschutzgerecht zu überprüfen

Der Präsident des Oberlandesgerichts fordert grundsätzlich die vollständigen Akten der Ausländerbehörde derjenigen heiratswilligen in Deutschland lebenden Ausländer an, deren Heimatstaaten nur über ein mangelhaftes Urkundswesen verfügen und deshalb nicht die erforderliche Bescheinigung darüber ausstellen können, dass keine Ehehindernisse bestehen.

Die Einsichtnahme in Akten der Ausländerbehörde seitens des Präsidenten des Brandenburgischen Oberlandesgerichts ist eine Datenerhebung bei Dritten, die nur in bestimmten Ausnahmefällen zulässig ist. Dies wäre dann der Fall, wenn die Bearbeitung eines vom Betroffenen gestellten Antrags ohne diese Datenerhebung nicht möglich oder es erforderlich ist, Angaben des Betroffenen zu überprüfen. Dagegen ist es nicht gerechtfertigt, die Akten der

Ausländerbehörde bei Antragstellern aus bestimmten Ländern pauschal – ohne Einzelfallprüfung – beizuziehen.

Wir halten es für unzulässig, stets vollständige Akten der Ausländerbehörde anzufordern und haben darum gebeten, künftig nur noch Daten im zulässigen Umfang aus den Akten der Ausländerbehörden zu erheben.

Andererseits sind nach Aussage des Gerichts nahezu alle Bestandteile der Ausländerakten für das Verfahren relevant. Eine auszugsweise Einsicht dürfte daher nicht praktikabel sein. Darüber hinaus ist die auszugsweise Übermittlung datenschutzrechtlich auch nicht unbedenklich, da dann die Ausländerbehörde Kenntnis von Umständen aus dem Verfahren beim Brandenburgischen Oberlandesgericht erlangen kann. In künftigen datenschutzrechtlichen Zweifelsfällen wird das Oberlandesgericht daher stets die schriftliche Einwilligung der Betroffenen einholen.

Werden Akten der Ausländerbehörden vom Oberlandesgericht zu Urkundszwecken bei einer Heirat von in Deutschland lebenden Ausländern angefordert, ist hierzu die Einwilligung der Betroffenen erforderlich.

5.5 Die Gerichte im Internet

5.5.1 Insolvente Verbraucher am globalen Pranger?

Um Kosten für die vorgeschriebenen Bekanntmachungen in Zeitungen und Amtsblättern zu sparen, gehen die Gerichte (in Brandenburg bisher nur das Amtsgericht Potsdam) dazu über, Entscheidungen in Insolvenzverfahren im Internet zu veröffentlichen. Dabei herrschte in der Justiz zunächst die Meinung vor, es bestünde kein Unterschied zwischen einer gedruckten Veröffentlichung und einer Einstellung in das WorldWide-Web.

Dieser Unterschied besteht durchaus. Auskunfteien und Wirtschaftsinformationsdienste können die online bereitgestellten Insolvenzinformationen auswerten und auch dann noch speichern, wenn das Insolvenzverfahren abgeschlossen ist. Außerdem durchsuchen Suchmaschinen (Web Spider, Crawler) automatisch das Internet und stellen die Suchergebnisse weltweit zum Abruf bereit. Das ist unproblematisch, solange die Zahlungsfähigkeit von Unternehmen in Frage steht. Die Insolvenzordnung regelt aber auch das Verfahren bei Verbraucherinsolvenzen, also überschuldeten Einzelpersonen, und will diesen einen wirtschaftlichen Neubeginn ermöglichen. Dieser Neubeginn wird letztlich erschwert, wenn der Schuldner an einen weltweiten Pranger gestellt wird.

Die Datenschutzbeauftragten haben deshalb den Bundesgesetzgeber aufgefordert, bei der Neufassung der Insolvenzordnung eine Regelung zu treffen, die den Schutz von insolventen Verbrauchern bei einer Veröffentlichung von Verfahrensdaten im Internet sicherstellt[62]. Der Gesetzgeber hat dies bei der Änderung des § 9 Insolvenzordnung[63] nicht mehr berücksichtigt, aber das Bundesministerium der Justiz ermächtigt, die Einzelheiten der Veröffentlichung im Internet durch Rechtsverordnung zu regeln.

Der uns vorliegende Verordnungsentwurf soll insbesondere darauf abzielen, die Integrität und die Authentizität der in das Internet eingestellten Daten zu sichern. Da es nach den derzeitigen technischen Möglichkeiten einen verlässlichen Kopierschutz noch nicht gibt, sind die nach dem jeweiligen Stand der Technik verfügbaren Mittel einzusetzen, um ein Kopieren zumindest zu erschweren.

Das Bundesministerium der Justiz hat in seinem Verordnungsentwurf allerdings einen großzügigen Maßstab für die Recherchekriterien angelegt. Nach dem Entwurf ist es möglich, sich eine komplette Übersicht der zu einem Familiennamen vorhandenen Datensätze anzeigen zu lassen, selbst wenn als Suchkriterien (neben dem Sitz des Insolvenzgerichts) lediglich der unvollständige Familienname (z. B. durch Eingabe von zwei Zeichen) eingegeben wurde.

Wir haben demgegenüber vorgeschlagen, eine zusätzliche Regelung zu treffen, die die Recherchemöglichkeit auf die Suche nach Namen von Firmen oder Einzelpersonen beschränkt, den Zugriff auf oder das Herunterladen ganzer Datenbestände dagegen ausschließt.

Wenn gewährleistet ist, dass die in das Internet eingestellten Daten auch tatsächlich von den Gerichten stammen, den Lauf des Verfahrens getreu abbilden und möglichst nicht elektronisch kopiert oder unbegrenzt systematisch durchsucht werden können, ist auch die Veröffentlichung des Insolvenzregisters im Internet datenschutzrechtlich hinnehmbar.

5.5.2 Zwangsversteigerungen

Einige Amtsgerichte veröffentlichen die Termine von Zwangsversteigerungen im Internet, die inhaltlich mit den üblichen Zeitungsinseraten übereinstimmen. Hierbei bedienen sie sich eines kommerziellen Anbieters.

---

[62] Entschließung v. 24.4.2001, Dokumente zu Datenschutz und Informationsfreiheit 2001, A.I.2

[63] durch das Gesetz zur Änderung der Insolvenzordnung und anderer Gesetze vom 26.10.2001, BGBl. I S.2710

Die Internetveröffentlichung fällt unter die Befugnis der Gerichte nach § 40 Abs. 2 Zwangsvollstreckungsgesetz, den Termin einer öffentlichen Zwangsversteigerung zu verbreiten. Die Gerichte übermitteln die Daten schriftlich an einen Internetanbieter, der diese aufbereitet und ins Internet einstellt. Der Name des zahlungsunfähigen Eigentümers wird nicht veröffentlicht. Mit Einstellung ins Internet vernichtet der Anbieter die schriftlichen Unterlagen. Nach Ablauf des Versteigerungstermins entfernt er auch die Daten aus seinem Internetangebot.

Mit der Internetveröffentlichung hofft das Zwangsvollstreckungsgericht, einen größeren Kreis von Bietern zu erreichen, um so den Erlös aus der Versteigerung eines Grundstücks zu erhöhen. Dies dient nicht nur dem Interesse des Gläubigers, sondern auch dem des Schuldners, die noch offenen Forderungen zu begleichen. Vor diesem Hintergrund kann ein möglicher Rückschluss auf die Identität des Schuldners hingenommen werden.

Die Veröffentlichung von Terminen zur Zwangsversteigerung ohne direkten Personenbezug im Internet mit Hilfe der Anschrift des Versteigerungsobjekts ist datenschutzrechtlich zulässig .

5.5.3 Handelsregister

Die Justiz treibt bundesweit die Bereitstellung von Daten aus dem Handelsregister zum Abruf über das Internet voran. Dass dies auch in Brandenburg geschieht, erfuhren wir allerdings erst durch eine Pressemitteilung des Ministeriums der Justiz und für Europaangelegenheiten im Herbst 2000. Auf unsere Nachfrage hin zeigte sich das Ministerium kooperationsbereit, betonte aber auch, bei dem geplanten Verfahren sei der „Schutz personenbezogener Daten nicht intendiert", weil das Handelsregister und vergleichbare Register dem Zweck dienten, die Daten der rechtlich handelnden Personen zu veröffentlichen.

Richtig ist, dass das Handelsregister (und ebenso die vergleichbaren Partnerschafts- und Genossenschaftsregister) dem Zweck dienen, die gesetzlich vorgeschriebene Publizität bestimmter Informationen über Unternehmen und Gewerbetreibende sicherzustellen, weil sie nur unter dieser Voraussetzung im Rechtsverkehr wirksam werden[64]. Deshalb ist auch jedem die Einsicht in das herkömmliche Handelsregister beim Registergericht ohne weitere Voraussetzungen gestattet.

[64] § 15 Handelsgesetzbuch (HGB)

Es liegt nahe, diese Informationen auch online, also internetgestützt jedem zugänglich zu machen. Auf diese Weise können die Gerichte ihre gesetzlich vorgeschriebene Dienstleistung „Zugang zum Handelsregister“ erheblich kostengünstiger und bürgerfreundlicher erbringen, als es bisher bei der persönlichen Vorsprache im Registergericht der Fall ist. Dazu mussten allerdings zunächst die notwendigen Rechtsgrundlagen geschaffen werden, weil das Handelsgesetzbuch den Abruf von Daten durch nicht öffentliche Stellen (also auch jede Bürgerin und jeden Bürger) aus dem maschinellen Handelsregister nur dann zuließ, wenn der Empfänger ein berechtigtes berufliches oder gewerbliches Interesse wahrnahm und kein Grund zu der Annahme bestand, dass die Daten zu anderen Zwecken abgerufen werden sollten. Mit dem am 15.12.2001 in Kraft getretenen Gesetz über elektronische Register und Justizkosten für Telekommunikation[65] und der wenig später erlassenen Verordnung zur Erleichterung der Registerautomation[66] sind jetzt die rechtlichen Voraussetzungen dafür geschaffen worden, dass eine „online-Einsicht“ in die entsprechenden Register für jedermann in der gleichen Weise ermöglicht werden kann, wie eine persönliche Einsichtnahme im Registergericht. Dies ist vor dem Hintergrund des Grundrechts auf Akteneinsicht zweifellos zu begrüßen.

Allerdings kann der Datenschutz auch bei der Umsetzung dieser Neuregelung nicht völlig außer Betracht bleiben. Denn das Handelsregister enthält auch Daten der für die Unternehmen handelnden Personen, die personenbezogene Daten im Sinne des Datenschutzrechts sind. Der Gesetzgeber hat den online-Abruf für jedermann deshalb nur „zu Informationszwecken“ zugelassen, um zu verhindern, dass gewerbliche Unternehmen massenhaft Handelsregisterdaten abrufen, um private Parallelregister aufzubauen. Zudem hat er die Möglichkeit des Ausschlusses von Nutzern für den Fall vorgesehen, dass die vorgeschriebene Stichprobenkontrolle einen Missbrauch des Abrufverfahrens oder der übermittelten Daten belegen.

Es bleibt abzuwarten, wie diese Missbrauchskontrolle in der Praxis erfolgt. Es sollte technisch sichergestellt werden, dass entsprechend den Intentionen des Gesetzgebers dem online-Nutzer nur der Ausdruck aus dem Handelsregister auf dem Bildschirm dargestellt wird. Der gesetzliche Zweck des Handelsregisters deckt keine Suchstrategien, die bei einer Einsichtnahme in den Räumen des Registergerichts ausgeschlossen sind. So muss zwar nach Firmennamen gesucht werden können; die Recherche nach den Namen handelnder Personen muss aber auch technisch ausgeschlossen bleiben.

---

[65] BGBl. I S. 3422

[66] BGBl. I S. 3688

Es ist zu begrüßen, dass die rechtlichen Voraussetzungen für eine online-Nutzung des Handelsregisters und anderer auf Publizität angelegter öffentlicher Register geschaffen worden sind. Datenschutzrechtlich ist aber sicherzustellen, dass nicht automatisierte Suchroutinen nach Personen durchgeführt werden können, die bei der konventionellen Registereinsicht ausgeschlossen sind.

6 Bildung, Jugend und Sport

6.1 Datensammlung im Ministerium – Umstellung der Schuldatenerhebung

Das Ministerium für Bildung, Jugend und Sport beabsichtigt, die jährliche Schuldatenerhebung in Brandenburg umzustellen. Zum einen habe sich in der Vergangenheit gezeigt, dass der bei Schulen und staatlichen Schulämtern erhobene Datenkatalog nicht ausreiche, um die Aufgaben des Ministeriums zu erfüllen. Zum anderen sei das bisherige papierförmige Verfahren vor allem für die Schulen mit sehr viel Aufwand und einer hohen Fehlerquote verbunden, sodass dieses durch ein automatisiertes Verfahren unter Beteiligung des Landesbetriebs für Datenverarbeitung und Statistik abgelöst werden soll. Dabei ist grundsätzlich zu unterscheiden zwischen den personenbezogenen Daten der Lehrkräfte und denen der Schülerinnen und Schüler.

Das Ministerium für Bildung, Jugend und Sport hat überzeugend dargelegt, dass der – verglichen mit der bisherigen Sachlage – wesentlich größere Datenumfang über die Lehrkräfte zur Erfüllung seiner Aufgaben erforderlich ist. Vor allem die erforderliche Ermittlung der Schüler-Lehrer-Relation ist derart komplex, dass es unabdingbar ist, eine Fülle von personenbezogenen Einzeldaten über jede Lehrkraft zu erheben.

Die rechtlichen Voraussetzungen für eine regelmäßige Übermittlung von Lehrereinsatz- und Unterrichtsdaten von den Schulen direkt an das Ministerium sind derzeit allerdings nicht ausreichend. Die hier einschlägige Vorschrift (§ 15 Abs. 1 Datenschutzverordnung Schulwesen – DSV) lässt eine Übermittlung personenbezogener Daten an das Ministerium nur in Einzelfällen zu. Im Übrigen können nach derzeitiger Rechtslage nur anonymisierte Daten an das Ministerium übermittelt werden.

Das Ministerium für Bildung, Jugend und Sport hat zugesagt, § 15 DSV entsprechend seinen Bedürfnissen zu ändern und beabsichtigt in diesem Zusammenhang, auch den Katalog der zu übermittelnden Daten detailliert festzulegen.

Für die vorgesehene elektronische Übermittlung der Daten der Lehrkräfte an das Ministerium müssen eine Reihe von technischen und organisatorischen Maßnahmen zum Datenschutz getroffen werden. Dabei ist zu berücksichtigen, dass es sich bei den Daten über die Lehrkräfte um Personaldaten, also um Daten einer hohen Schutzstufe handelt.

Offen ist bisher noch die Umstellung der Schuldatenerhebung hinsichtlich der Daten der Schülerinnen und Schüler. Auch hier beabsichtigt das Ministerium, ebenfalls für jede Schülerin und jeden Schüler personenbeziehbare Einzeldatensätze zu erheben. Das Ministerium für Bildung, Jugend und Sport konnte nicht überzeugend darlegen, für welche Aufgaben des Ministeriums die Übermittlung derart detaillierter Daten über die Schülerinnen und Schüler erforderlich ist, sodass wir die Gefahr einer Datenspeicherung auf Vorrat sehen. Unser Vorschlag, den Landesbetrieb für Datenverarbeitung und Statistik mit diesen Aufgaben zu befassen und dem Ministerium für Bildung, Jugend und Sport die Daten nur anonymisiert zur Verfügung zu stellen, ist bisher nicht aufgegriffen worden.

Die vom Ministerium für Bildung, Jugend und Sport beabsichtigte Umstellung der Schuldatenerhebung bedarf hinsichtlich der personenbezogenen Daten der Lehrkräfte einer Änderung der Datenschutzverordnung Schulwesen. Die Ablösung der weitgehend papiergestützten Schuldatenerhebung durch elektronische Verfahren ist durch besondere technische und organisatorische Maßnahmen abzusichern, die der Sensibilität der verarbeiteten Daten Rechnung tragen. Für eine personenbezogene zentrale Verarbeitung von Daten aller Schülerinnen und Schüler im Ministerium ist kein Erfordernis erkennbar.

6.2 „Führerscheinprüfung“ für Internet und PC – Klassenziel verfehlt!

Mit der Initiative m.a.u.s – Medien an unsere Schulen – hat sich die Landesregierung zum Ziel gesetzt, die Nutzung neuer Medien im Unterricht voranzutreiben. Das Ministerium für Bildung, Jugend und Sport bietet Schülerinnen und Schülern der Sekundarstufe I hierzu die interaktive CD-ROM „Internet-Führerschein“ an, um Grundkenntnisse für die Nutzung von Computer und Internet zu vermitteln.

Zu begrüßen ist, dass mit diesem Projekt die Teilnahme der Schülerinnen und Schüler an der Informations- und Wissensgesellschaft erheblich gefördert wird. Allerdings klärt die CD-ROM über die Risiken der Kommunikation in offenen, globalen Netzen nur unzureichend auf. Eine umfassende Sensibilisierung auch für die vorhandenen Instrumente und Techniken zum Schutz der Privatsphäre ist die Voraussetzung für einen verantwortungsbewussten Umgang mit den vielfältigen Möglichkeiten der „Neuen Medien“.

Die CD-ROM wurde ausgeliefert, ohne dass wir auf deren Inhalt hätten Einfluss nehmen können. Um die Schülerinnen und Schülern dennoch bereits beim Einstieg in die Nutzung des Internet über die Themen Datenschutz und Informationsfreiheit informieren zu können, schlug das Ministerium für Bildung, Jugend und Sport vor, entsprechende Lerninhalte in die Angebote des Medienpädagogischen Zentrums aufzunehmen. Diese Einrichtung ist intensiv in die m.a.u.s.-Initiative eingebunden und erklärte sich bereit, das Projekt durch Einstiegsangebote zum Datenschutz zu begleiten. Zu diesem Zweck sollen auf dem bereits bestehenden Bildungsserver (http://www.bildung-brandenburg.de) die Themen Datenschutz und Datensicherheit behandelt werden.

Selbst die besten Weiterbildungsangebote zu Datenschutzthemen nützen allerdings wenig, wenn multimediale Lernmedien vom Ministerium verteilt werden, die Grundelemente des Datenschutzes außer Acht lassen. Von einem aufmerksamen Lehrer wurden wir darauf hingewiesen, dass das Ministerium eine weitere CD-ROM zum Erwerb eines „PC-Führerscheins“ an die Schulen verteilen ließ und die Lehrkräfte aufforderte, im Rahmen des Unterrichts den Erwerb eines solchen PC-Führerscheins zu ermöglichen. Die CD-ROM sei ein Geschenk einer privaten Firma, die sie u. a. mit Unterstützung einer Krankenkasse entwickelt hatte.

Bei der Benutzung dieses Programms im offline-Betrieb wurden die Schülerinnen und Schüler aufgefordert, zahlreiche personenbezogene Daten und auch den Namen der Krankenkasse, bei der sie versichert sind, in den Computer einzugeben. Der größte Teil dieser Angaben stand in keinem erkennbaren Zusammenhang mit dem Erwerb des PC-Führerscheins. Am Ende des Programms wurden die „Fahrschüler“ aufgefordert, ihren Namen mit Anschrift und weiteren Angaben in einem Formular sowie einen Lebenslauf auszudrucken, die an die private Herstellerfirma geschickt werden sollten, damit diese die eigentlichen PC-Führerscheine ausstellen und verschicken könne. Eine andere Möglichkeit, dieses Zertifikat zu erhalten, wurde nicht angeboten. Auch eine Aufklärung über die Verwendung dieser Daten war nicht vorgesehen. Dem unbefangenen Beobachter drängte sich der Eindruck auf, dass die Herstellerfirma (und möglicherweise auch die beteiligte Krankenkasse) ein wirtschaftliches Interesse an den von den „Fahrschülern“ übermittelten Daten haben könnte. Außerdem enthielt das Programm einen Link zur Website der Herstellerfirma, auf der die Schüler aufgefordert werden, weitere personenbezogene Daten ohne Möglichkeit der Verschlüsselung an diese Firma zu übermitteln.

Der Landesbeauftragte hat den zuständigen Minister aufgefordert, die weitere Verwendung dieser mangelhaften CD-ROM unverzüglich zu unterbinden und

sicher zu stellen, dass sie nur in einer datenschutzgerechten Weise, also nach umfassender Aufklärung der Schülerinnen und Schüler und der Einräumung einer Möglichkeit zum dezentralen Ausdruck der Zertifikate in den Schulen weiter verwandt werden darf.

Kenntnisse über die Gefährdung und den möglichen Schutz der Privatsphäre im Internet sind die Voraussetzung für eine verantwortungsvolle Nutzung der „Neuen Medien“ und sollten so früh wie möglich an den Schulen vermittelt werden.

Lernmedien wie die CD-ROMs „Internet-Führerschein“ und „PC-Führerschein“ genügen diesem Anspruch bisher nicht, sondern lassen datenschutzrechtliche Grundregeln außer Acht.

6.3 Anbindung von Schulen an das Internet

Im Rahmen der Medienoffensive m.a.u.s. zur IT-Ausstattung der Schulen hat das Ministerium für Bildung, Jugend und Sport gemeinsam mit der Deutschen Telekom AG das Projekt „Security@School“ ins Leben gerufen. Ziel dieses Projektes ist die sichere und kostengünstige Anbindung des Schüler- und Schulverwaltungsnetzes an das Internet.

Datenverarbeitungsgeräte der Schulverwaltung dürfen nicht mit im Unterricht verwendeten Datenverarbeitungsgeräten vernetzt werden (§ 4 Abs. 1 Datenschutzverordnung Schulwesen). Der Verordnungsgeber beabsichtigte mit dieser Regelung, den unbefugten Zugriff auf das Schulverwaltungsnetz zu verhindern. Im Rahmen der m.a.u.s.-Offensive wird den Schulen des Landes Brandenburg u. a. ein kostenloser Internetzugang von der Deutschen Telekom AG zur Verfügung gestellt. Das Problem bestand nun darin, der Datenschutzverordnung Schulwesen gerecht zu werden und eine technische Lösung zu finden, um das Schulverwaltungs- und das Schülernetz über nur einen Zugang an das Internet anzuschließen und die gegenseitige Abschottung beider Schulnetze zu gewährleisten.

Im Projekt „Security@School“ wird die Abschottung des Schulverwaltungsnetzes vom Schülernetz sowie beider Netze vom Internet durch ein Firewallsystem realisiert. Die hierbei eingesetzten Komponenten werden derzeit in einem Pilotprojekt an einigen Schulen des Landes getestet. Die technische Betreuung wird zentral von der Deutschen Telekom AG durchgeführt. Durch Einsatz eines Content-Filters können Zugriffe aus dem Schülernetz auf bestimmte WWW-Seiten vor allem aus den Bereichen Pornografie, Gewalt und Drogen gesperrt werden.

Nach dem heutigen Stand der Technik und unter Berücksichtigung der hinnehmbaren Restrisiken ist eine logische Trennung des Schülernetzes vom Schulverwaltungsnetz und der gleichzeitige Anschluss beider Netze an das Internet durch Einsatz eines Firewallsystems datenschutzrechtlich zulässig.

6.4 Geheimnisse bei der Zeugnisübergabe

Während der Zeugnisübergabe waren auch Eltern von Mitschülern ohne offizielle Einladung zugegen. Die Übergabe erfolgte in der Weise, dass die Klassenlehrerin jedes Kind auf seinen Leistungsstand angesprochen hat.

Nach § 46 Abs. 2 Brandenburgisches Schulgesetz (BbgSchulG) haben die Eltern das Recht, unter Berücksichtigung der pädagogischen Situation der Klasse nach vorheriger Anmeldung bei der unterrichtenden Lehrkraft den Unterricht zu besuchen. Es bedarf keiner förmlichen Einladung, sondern der vorherigen Anmeldung. Der Gesetzgeber hat hier das Informationsrecht der Eltern nicht nur in Bezug auf das jeweils eigene Kind gesehen, sondern betrachtet dieses Informationsrecht als Einblick in den gesamtpädagogischen Prozess innerhalb der Klasse und die Arbeit der Lehrkraft. Hierzu gehört auch die im Rahmen der pädagogischen Freiheit der Lehrkraft zulässige Äußerung von Werturteilen über die Leistungen der Schüler.

Die Schule soll gem. § 46 Abs. 3 BbgSchulG die Schülerinnen und Schüler sowie deren Eltern individuell in angemessenem Umfang informieren. Die Vorschrift zielt darauf ab, dass die Schülerinnen und Schüler jeweils über ihre eigenen Leistungen zu informieren sind, sowie die Eltern über die ihrer Kinder. Eine solche Information ist aber nur sinnvoll, wenn der Leistungsstand eines Schülers auch im Verhältnis zu den anderen Schülerinnen und Schülern festgestellt werden kann.

Auch mündliche Leistungen, die im Beisein der Mitschüler erbracht werden, werden sinnvoller Weise im Beisein der Mitschüler bewertet. Dies gehört zu den in § 67 Abs. 2 BbgDSG umschriebenen pädagogischen Verantwortlichkeiten der Lehrkräfte; die damit möglicherweise einhergehende Einschränkung des Rechts auf informationelle Selbstbestimmung ist insoweit als unabdingbar und zulässig anzusehen.

Eine wortlose oder gar „geheime“ Übergabe von Schulzeugnissen ist mit dem Bildungs- und Erziehungsauftrag der Schule nicht zu vereinbaren. Gerade die Übergabe der Zeugnisse stellt einen Höhepunkt im Schulalltag dar. Sie ist auch Ausdruck der sozialen Einbindung der einzelnen Schülerinnen und Schüler in den Klassenverband. Eine Kommentierung der Zeugnisse und des darin dokumentierten Leistungsstands der Schülerinnen und Schüler bei ihrer Übergabe durch die Klassenlehrerin oder den Klassenlehrer ist – sofern sie

nicht unter entwürdigenden oder diskriminierenden Umständen erfolgt – aus pädagogischen Gründen u.a. zur Motivation für die weitere Lernentwicklung als wünschenswert zu erachten. Anderes wäre nur anzunehmen, wenn sich Lehrkräfte außerhalb des direkten Schulzusammenhangs über die Leistungen ihrer Schülerinnen und Schüler äußerten.

Eine geheime Übergabe von Schulzeugnissen ist nicht mit dem Bildungs- und Erziehungsauftrag der Schule zu vereinbaren. Auch aus pädagogischen Gründen ist eine Kommentierung der Zeugnisse zulässig.

6.5 Datenschutz bei Adoptionen

Bürger fragten bei uns an, ob andere Behörden als das Geburtsstandesamt Daten des Kindes aus der Zeit vor der Adoption verarbeiten dürfen.

Zentrale Vorschrift zum Schutz von Informationen über Adoptionen ist das in § 1758 des Bürgerlichen Gesetzbuches (BGB) festgelegte Adoptionsgeheimnis, welches für jeden gilt, der Kenntnis über die Tatsache der Adoption oder ihre Umstände hat, also auch für Behörden.

Das Adoptionsgeheimnis kann nur durchbrochen werden, wenn besondere Gründe des öffentlichen Interesses dies erfordern. Soweit eine Behörde das Adoptionsgeheimnis im besonderen öffentlichen Interesse durchbrechen will, handelt es sich um eine Übermittlung personenbezogener Daten, die lediglich auf Grund einer gesetzlichen Grundlage zulässig ist.

Solche Vorschriften sind beispielsweise im Personenstandsgesetz – dem Gesetz für die Tätigkeit der Standesämter – zu finden. So wird in das Geburtenbuch beim Standesamt eingetragen, wer die leiblichen Eltern eines (später) adoptierten Kindes sind. In diesen Geburtseintrag dürfen nur Behörden, die Adoptiveltern, deren Eltern, der gesetzliche Vertreter des Kindes sowie das Kind selbst Einsicht nehmen.

Wichtig ist hierbei, dass die Geburtsurkunde keinen Hinweis auf eine Adoption enthalten darf. Das durch Adoption angenommene Kind gilt nach § 1755 BGB als eheliches Kind der Annehmenden, sodass letztere als die Eltern in die Geburtsurkunde einzutragen sind. In der Abstammungsurkunde, die beispielsweise bei einer Heirat vorgelegt werden muss, sind hingegen auch die leiblichen Eltern angegeben.

Behörden erhalten nur dann Einsicht in den Geburtseintrag oder Personenstandsurkunden, wenn die Informationen im Rahmen ihrer Zuständigkeit erforderlich sind und sie den Zweck angeben, für den sie diese Daten benötigen. Aus der rechtlichen Stellung des Kindes als eheliches Kind der Anneh-

menden folgt, dass kaum Fälle vorstellbar sind, bei denen die Tatsache der Adoption für die Aufgaben anderer Behörden erforderlich sein soll. In der Regel wird es ausreichen, dass Behörden nur solche Informationen vom Standesamt bekommen, die nicht auf die Adoption schließen lassen.

Der frühere Name des Kindes wird darüber hinaus auch im Melderegister gespeichert. Er kann nur ausnahmsweise bei einem besonderen öffentlichen Interesse an andere Behörden übermittelt werden.

Eine Auskunft über die Tatsache der Adoption aus dem Melderegister an Dritte ist hingegen nur dann zulässig, wenn auch eine Einsicht in das Geburtsregister beim Standesamt unter den Voraussetzungen des Personenstandsgesetzes zulässig wäre.

Das Adoptionsgeheimnis hat einen hohen Rang. Daten über die Adoption dürfen an Behörden und Dritte nur ganz ausnahmsweise weitergegeben werden.

6.6 Aktenführung im Jugendamt

Bei Kontrollen in zwei Jugendämtern stellten wir Defizite und Unsicherheiten bei der Aktenführung, Datenübermittlungen sowie Akteneinsichtsbegehren fest.

Bürger beschwerten sich bei uns über die Unvollständigkeit von Jugendhilfeakten. Durch fehlende Paginierung – also die durchgehende, unveränderliche Nummerierung der Seiten – war für die Beteiligten schwer oder gar nicht nachzuweisen, ob Dokumente Bestandteil eines Vorgangs geworden sind. Dies verstößt gegen § 78 a des Zehnten Buches des Sozialgesetzbuches (SGB X). Aus der Verpflichtung des Jugendamtes, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, folgt auch eine Pflicht zur vollständigen Dokumentation aller Verarbeitungsvorgänge. Diese müssen für Akteneinsicht nehmende Dritte transparent und nachvollziehbar sein. Eine Paginierung, die vor allem dem Nachweis der Vollständigkeit der Akte dient, liegt auch im Interesse des Jugendamtes. Dadurch können Vermutungen, die Akte sei manipuliert worden, auf relativ einfache Weise entkräftet werden.

Ein Jugendamt mussten wir darauf hinweisen, dass die Kenntnisnahme von personenbezogenen Daten Dritter durch Verfahrensbeteiligte bei der Akteneinsicht gem. § 25 SGB X als Datenübermittlung anzusehen ist.

Deshalb muss zusätzlich zu § 25 Abs. 3 SGB X noch geprüft werden, ob eine Übermittlungsbefugnis im SGB gegeben ist. Nach § 25 Abs. 3 SGB X ist die Behörde zur Gewährung von Akteneinsicht nicht verpflichtet, wenn berechtig-

te Interessen der anderen Beteiligten oder Dritter eine Geheimhaltung erfordern. Soweit Sozialdaten betroffen sind, wird durch die Vorschriften zum Sozialdatenschutz konkretisiert, wann bestimmte Informationen in diesem Sinne geheim zu halten sind.

Nach § 64 SGB VIII i. V. m. § 69 Abs. 1 Nr. 1 SGB X kommt bei einer Akteneinsicht eine Übermittlung der Sozialdaten zur Erfüllung sozialer Aufgaben in Betracht. Bei der Prüfung von Akteneinsichtsbegehren ist seitens der Jugendämter ein vorsichtiger Umgang mit den Sozialdaten der Beteiligten auch untereinander angeraten.

Die Jugendämter sind verpflichtet, ihre Datenverarbeitungsvorgänge in den Akten vollständig zu dokumentieren. Im Rahmen der Akteneinsicht nach § 25 Abs. 1 SGB X können Sozialdaten anderer Beteiligter zur Kenntnis gegeben werden, soweit dies in den Grenzen von § 25 Abs. 3 SGB X, § 64 SGB VIII und §§ 68 - 77 SGB X zulässig ist.

6.7 Einkommensnachweise

Immer wieder erreichen uns Anfragen über den Umgang mit Einkommensnachweisen bei der Elternbeitragsfestsetzung durch den Träger der Einrichtung.

Nach § 17 Abs. 3 Satz 3 Kindertagesstättengesetz (KitaG) darf der Träger personenbezogene Daten verarbeiten, soweit dies für die Erhebung und Festsetzung der Elternbeiträge erforderlich ist. Welche Daten im Einzelnen benötigt werden, ergibt sich aus den entsprechenden Satzungen sowie aus § 17 Abs. 2 KitaG. Da die Elternbeiträge nach dem Einkommen gestaffelt werden, ist es unabdingbar, das Einkommen der Eltern festzustellen.

Bei der Vorlage von Einkommensnachweisen ist allerdings zu beachten, dass diese Nachweise in der Regel Informationen enthalten, die nicht für die Festsetzung der Elternbeiträge erforderlich sind. So kann einem Steuerbescheid beispielsweise eine etwaige Religionszugehörigkeit entnommen werden. Hinsichtlich dieser Daten müssen die Eltern das Recht haben, diese Angaben zu schwärzen.

Die aus datenschutzrechtlicher Sicht günstigste Lösung besteht darin, dass die zur Festsetzung des Elternbeitrages erforderlichen Angaben über das Einkommen den Nachweisen entnommen werden und darüber ein Aktenvermerk gefertigt wird.

Die eigentlichen Nachweise könnten dann an die Eltern zurückgegeben oder im Falle von Kopien vernichtet werden. Damit würde sowohl der Löschungs-

verpflichtung in § 17 Abs. 3 Satz 4 KitaG als auch der Forderung nach Datensparsamkeit (§ 11b Abs. 2 BbgDSG) Rechnung getragen werden.

Für die Festsetzung des Elternbeitrages ist der Nachweis des Einkommens erforderlich. Die Träger der Einrichtungen müssen jedoch darauf achten, dass die erhobenen personenbezogenen Daten zu löschen sind, wenn sie nicht mehr für die Festsetzung benötigt werden.

7 Wissenschaft, Forschung und Kultur

7.1 Die Chipkarte an der Europa-Universität Viadrina in Frankfurt (Oder)

Bei der Einführung von Chipkarten an den Universitäten ist häufig nicht genau klar, welche Zwecke damit erreicht werden sollen. Während die technischen Möglichkeiten von der universell einsetzbaren Zahlungsfunktion bis zum Einsatz im Personalbereich fast unbegrenzt erscheinen, werden die rechtlichen Probleme sowie die Kosten der Realisierung oft unterschätzt. Nachdem es nicht gelang, sich im Land Brandenburg auf eine einheitliche Lösung zu verständigen, setzte die Europa-Universität Viadrina in Frankfurt (Oder) ein eigenes Chipkartenkonzept um.

An der Europa-Universität wird die Chipkarte in mehreren Phasen eingeführt. Sie dient derzeit als Studierendenausweis und Semesterticket. Darüber hinaus beinhaltet sie eine bankunabhängige Bezahlfunktion und ermöglicht die Rückmeldung von Terminals auf dem Campus. Zu einem späteren Zeitpunkt ist die Aufnahme einer elektronischen Signatur vorgesehen.

Mit den genannten Funktionen unterscheidet sich die Chipkarte hinsichtlich des Umfangs der auf der Karte gespeicherten Daten nur unwesentlich vom traditionellen papierenen Ausweis. Es werden Matrikelnummer und Namen gespeichert; zusätzlich wird ein Lichtbild aufgebracht. Dies ist nach dem Hochschulgesetz zulässig.

Problematischer sind die eingeführten Bezahlfunktionen und die Möglichkeiten, sich mit Hilfe der Chipkarte von bestimmten Terminals Bescheinigungen ausdrucken zu lassen sowie die Rückmeldung und die damit verbundenen Einzahlungen vornehmen zu können. Die Europa-Universität Viadrina hat davon Abstand genommen, die Zahlfunktion mit einer allgemein gültigen Kreditkartenfunktion zu verbinden. Vielmehr beschränkt sie sich auf die Installation eines wiederaufladbaren Chips, der die weiteren Zahlungen (Rückmeldegebühr, Bibliotheksgebühren) ermöglicht. Somit werden nur wenige personenbeziehbare Daten gespeichert, die zudem lediglich innerhalb des geschlossenen Systems der Universität Verwendung finden. Durch die erfolgte (tech-

nische) Abschottung lassen sich zudem die Gefahren des unberechtigten Zugriffs auf die Datenbestände etwa beim Abrufen von Bescheinigungen, die personenbezogene Daten über den Studienverlauf enthalten können, begrenzen. Insgesamt zeigt sich durch die Einführung der Chipkarte eine Möglichkeit, durch eine weitgehende Abkoppelung der Verwaltung von festen Öffnungszeiten für die Studierenden ein Mehr an Service zu verwirklichen und damit letztlich auch Verwaltungsabläufe zu erleichtern.

Gleiches gilt für die Kartenversion, die dem Personal der Universität zur Verfügung gestellt wurde. Diese ist als Zugangskarte und Teil des Zeiterfassungssystems konzipiert, enthält aber selbst nur einen Ident-Datensatz. Die Verarbeitung und Speicherung weiterer personenbezogener Daten (z. B. Arbeitszeit) erfolgt nicht auf der Karte selbst.

Gegenüber universell denkbaren Lösungen bietet der hier umgesetzte Ansatz deutlich geringere Risiken für die Sicherheit der Daten. Die Einführung der weiteren Stufen wird jedoch zu beobachten sein.

Kartentechnologien können durchaus Vorteile für die Beteiligten bringen. Durch ihre gewollte Begrenzung auf einen bestimmten (räumlichen) Bereich lassen sich die sicherheitstechnischen Risiken begrenzen. Dafür sind Einschränkungen hinsichtlich der universellen Verwendbarkeit hinzunehmen.

7.2 Prüfungsergebnisse weltweit – auch mit Nummer nicht nur eine Nummer

Immer wieder taucht die Frage auf, wie Noten von Klausuren so bekannt gegeben werden können, dass sie für Studierende möglichst einfach in Erfahrung zu bringen sind. Dafür bietet sich das Internet an; es birgt jedoch die Gefahr, dass Noten auch solchen Personen zur Kenntnis gelangen, die hiervon nichts erfahren sollen.

Die Zeiten der Präsenz-Universität, in denen sich zum Semesterende noch einmal die Gänge füllten und die Klausur-Noten persönlich in Empfang genommen wurden sind vorbei. Früher wurden die Noten an „Schwarzen Brettern“ bekannt gegeben. Das datenschutzrechtliche Problem, mit dem Makel „nicht bestanden“ versehen zu werden, wurde dahingehend gelöst, dass die Klausurnoten lediglich mit der Immatrikulationsnummer aber ohne den Namen der Prüfungsteilnehmer ausgehängt wurden. Der Rückschluss von der Nummer auf die Person war für Unbefugte somit nicht möglich. Dieses Modell lässt sich nicht ohne Weiteres auf das Internet übertragen: Beim Aushang war es zu aufwändig, die vorhandenen Daten in eine elektronisch auswertbare Datei zu überführen. Damit war das Geheimnis um die Identität von Prüfungsteilnehmern in aller Regel hinreichend gesichert, obwohl jede Note auf-

grund der Immatrikulationsnummer personenbeziehbar war. Die Verwendung des gleichen Merkmals im Internet erlaubt es demgegenüber, alle Noten zusammenzuführen, mithin sich einen Noten- und damit auch Fächerüberblick über eine einer Immatrikulationsnummer zugeordneten Person zu verschaffen. In anderen Zusammenhängen – etwa bei der Vergabe von E-Mail-Adressen oder anderer universitärer Leistungen – besteht häufig eine Verbindung zwischen der konkreten Person und deren Immatrikulationsnummer, sodass über Suchfunktionen leicht ein Zusammenhang zu weiteren im Netz befindlichen Daten der Studierenden herzustellen sein wird. Aufgrund dessen hat die Veröffentlichung von Noten im Internet mit seinen Suchmaschinen und Möglichkeiten der Profilbildung eine deutlich andere Qualität als deren Aushang am Schwarzen Brett.

Fraglich ist, wie die Bekanntgabe der Prüfungsnoten durch die Universitäten datenschutzgerechter, aber mit möglichst geringem Aufwand zu realisieren ist. Der Einsatz von Chipkarten oder Krypto- und Autorisierungsverfahren ist zwar denkbar, doch letztlich mit dem Einsatz erheblicher technischer, personeller und damit auch finanzieller Ressourcen verbunden.

Datenschutzfreundlicher ist es, jede einzelne Klausur zusätzlich mit einer laufenden Nummer zu versehen, die sich die Studierenden merken müssen.

Nach der Korrektur der Aufgaben würde dann die Note der Klausurnummer zugeordnet werden können, während die Verarbeitung der übrigen Daten wie Name und Immatrikulationsnummer im internen Bereich der Prüfungsverwaltung verbleibt. Ins Internet (oder auch wie bisher ans Schwarze Brett) würden dann nur die Nummer der Klausur nebst Note gestellt werden. Eine über diese Einzelprüfung hinausgehende Zusammenfassung von unterschiedlichen Leistungen anhand einer einheitlichen Nummer ist damit unmöglich, da für jede Prüfung neue Nummern vergeben werden.

Diese Lösung bedarf zudem keinerlei Schlüsselverwaltung oder besonderer technischer Sicherungen und verursacht lediglich durch das Herstellen einer zusätzlichen Liste (Nummer der ausgeteilten Klausur und Note) einen geringfügigen, aber vertretbaren Verwaltungsmehraufwand.

Angesichts der Möglichkeiten im Internet per Suchfunktionen alle einer Immatrikulationsnummer zugeordneten und offen ins Netz gestellten Daten, insbesondere auch der Prüfungsleistungen zu kombinieren und sich so ein umfassendes Bild über das Studierverhalten der Betroffenen zu verschaffen, ist das Verwenden der Immatrikulationsnummer statt des Klarnamens kein geeignetes Mittel, Informationen zu anonymisieren. Statt dessen sollten für jede einzelne Klausur Nummern vergeben werden, die einen nur einmaligen Bezug zu einer bestimmten Person haben

7.3 Ewige Bindung der Studierenden an die Universität?

Immer mehr sind Universitäten darauf bedacht, den Kontakt zu ihren „Ehemaligen“ zu halten und legen zu diesem Zweck so genannte „Alumni-Programme“ auf. Sie laden Absolventen ihrer Hochschule zu Veranstaltungen ein oder weisen sie auf andere Aktivitäten – wie z. B. Berufseinsteigerprogramme – hin.

Die Pflege des Kontakts mit den „Ehemaligen“ verlangt die Kenntnis der Adresse der Absolventen und wirft daher ähnliche datenschutzrechtliche Probleme wie in der Werbewirtschaft auf. Was den einen eine liebe Erinnerung an vergangene Studienzeiten ist, wird von anderen als Belästigung empfunden. Die verschiedentlich angetroffene Ansicht, man könne die Datei der Studierenden eines Abschlussjahrgangs für Einladungsschreiben aller Art verwenden und sie zu diesen Zwecken gar an Dritte – Nachwuchsförderer oder Arbeitsvermittler – herausgeben, erscheint schon aus diesem Grunde nicht unproblematisch. Abgesehen von der rein praktischen Erwägung, dass Adressen von ehemaligen Studierenden innerhalb sehr kurzer Zeit nach dem Studium für solche Zwecke unbrauchbar werden, ist eine solche Praxis auch mit dem geltenden Recht nicht vereinbar: Zwar kann insbesondere die Pflege der Beziehungen zu ehemaligen Studierenden durchaus als eine ehrenwerte Tradition angesehen werden, doch bedarf sie des Einverständnisses der Betroffenen. Das gilt um so mehr für die häufig als Fürsorge verstandene Weitergabe von Daten an Agenturen zur „Vermittlung von Jungen Führungskräften“. Auch hier gilt, dass eine gute Idee nicht ohne den Willen der von der guten Tat Bedachten umgesetzt werden darf. Gegen oder ohne den Willen der Absolventen dürfen deren Adressen nach Abschluss des Studiums von der Hochschule nicht mehr verwandt werden. Ihre Aufgabe und damit auch die Befugnis zur Verarbeitung von personenbezogenen Daten endet mit der Aushändigung des Abschlusszeugnisses.

Die Einholung einer Zustimmung ist hier ohne großen Verwaltungsaufwand zu erzielen und könnte mit der Ausgabe der Diplome verbunden werden (ohne dass diese natürlich von der Einwilligung abhängig gemacht werden darf). Dieses hätte zudem den Vorteil, dass nur aktuelle Adressen bekannt gegeben werden und die spätere Quote der unzustellbaren Post gesenkt werden könnte. Allerdings sollte bereits hier deutlich getrennt werden zwischen reiner Kontaktpflege der Hochschule zu ihren Ehemaligen einerseits und der Einholung der Erlaubnis zur Weitergabe von Daten an Dritte andererseits. Denn selbst, wenn man es als Aufgabe der Hochschule ansehen sollte, den Berufseinstieg zu erleichtern, müssen die ehemaligen Studierenden genau einschätzen können, an wen ihre Daten weitergegeben werden.

Die Pflege der Beziehungen der Hochschule zu ihren ehemaligen Studierenden setzt das Einverständnis der Betroffenen voraus.

7.4 Von Forschern und Beforschten

Mitglieder von Forschungsinstituten – gleich ob universitärer oder privater Art – beschäftigen sich mit vielen Projekten, in deren Mittelpunkt die Auswertung personenbezogener Daten steht. Fragebögen, die die intimsten Lebensbereiche ausleuchten oder Gewebeproben, die Aufschluss über gesundheitliche Dispositionen geben sollen, werden ausgewertet und interpretiert. Besteht eine Pflicht zur Duldung solcher Untersuchungen?

Bei der Beurteilung des Verhältnisses von Forschung und Forschungssubjekten ist zunächst zu bemerken, dass beide Seiten sich auf Grundrechte berufen können und somit verfassungsrechtlich geschützte Positionen haben. Einerseits regeln die Grundrechte die Freiheit der Forschung vor staatlichen Eingriffen. Die Wissensermittlung und Forschung sollen frei sein und sich nicht nach politischen Opportunitäten ausrichten müssen sowie teilhaben können an finanziellen Förderungen des Staates. Auf der anderen Seite ist auch das Persönlichkeitsrecht – also das Recht seine eigene Sphäre frei von forschenden Augen anderer zu halten – verfassungsmäßig geschützt. Einen prinzipiellen Vorrang hat keines der beiden Rechte. Nach den Forschungsklauseln der Datenschutzgesetze, so auch der des Brandenburgischen Datenschutzgesetzes (§ 28), dürfen öffentliche Stellen – und damit insbesondere die Universitäten und deren Institute – personenbezogene Daten auch ohne Einwilligung der Betroffenen zu Forschungszwecken verarbeiten. Das verlangt allerdings die Genehmigung durch eine Aufsichtsbehörde, die nur dann erteilt werden darf, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen überwiegt und der Forschungszweck auf andere Art und Weise nicht zu erreichen ist. Eine solche Konstellation ist nur im Ausnahmefall gegeben. Viele Forschungsprojekte sind zudem auf die freiwillige Mithilfe ihrer Probanden angewiesen. Für die Zulässigkeit der Forschung mit personenbezogenen Daten muss daher in den allermeisten Fällen die Einwilligung der Betroffenen eingeholt werden. Sie muss freiwillig und informiert erfolgen, was zugleich voraussetzt, dass umfassend über das Forschungsvorhaben und die geplante Verwendung des personenbezogenen Datenmaterials aufgeklärt wird. Auch ist sie widerrufbar und kann in einem späteren Stadium ohne Angabe von Gründen zurückgenommen werden. Auf Verlangen sind noch vorhandene personenbezogene Daten zu löschen oder zu anonymisieren.

Insbesondere bei soziologischen Studien mit Minderjährigen wird häufig vernachlässigt, dass es neben der Einwilligung „beforschter Minderjähriger“ auch

die der gesetzlichen Vertreter – i. d. R. der Eltern – bedarf. Die Einwilligungen der Minderjährigen und deren Eltern müssen stets beide vorliegen. Es gibt damit auch kein Weisungsrecht der Eltern gegenüber ihren minderjährigen Kindern, an einem Forschungsprojekt teilzunehmen. Auch Lehrkräfte von Bildungseinrichtungen können gegenüber ihren Schülerinnen und Schülern keine Anweisungen treffen. Daher können Minderjährige trotz bestehender Zustimmung ihrer Eltern beispielsweise das Ausfüllen eines Fragebogens im Rahmen einer soziologischen Untersuchung eigenständig verweigern, während umgekehrt eine Teilnahme von Minderjährigen an einer Studie, bei der personenbezogene Daten erhoben werden, ohne die elterliche Zustimmung unzulässig bleibt.

Bei der Durchführung von Forschungsvorhaben innerhalb von Schulen und Klassenverbänden muss zudem immer sichergestellt werden, dass die unterrichtenden Lehrkräfte keinen Einblick in die beantworteten Fragebögen erhalten und an den Diskussionsrunden nicht teilnehmen. Auch dürfen Jugendlichen, die eine Teilnahme an einem Forschungsprojekt verweigern, daraus keine Nachteile erwachsen.

Zur Freiwilligkeit der Teilnahme an einem Forschungsprojekt gehört auch die Möglichkeit der Verweigerung der Teilnahme. Sich selbstbestimmt zu verweigern und sich damit dem forschenden Blick anderer entziehen zu können, ist geradezu das entscheidende Moment der Freiwilligkeit und keineswegs eine Beschränkung der Forschungsfreiheit. Allein die Besorgnis, dass eine Einwilligung verweigert werden könnte oder die, dass der Rücklauf von versandten Fragebögen zu gering ausfällt, macht ein wissenschaftliches Vorhaben weder zu einem solchen von besonderem öffentlichen Interesse, bei dem das Einholen einer Einwilligung nach den Forschungsklauseln entbehrlich wird, noch entbindet es von Aufklärungspflichten, um das Aufkommen von Bedenken zu verhindern. Die Notwendigkeit, die Probanden von der Sinnhaftigkeit eines Vorhabens zu überzeugen und sie zur freiwilligen Mitwirkung zu bewegen, ist vielmehr ein notwendiger Bestandteil der Forschungsvorhaben.

Forschung ohne die freiwillige Einwilligung der Probanden ist in aller Regel unzulässig. Bei Minderjährigen ist zudem die Einwilligung der gesetzlichen Vertreter erforderlich.

8 Arbeit, Soziales, Gesundheit und Frauen

8.1 Soziales

8.1.1 Sozialhilfe

8.1.1.1 Wohnsitzlose auf „Tour de Sozialamt“

Die Mobilität der Wohnsitzlosen führt dazu, dass bei ihnen anders als bei sonstigen Hilfeempfängern nicht an einem bestimmten Ort eine einzige Akte geführt wird, aus der die bereits erbrachten Leistungen hervorgehen. Immer wieder stellen Sozialhilfeträger fest, dass dieser Personenkreis deshalb bei einmaligen Leistungen wie z. B. beim Bezug von Bekleidung, relativ einfach Sozialhilfemissbrauch betreiben kann. Ein Landkreis, der regelrechte Fahrgemeinschaften zur Förderung des Sozialhilfebetruges aufdeckte, wollte sich vor weiteren Schäden durch die Einrichtung einer kreisweiten Datei oder sogar einem kreis- bzw. länderübergreifenden Datenabgleich über einmalige Leistungen an Obdachlose schützen.

Weil die für die Gewährung von Sozialhilfe herangezogenen Gemeinden und Ämter verschiedene datenschutzrechtlich verantwortliche Stellen sind, finden die Übermittlungsvorschriften des Sozialgesetzbuches bei einem Datenabgleich Anwendung. Würden alle Sozialämter eines Landkreises, die eine Leistung an einen Wohnsitzlosen gewährt haben, diese namensbezogen an ein zentrales Register beim Landkreis melden, so wäre dies als Datenverarbeitung auf Vorrat zu bewerten, die gegen das Erforderlichkeitsprinzip verstößt.

Was für Datenübermittlungen innerhalb des Landkreises gilt, gilt selbstverständlich erst recht bei einem Datenabgleich mit anderen Sozialleistungsträgern, sei es in Brandenburg oder gar bundesweit. Anfragen an ein zentrales Register würden meist ohne konkreten Anlass erfolgen und müssten schon deshalb als unverhältnismäßig beurteilt werden: Außerhalb des Sozialhilfedatenabgleichsverfahrens nach dem Bundessozialhilfegesetz und der dazugehörigen Verordnung ist ein regelmäßiger Datenabgleich über den Leistungsbezug nicht zulässig. Damit lassen sich Missbrauchsfälle immer erst im Nachhinein aufdecken.

Bestehen konkrete Anhaltspunkte dafür, dass bereits bei einem bestimmten anderen Sozialamt Leistungen entgegengenommen wurden, die nunmehr erneut beantragt werden, so kann eine Kontaktaufnahme mit diesem Sozialamt zulässig sein, unabhängig davon, ob es im gleichen Kreis oder außerhalb liegt. Es bestünden auch keine Bedenken, beim Landkreis – wie in einem Fall

geschehen – eine Datei zu Leistungen an Obdachlose für den gesamten Kreis zu führen, wenn der Landkreis sich diese Aufgabe in einer Heranziehungssatzung vorbehalten hätte.

Als denkbar haben wir es auch angesehen, personenbezogene Daten wie Name und Geburtsdatum so zu verschlüsseln, dass das vergebene Pseudonym im Einzelfall (bei konkretem Missbrauchsverdacht) aufgehoben und ein Personenbezug hergestellt werden kann.

Eine hundertprozentige Missbrauchsbekämpfung ist – und bleibt – ein Wunschtraum. Jedoch verhindern datenschutzrechtliche Vorgaben nicht eine effektive Missbrauchsbekämpfung.

8.1.1.2 Krankenhilfeabrechnung für Sozialhilfeempfänger durch private Dienstleiter

Das Sozialministerium informierte uns über eine geplante Sozialdatenverarbeitung im Auftrag durch einen örtlichen Träger der Sozialhilfe. Der Auftragnehmer erklärte lediglich, dass die erforderlichen technisch-organisatorischen Maßnahmen gewährleistet würden.

Durch einen anderen Landesbeauftragten für den Datenschutz wurden wir darauf aufmerksam gemacht, dass ausgerechnet der Dienstleister, dessen Mustervertrag uns vorgelegt wurde, im Hinblick auf die getroffenen technisch-organisatorischen Maßnahmen wenig empfehlenswert war. So wurde festgestellt, dass eine abgeschottete Verarbeitung der Sozialdaten der einzelnen Auftraggeber nicht stattfand. Dies führte außerdem zu Zweifeln daran, ob die Datenverarbeitung im Auftrag durch die private Stelle mit der Argumentation zugelassen werden könne, dass sie erheblich kostengünstiger sei. Die Prüfung eines Leistungsangebotes muss berücksichtigen, ob die Kalkulation beim Auftragnehmer nicht ohne die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Sozialdaten vorgenommen wird. Zu bedenken ist bei der Kalkulation auch, dass der öffentliche Auftraggeber außerdem Personalressourcen mit entsprechendem Wissen und Können vorhalten muss, die es ihm erlauben, durch Kontrollen vor Ort die Auftragserledigung durch den Auftragnehmer auf ihre Rechtmäßigkeit und ihre Vereinbarkeit mit der Auftragsvereinbarung tatsächlich zu prüfen. Er muss weiter in der Lage sein, etwa beim Konkurs des Auftragnehmers oder bei einer Kündigung des Auftrages die Aufgaben wieder selbst erledigen zu können.

Die Gewährleistung des technisch-organisatorischen Schutzes für Sozialdaten, die im Rahmen einer Datenverarbeitung im Auftrag einem Auftragnehmer überlassen werden, ist ein wesentlicher Punkt bei der Vereinbarung der Vertragspartner und kann sich auch auf weitere Zulässigkeitsvoraussetzungen auswirken. Hierzu ist mit den Angebotsunterlagen ein Datenschutzkonzept vorzulegen, das eine Beurteilung zulässt, ob die erforderlichen Maßnahmen getroffen werden.

8.1.1.3 Kritischer Blick in Sozialhilfeakten

Stichprobenweise nahmen wir bei einem örtlichen Träger der Sozialhilfe Einsicht in Sozialhilfeakten. In mehreren Fällen wurde in den Unterlagen mehr dokumentiert, als das Sozialamt selbst als erforderlich befand.

Erfreulich für unsere Kontrolltätigkeit war die Übersichtlichkeit der Akten, die nach Sachthemen gegliedert, zugleich aber auch überwiegend paginiert waren.

Entgegen der bereits früher mitgeteilten Absicht waren Personalausweise kopiert worden, obwohl diese Daten wie z. B. ein Bild enthalten, die für die eigentliche Bearbeitung des Sozialhilfeantrags nicht erforderlich sind. Im Rahmen der Identitätsprüfung genügt es, Vermerke über das Ausweispapier, die ausstellende Behörde und den Ausstellungstag zu fertigen. In Zweifelsfällen bleibt dem Sozialamt die Möglichkeit, die Angaben durch einen Abgleich mit der Meldebehörde zu überprüfen.

In einer Akte fanden wir die Kopie eines Mutterpasses mit umfangreichen medizinischen Daten. Das Sozialamt kann sich das Vorliegen einer Schwangerschaft nachweisen lassen, weil sie zu höheren Leistungen berechtigt. Durch die Kopie wurden jedoch wesentlich mehr als die erforderlichen Daten zur Akte genommen. Das Sozialamt hat uns mitgeteilt, dass in Zukunft nur noch die erste Seite des Mutterpasses kopiert werde und darauf ein Vermerk mit Ausstellungsdatum, voraussichtlichem Entbindungstermin, derzeitiger Schwangerschaftswoche und dem feststellenden Arzt gefertigt werde. Medizinische Daten in Mutterpässen, die sich noch in laufenden Sozialhilfeakten befänden, würden entfernt.

Zusammen mit den Sozialhilfeträgern war jeweils eine Ermächtigung zur Einholung von Bankauskünften von den Antragstellern unterschrieben worden. Andererseits war in der Akte dokumentiert, dass entweder Kontoauszüge bereits vorgelegen hatten oder zumindest die Bereitschaft bestand, diese nachzureichen. Die Einholung von Bankauskünften kann jedoch nur dann erforderlich werden, wenn Zweifel an den vom Betroffenen beigebrachten Kontoauszügen bestehen.

In allen Akten befanden sich ungeschwärzte Kopien von Kontoauszügen, die jedoch zum Teil Markierungen aufwiesen, die darauf schließen ließen, dass es dem zuständigen Sachbearbeiter um ganz konkrete Fragestellungen ging, als er die Kontoauszüge anforderte. Die Daten, die für die Arbeit des Sozialamtes nicht relevant sind, müssen jedoch aus der Akte gelöscht werden.

Zum Nachweis einer Scheidung enthielt eine Akte den Prozesskostenhilfeantrag des Ehegatten im Scheidungsverfahren, in dem auch strafrechtlich relevante Vorwürfe gegen diesen erörtert wurden. Es reicht jedoch, die erste Seite des Scheidungsurteiles zu kopieren und darauf Angaben zur Sorgerechtsentscheidung sowie Unterhaltshöhe für die Sachverhaltsaufklärung zu vermerken.

In einem Fall wurde festgestellt, dass das Wohngeld direkt an den Vermieter bezahlt wurde, ohne dass aus der Akte ersichtlich war, wieso diese Verfahrensweise gewählt worden war. Sie kann dann nur in Betracht kommen, wenn der Betroffene dies ausdrücklich wünscht oder wenn Anhaltspunkte dafür bestehen, dass er das Geld anderweitig verwenden würde. So ist auch bei einem Zuschuss für Klassenfahrten von Schulkindern zu verfahren. Der Betrag sollte möglichst direkt an den Sozialhilfeempfänger und nicht an die Schule gezahlt werden. Der Nachweis über die ordnungsgemäße Verwendung kann durch eine dem Sozialhilfeempfänger durch die Schule ausgestellte Quittung erbracht werden.

Darüber hinaus fragte das Sozialamt in einem Formular, ob die anderen Schüler der Klasse an der Fahrt teilnehmen und ob diejenigen Schüler, die nicht teilnehmen, dies aus finanziellen oder sonstigen Gründen tun. Ergänzend wurde um die jeweilige Anzahl der betroffenen Schüler gebeten. Solche Fragen sind nicht erforderlich, weil grundsätzlich jedem hilfebedürftigen Kind die Teilnahme an einer Klassenfahrt zu ermöglichen ist, unabhängig davon, ob und weshalb einzelne Klassenkameraden zu Hause bleiben. Außerdem könnte das Persönlichkeitsrecht der anderen Schüler dadurch verletzt werden.

Das Sozialamt überdachte aufgrund unserer Kritik seine Vorgehensweise nochmals grundlegend und stellte fest, dass viele Datenerhebungen und -speicherungen in den Sozialhilfeakten zur Aufgabenerfüllung nicht erforderlich sind und dass bisherige Verfahren datenschutzgerecht zu gestalten sind.

8.1.2 Sozialversicherung: Kasse lässt Rechnungen durch Dritte prüfen

Anfang 1998 informierte uns eine Krankenkasse über ihr Vorhaben, die Rechnungsprüfung für die Abrechnung mit so genannten „Sonstigen Leistungserbringern“ (Krankengymnasten, Logopäden,...) einer privaten Firma zu übertragen. Um festzustellen, ob eine Funktionsübertragung oder Datenverarbeitung im Auftrag vorliegt, haben wir zusammen mit dem Ministerium des Innern die beauftragte GmbH überprüft.

Bei einer Datenverarbeitung im Auftrag nimmt der Beauftragte aufgrund festgelegter Weisungen lediglich eine unselbständige Hilfstätigkeit wie die bloße elektronische Erfassung personenbezogener Daten aus den Abrechnungsunterlagen in vorgegebene Masken für den Auftraggeber wahr. Letzterer bleibt für die Daten verantwortlich. Bei einer Funktionsübertragung, die eine Übermittlungsbefugnis voraussetzt, werden dem Auftragnehmer dagegen Aufgaben ganz oder teilweise zur selbständigen Erledigung übertragen und er tritt auch nach außen eigenständig auf. Ein solcher „Auftragnehmer“ im zivilrechtlichen Sinne verarbeitet Daten für sich selbst und ist gerade kein Auftragsdatenverarbeiter im Sinne des Datenschutzes.

Um von einer unselbständigen unterstützenden Tätigkeit des Auftragsdatenschützers ausgehen zu können, ist es jedoch auch erforderlich, ihm detailliert vorzuschreiben, was er aufgrund eines Prüfergebnisses im Einzelfall zu veranlassen hat. Nach unserem Hinweis darauf wurde ein Katalog von etwa 200 Prüfkriterien nebst Anweisungen für die Vorgehensweise der Firma je nach dem Ergebnis der Überprüfung entwickelt.

Ein starkes Indiz für eine Funktionsübertragung war, dass die GmbH im Schriftverkehr mit den Leistungserbringern ihre eigenen Briefköpfe verwendete und für Rückfragen auf eine Telefonnummer bei ihrer Hauptverwaltung verwies. Es muss jedoch deutlich werden, dass die GmbH im Auftrag der Krankenkasse handelt. Außerdem darf der Auftragnehmer nur schlichte Erläuterungen seiner Tätigkeit abgeben, inhaltliche Rückfragen sind an die Krankenkasse zu verweisen.

Auch wenn festgestellt wurde, dass insgesamt von einer Datenverarbeitung im Auftrag auszugehen ist, erklärt § 80 Abs. 2 SGB X eine solche Auftragserteilung nur für zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Das Sozialgesetzbuch bestimmt, dass besonders schützenswerte Sozialdaten grundsätzlich nur mit Einwilligung übermittelt werden dürfen. Bei einer Datenverarbeitung im Auftrag steht allerdings keine Übermittlung in Rede, weil die Vertragspartner datenschutzrechtlich als eine Stelle gelten. Die Wahrung der Schweigepflicht nach § 203 StGB ist aber unabhän-

gig davon zu beachten. Selbst wenn man davon ausginge, dass die Datenverarbeitung im Auftrag nach § 80 SGB X eine Befugnis zum Bruch der Schweigepflicht beinhaltete, könnten die Daten bei der privaten Stelle regelmäßig nicht genauso wie beim Auftraggeber geschützt werden. Ein Sozialversicherungsträger ist nämlich nach § 35 Abs. 3 SGB I vor Beschlagnahmen geschützt. Auch bei Ärzten, Zahnärzten, Apothekern und Hebammen, die nach der Strafprozessordnung zeugnisverweigerungsberechtigt sind, besteht nach § 97 Abs. 2 StPO ein Beschlagnahmeverbot, wenn sie die Unterlagen in ihrem Gewahrsam haben. Unterlagen, die die Krankenkassen von diesem Personenkreis erhalten, dürfen daher schon ihrer Art nach nicht in eine Datenverarbeitung im Auftrag bei einer privaten Stelle einbezogen werden, die diesen Beschlagnahmeschutz nicht gewährleisten kann. Dementsprechend hat die Krankenkasse z. B. auch davon abgesehen, die Abrechnung für ambulantes Operieren der Firma zu überlassen.

Die Festlegung der technisch-organisatorischen Maßnahmen zum Schutz der Sozialdaten bei der GmbH wurde auf unsere Veranlassung hin in einem Sicherheitshandbuch an die tatsächlichen Verhältnisse der Firma angepasst.

Mehr und mehr öffentliche Stellen möchten Teile ihrer Datenverarbeitung bei privaten Unternehmen in Auftrag geben. Dabei wird zunächst häufig unterschätzt, wie viel Aufwand für genaue Anweisungen an den Auftragnehmer, Festlegungen aller datenschutzrechtlichen und technisch-organisatorischen Sicherungen für die betroffenen Daten und die Kontrolle der Durchführung der Datenverarbeitung beim Auftragnehmer notwendig ist. Da der Auftraggeber jedoch für den Datenschutz der von ihm stammenden Daten verantwortlich bleibt, hat er sich im Rahmen einer Beauftragung einer Firma all den angesprochenen Fragen möglichst frühzeitig zu stellen.

8.2 Gesundheit

8.2.1 Gesetze und Verordnungen

8.2.1.1 Erste Ergänzungen zum Brandenburgischen Psychisch-Kranken-Gesetz

Ende des Jahres 2000 hatte der Minister für Arbeit, Soziales, Gesundheit und Frauen eine „Unabhängige Kommission Maßregelvollzug im Land Brandenburg“ mit dem Auftrag eingesetzt, den Maßregelvollzug im Land Brandenburg zu untersuchen und konkrete Verbesserungsvorschläge zu unterbreiten[67]. Soweit die Empfehlungen eine Novellierung landesrechtlicher Vorschriften betrafen, sind sie in dem „Gesetz zur Änderung des

[67] vgl. Tätigkeitsbericht 2000, A 8.2.3

Brandenburgischen Psychisch-Kranken-Gesetzes, des Gesetzes über Grundsätze und Vorhaben zur Optimierung der Landesverwaltung und des Krankenhausgesetzes des Landes Brandenburg“[68] berücksichtigt worden.

In der Ergänzung zum Brandenburgischen Psychisch-Kranken-Gesetz wird zunächst die fachliche Verantwortung für den Maßregelvollzug festgelegt. Sie trifft die ärztliche Leitung der Einrichtung. Dies dürfte zur Folge haben, dass sich insoweit selbst die abteilungsleitenden Ärzte gegenüber dem Chefarzt nicht auf ihre ärztliche Schweigepflicht berufen können. Dementsprechend wurde eine Datenverarbeitungsbefugnis zur Erfüllung von Aufsichtsbefugnissen geschaffen. Der beruflichen Schweigepflicht wurde dabei insoweit Rechnung getragen, als Einsicht in Patientenakten für Aufsichtszwecke - aber auch für Kontrollzwecke oder zur Rechnungsprüfung, soweit der Inhalt von Therapiegesprächen betroffen ist, nur durch einen Arzt oder Psychologen erfolgen darf.

Bedenken äußerten wir vor allem gegen eine geplante Vorschrift, die erkennungsdienstliche Maßnahmen der Maßregelvollzugseinrichtungen vorsah. Solche Maßnahmen werden lediglich im Hinblick auf einen Fluchtfall ergriffen und sollen dann der Fahndung dienen. Für die eigene Aufgabenerfüllung der Maßregelvollzugsanstalten war daher eine Erforderlichkeit nicht zu erkennen; selbst im Strafvollzug findet keine generelle erkennungsdienstliche Behandlung statt. Außerdem verfügt die Polizei wegen des vorangegangenen Ermittlungsverfahrens bereits über erkennungsdienstliche Unterlagen, die sie bis zum Ende der Freiheit entziehenden Maßnahme aufzubewahren hat. Keine Einwände bestehen jedoch gegen die jetzt vorgeschriebene Herstellung aktueller Fotos.

Die Einrichtung darf außerdem nunmehr notieren, wer wann welchen Insassen besucht. Die Besucher sind über die Datenverarbeitung zu unterrichten. Verbessert wurden auch die Löschungsregelungen: Nicht nur spätestens nach der Entlassung der untergebrachten Person, sondern jeweils längstens fünf Jahre nach dem Besuch sind die Daten zu löschen.

Unsere Empfehlungen zur Novellierung sind in dem „Gesetz zur Änderung des Brandenburgischen Psychisch-Kranken-Gesetzes, des Gesetzes über Grundsätze und Vorhaben zur Optimierung der Landesverwaltung und des Krankenhausgesetzes des Landes Brandenburg“ berücksichtigt. Es wird deutlich, dass der Schutz der beruflichen Schweigepflichten eine geringere Rolle spielt als in anderen medizinischen Bereichen. Dennoch sind die Patientendaten auch hier so weit wie möglich zu schützen.

[68] v. 6.12.2001, GVBl. I S. 242

8.2.1.2 Einführung von Substitutionsregistern im Betäubungsmittelrecht

Im Berichtszeitraum haben wir zur 15. Verordnung zur Änderung betäubungsmittelrechtlicher Vorschriften Stellung genommen. Der Verordnungsentwurf sah im Rahmen einer Änderung der Betäubungsmittel-Verschreibungsverordnung die Einführung des Substitutionsregisters vor. Durch das Register soll die erforderliche Qualifikation des verschreibenden Arztes geprüft und statistische Auswertungen vorgenommen werden. Vorrangig dient es aber dem Zweck, Mehrfachverschreibungen für einen Patienten zu verhindern. Damit soll zugleich der illegale Handel opiatabhängiger Patienten mit den ihnen verschriebenen Substitutionsmitteln unterbunden werden.

Das Substitutionsregister wird stufenweise eingeführt. Zunächst hat das für die Führung des Registers zuständige Bundesinstitut für Arzneimittel und Medizinprodukte (Bundesinstitut) die organisatorischen Festlegungen zur Führung des Registers zu treffen. Ab dem 1. Juli 2002 werden dann Meldungen an das Register erfolgen und Rückmeldungen vom Bundesinstitut an die verschreibenden Ärzte sowie Mitteilungen des Bundesinstitutes an Überwachungsbehörden, um Mehrfachverschreibungen zu unterbinden, möglich sein. Ab dem 1. Januar 2003 werden Mitteilungen des Bundesinstitutes an die Überwachungsbehörden der Länder aus weiteren Gründen sowie an die obersten Landesgesundheitsbehörden zugelassen.

§ 13 Abs. 3 BtMG sieht Meldungen der verschreibenden Ärzte an das Bundesinstitut über das Verschreiben eines Substitutionsmittels für einen Patienten in anonymisierter Form vor. Die entsprechende Regelung in der Betäubungsmittel-Verschreibungsverordnung bestimmt einen Patientencode, der aus dem ersten und zweiten Buchstaben des Vornamens, dem ersten und zweiten Buchstaben des Familiennamens, „F“ oder „M“ für das jeweilige Geschlecht und der jeweils letzten Ziffer von Geburtstag, -monat und -jahr besteht. Außer dem Patientencode sind im Regelfall das Datum der ersten und letzten Verschreibung sowie Name und Anschrift des verschreibenden Arztes und das Substitutionsmittel zu melden. Bereits aus den erweiterten Initialen kann u. U. ein Personenbezug hergestellt werden. Es liegt keine Anonymisierung vor, allenfalls liegt eine schwache Pseudonymisierung vor. Wir haben es insoweit bedauert, dass der Gesetzgeber, der absehen konnte, dass ein Substitutionsregister mit anonymisierten Angaben nicht funktionieren kann, dies in der Ermächtigungsgrundlage nicht deutlich gemacht hat.

Im Hinblick darauf, dass die übermittelten Daten als personenbeziehbar zu bewerten sind, aber auch wegen des Grundsatzes der Datensparsamkeit

sind die Meldungen auf ein Minimum zu reduzieren. Ursprünglich sollten neben dem Datum der ersten Verschreibung halbjährlich die Patientencodes mitgeteilt werden, für die weiterhin ein Substitutionsmittel verschrieben wird. Das Ende einer Substitution hätte sich daraus nur indirekt ergeben. Wir haben demgegenüber angeregt, das Ende des Verschreibens unverzüglich anzuzeigen. Dies würde zugleich die Aktualität des Registers verbessern. Dieser Kritikpunkt wurde vom Verordnungsgeber aufgegriffen.

Das Bundesinstitut vergleicht die Neueingänge mit den bereits vorhandenen Informationen. Stellt es eine Übereinstimmung fest, so sollte es nach der ursprünglichen Fassung der Verordnung den zuletzt meldenden Arzt unter Angabe des Patientencodes und des zuerst meldenden Arztes auf die Übereinstimmung aufmerksam machen. Der zuletzt meldende Arzt seinerseits sollte das Bundesinstitut darüber in Kenntnis setzen, welcher Arzt die Behandlung fortführt. Erforderlichenfalls kann das Bundesinstitut die zuständigen Überwachungsbehörden der beteiligten Ärzte informieren, um Verschreibungen von Substitutionsmitteln von mehreren Ärzten für einen Patienten zu unterbinden. Ein Einschreiten der Überwachungsbehörde des zuerst meldenden Arztes erschien jedoch nur dann verhältnismäßig, wenn diese die Information auch sicher erhalten hatte. Deshalb geht die Mitteilung des Bundesinstitutes, wie dies auch die Ermächtigungsgrundlage vorsieht, inzwischen an alle beteiligten Ärzte.

Da die Abstimmung der Ärzte untereinander die ärztliche Schweigepflicht berührt, muss der Datenaustausch konkret geregelt werden. Wesentlich erschien uns ein gestuftes Vorgehen der Mediziner. Zunächst sollte geklärt werden, ob die Ärzte tatsächlich denselben Patienten behandeln. Erst wenn dies der Fall ist, kann eine Verständigung dazu denkbar sein, wo der Patient zukünftig behandelt werden soll. Bei der Rückmeldung an das Register war nicht vorgesehen, dass die Meldung unter Übermittlung des Patientencodes erfolgt. Auch war eine Aktualisierung der Angaben beim Register nicht bedacht worden. Sämtliche Kritikpunkte wurden vom Verordnungsgeber aufgegriffen.

Der Verordnungsentwurf forderte zunächst, dass das Bundesinstitut zweimal im Jahr den Ärztekammern Namen und Anschriften der Ärzte mitzuteilen habe, die das Verschreiben von Substitutionsmittel gemeldet hatten. Die Ärztekammern sollten dann unverzüglich diejenigen Ärzte benennen, die die erforderliche Qualifikation nicht erfüllten. Im Gegensatz dazu sah die Ermächtigungsgrundlage im Betäubungsmittelgesetz vor, dass die Ärztekammern dem Bundesinstitut all diejenigen Ärzte melden, welche berechtigt sind, Verschreibungen von Substitutionsmitteln vorzunehmen. Diese Verfahrensweise ermöglicht es dem Bundesinstitut, selbst nichtqualifizierte Ärzte herauszufiltern. Für uns war nicht ersichtlich, welche Vorteile die vom Betäubungsmittelge-

setz abweichende Verfahrensweise in der Verordnung bringen sollte. Wir haben darauf hingewiesen, dass diese Verfahrensweise von der Rechtsgrundlage nicht gedeckt ist. Auch insoweit wurden unsere Bedenken aufgegriffen.

Gerade am Beispiel des Substitutionsregisters mit seinen vielfältigen Datenflüssen, wird deutlich, dass es für die Regelung des gesamten Verfahrens nur von Vorteil ist, genau zu bedenken, welche Daten zu welchem Zweck von welchem der Beteiligten benötigt werden. Die datenschutzrechtliche Kritik hat deshalb auch zu einer deutlichen Verbesserung des Verfahrens geführt.

8.2.2 Heilberufskammern: Anregungen zur Änderung der Berufsordnung der Landesärztekammer Brandenburg

Nach langer Diskussion steht nun die Neufassung der Berufsordnung der Landesärztekammer Brandenburg vor der Veröffentlichung.

Wir hatten der Landesärztekammer verschiedene Änderungsvorschläge gemacht, um die Normenklarheit in der Berufsordnung zu erhöhen. Da unsere Anhörung erst im Nachhinein erfolgte, war jedoch die Bereitschaft, sich mit solchen Vorschlägen auseinander zu setzen, nicht sehr hoch.

Im Wesentlichen beschränkte sich die Diskussion letztlich auf drei Regelungen. Diese betrafen die Offenbarungsbefugnis für Ärzte, das Recht der Patienten auf Akteneinsicht und die Verfahrensweisen bei der Auf- bzw. Übergabe einer Arztpraxis.

Die Berufsordnung sieht vor, dass ein Arzt zur Offenbarung von Patientendaten befugt ist, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Eine Offenbarungsbefugnis aufgrund einer Einwilligung des Patienten ist unproblematisch. Grundsätzlich unbedenklich ist die Offenbarung zum Schutze eines höherwertigen Rechtsgutes. Die konkrete Formulierung ist allerdings sehr eng an einen Rechtfertigungsgrund des Strafgesetzbuches angebunden, ohne jedoch alle seine Voraussetzungen zu berücksichtigen. Zum einen erwähnt die Berufsordnung nicht, dass eine gegenwärtige, nicht anders abwendbare Gefahr für ein Rechtsgut vorliegen muss, außerdem sind beim rechtfertigenden Notstand nicht nur die betroffenen Rechtsgüter abzuwägen, sondern auch der Grad der ihnen drohenden Gefahr, und das geschützte Interesse muss wesentlich überwiegen. Unsere Warnung, dass ein Arzt, der sich für eine Durchbrechung der ärztlichen Schweigepflicht auf die Berufsordnung stützen will, Gefahr läuft, sich dennoch strafbar zu machen, weil er die Voraussetzungen der Rechtfertigungsgründe nicht hinreichend

geprüft hat, fand immerhin insoweit Beachtung als der Text der Berufsordnung nun eine „zwingende“ Erforderlichkeit voraussetzt.

Zum Akteneinsichtsrecht des Patienten enthielt die Berufsordnung die Aussage, dass der Arzt dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren habe. Ausgenommen sollten diejenigen Teile sein, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten. Bereits die höchstrichterliche Rechtsprechung hatte zum Akteneinsichtsrecht für Patienten festgelegt, dass zwar grundsätzlich subjektive Wertungen davon ausgenommen seien. Da Ausnahmen von dieser Regel jedoch denkbar seien, müsse in jedem Fall eine Prüfung dieser Frage stattfinden. Keinesfalls dürfe immer automatisch eine Ablehnung der Akteneinsicht in Dokumentationen subjektiver Eindrücke oder Wahrnehmungen erfolgen. Außerdem wiesen wir darauf hin, dass die Akteneinsichtsrechte in den Datenschutzgesetzen eine Unterscheidung in subjektive und objektive Daten nicht kennen. Nach der zuletzt beschlossenen Fassung sind vom grundsätzlichen Akteneinsichtsrecht der Patienten „in der Regel diejenigen Teile ausgenommen, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten“. Es ist zu befürchten, dass der Ausnahmefall zur Regel wird und nicht mehr geprüft wird, ob tatsächlich Ausnahmen vorliegen.

Der Entwurf der Berufsordnung sah bei einer Praxisaufgabe vor, dass der Arzt seine ärztlichen Aufzeichnungen und Untersuchungsbefunde entweder selbst ordnungsgemäß aufzubewahren oder dafür Sorge zu tragen hat, dass sie in gehörige Obhut gegeben werden. Es ist weiter festgelegt, dass der Arzt, dem bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, diese Aufzeichnungen unter Verschluss halten muss und sie nur mit Einwilligung des Patienten einsehen oder weitergeben darf.

Im Hinblick auf die auch bei Praxisübergabe bestehende ärztliche Schweigepflicht ist eine rein rechtliche Regelung der Thematik nicht ausreichend. Nach der von der Landesärztekammer bevorzugten Formulierung hätte der Arzt, der die Patientenunterlagen übernimmt, zumindest die tatsächliche Möglichkeit, Krankenunterlagen zur Kenntnis zu nehmen. Hier ist jedoch auf den Willen des Patienten als wesentliches Kriterium abzustellen. Im Vorfeld einer konkreten Praxisübergabe müssten die in dieser Zeit behandelten Patienten einbezogen werden. Wir haben daher eine Formulierung vorgeschlagen, die vorrangig auf die Einwilligung der Patienten abhebt, aber auch praktikable Ersatzlösungen ermöglicht. Die Landesärztekammer hat letztlich immerhin in der Berufsordnung klargestellt, dass ein Arzt nach Aufgabe seiner Praxis dafür verantwortlich ist, dass der Geheimnisschutz bezüglich der Patientendaten auch gegenüber einem Praxisübernehmer gewahrt bleibt.

Die langwierige Diskussion um neue Formulierungen in der Berufsordnung der Landesärztekammer Brandenburgs zeigte deutlich, wie schwierig es ist, gewachsene Einstellungen und seit langem praktizierte Verhaltensweisen zu ändern. Dabei erhöhte sich der Widerstand gegen datenschutzrechtliche Verbesserungsvorschläge wohl auch deshalb, weil man es versäumt hatte, uns frühzeitig in den Entscheidungsprozess einzubeziehen.

8.2.3 Krankenhäuser: Kontrollbesuch im Krankenhaus

Im Laufe des Berichtszeitraumes wurde eine Prüfung in einem Krankenhaus durchgeführt.

8.2.3.1 Verträge mit Dienstleistern

Das Krankenhaus hat verschiedene Verträge mit Firmen geschlossen. Diese reichen von der Reinigung der Gebäude über die Wartung des IT-Systems bis zur Pflege von Datenverarbeitungsprogrammen. Zum Teil enthielten die Verträge keinerlei Bestimmungen zum Datenschutz, zum Teil war darauf hinzuwirken, dass auch Subunternehmer an dieselben datenschutzrechtlichen Vorgaben gebunden werden wie der eigentliche Vertragspartner.

8.2.3.2 Formulare

Eine Vielzahl von Formularen wird verwendet; häufig werden Daten erhoben und Einwilligungen zu Datenweitergaben abverlangt, deren Erforderlichkeit unklar ist.

Ein Teil der vom Krankenhaus erhobenen Patientendaten werden an gesetzliche Krankenkassen als Kostenträger übermittelt. Dabei schreibt § 301 Abs. 1 Fünftes Buch Sozialgesetzbuch (SGB V) abschließend vor, welche Daten für die Abrechnung übermittelt werden dürfen. Abweichend von dieser Vorschrift enthielt die Aufnahmeanzeige an die Krankenkassen Angaben zum Arbeitgeber und Beruf des Patienten. Neben Angaben zum Patienten finden sich außerdem Angaben zum Versicherten. Diese Übermittlungen sind in § 301 SGB V nicht vorgesehen und müssen deshalb unterbleiben.

Auf dem Formular für die Geburtsanzeige ist eine „Einwilligung zur Weitergabe personenbezogener Daten“ vorgesehen. Wir haben angeregt, den Eltern bzw. der oder dem Sorgeberechtigten die Möglichkeit einzuräumen, das Einverständnis auf bestimmte Stellen zu beschränken, falls jemand nicht sämtliche aufgezählte Stellen informiert wissen möchte. Problematisiert haben wir auch, dass in eine Übermittlung an „andere interessierte Stellen“ eingewilligt werden kann. Damit wird eine Vielzahl von Möglichkeiten für die Datenüber-

mittlung eröffnet, die für die Betroffenen nicht überschaubar sind. Insoweit ist auch die Wirksamkeit der Einwilligungserklärung insgesamt fraglich.

Das Krankenhaus verwendet ein von der Deutschen Krankenhausgesellschaft entwickeltes Formular mit der Überschrift „Datenübermittlungen an den Hausarzt (§ 73 Abs. 1 b SGB V)“. Entgegen dieser Überschrift soll das Formular auf alle weiterbehandelnden Ärzte Anwendung finden und auch Datenübermittlungen durch den Hausarzt ermöglichen. Die zitierte Vorschrift des Fünften Buches Sozialgesetzbuch bezieht sich allein auf Hausärzte. Für andere Ärzte wäre mithin die Krankenhausdatenschutzverordnung anzuwenden. Nach dieser dürfen Übermittlungen an weiterbehandelnde Ärzte stattfinden, wenn der Patient dem nicht widersprochen hat. Nach dem Sozialgesetzbuch ist dagegen für die Datenübermittlungen eine Einwilligungserklärung des Patienten erforderlich.

Wir gehen davon aus, dass § 73 Abs. 1b SGB V eine zentrale Datensammlung beim Hausarzt auch über einen konkreten Behandlungszusammenhang hinaus ermöglichen will und deshalb dabei die strengeren Voraussetzungen einer Einwilligungslösung einzuhalten sind. Bei einem konkreten Behandlungszusammenhang sehen wir die Vorschrift der Krankenhausdatenschutzverordnung nicht als durch das Sozialgesetzbuch verdrängt an. Dementsprechend ist es nach unserer Auffassung nicht korrekt, das Formular auf andere Ärzte als Hausärzte auszudehnen. Darüber hinaus sollte der Zweck der Übermittlung in der Einwilligungserklärung festgelegt werden.

8.2.3.3 Patientenaufnahme

In der Patientenaufnahme beschäftigt sich jeweils nur eine einzelne Person in einem abgeschlossenen Raum mit einem einzigen Patienten. Diese Gestaltung ist datenschutzgerecht.

Für die Neuaufnahme eines Patienten gibt es Erfassungsbelege in elektronischer und in Papierform. Erscheint der Betroffene direkt bei der Patientenaufnahme, so werden seine Daten unmittelbar in den PC übernommen. Nur in Ausnahmefällen, z. B. bei Notaufnahmen, erfolgt die Erfassung der Daten durch die Patientenaufnahme auf der Station.

Bei der Aufnahme sind die Fragen nach Beruf und Arbeitgeber allenfalls bei Berufsunfällen oder Berufskrankheiten notwendig. Nicht ersichtlich war für uns weiter, wozu Angaben über den Familienstand dienen sollen. Auch Angaben zum Hauptversicherten schienen uns nicht relevant zu sein. Bei Informationen zu den nächsten Angehörigen, zur Konfession und zur Telefonnummer wiesen wir darauf hin, dass der Betroffene vor der Befragung auf die Freiwilligkeit der Angaben aufmerksam zu machen ist. Dabei fanden wir ins-

besondere das Feld „ohne Konfession“ überflüssig. Die Frage nach der Konfession dient allein dem Zweck, dem Patienten einen gewünschten Beistand durch einen Seelsorger seiner Konfession zu vermitteln. Ist er konfessionslos, kann ein solcher Zweck nicht verfolgt werden. Eine Dokumentation der Konfessionslosigkeit ist daher nicht erforderlich.

8.2.3.4 Informationen an der Pforte

Da es bei den Mitarbeitern der Pforte solche mit Sehbehinderungen gibt, existieren zwei verschiedene Tageslisten: Zum einen gibt es einen Ausdruck, der Name, Vorname, Adresse, Station, Aufnahmedatum und Patientennummer enthält, zum anderen können auf dem Bildschirm zu all den Patienten, die sich derzeit im Krankenhaus befinden und einer Auskunft über ihren Aufenthaltsort im Klinikum nicht widersprochen haben, Name, Vorname, Geburtsdatum, Station, Fachabteilung, Aufnahmedatum und Patientennummer angesehen werden.

Bereits die Abweichungen in den Listen zeigen eindrücklich, dass nicht alle Informationen benötigt werden. An der Pforte müssen lediglich Name, Vorname und Station bekannt sein.

8.2.3.5 Poststelle

Datenschutz und ärztliche Schweigepflicht werden in der Poststelle insoweit gewahrt, als ein- und ausgehende Schreiben die Poststelle ungeöffnet passieren und dort auch nicht dokumentiert werden. Anders sieht es bei der innerbetrieblichen Post aus, die regelmäßig – abgesehen von Personalangelegenheiten - unverschlossen in der Poststelle abgegeben und dort auf offene Postfächer verteilt wird. Das Krankenhaus hat bereits bei unserem ersten Besuch mitgeteilt, dass es vor hat, geschlossene Postfächer zu beschaffen. Dies löst jedoch nur einen Teil des Datenschutzproblems im Umgang mit der innerbetrieblichen Post.

Einschreiben und Sendungen, für die die Mitarbeiterin der Poststelle unterschreiben muss, werden dort in Posteingangsbücher eingetragen. Diese Bücher reichen bis ins Jahr 1991 zurück, was zu lang ist. Hierzu muss ein Löschungskonzept erarbeitet werden. Dieses sollte beispielsweise die Chefarztsekretariate einbeziehen, in denen Posteingangs- und -ausgangsbücher für andere Sendungen geführt werden.

8.2.3.6 Archiv

Nach der Krankenhausdatenschutzverordnung sind Patientendaten, die nicht mehr für die aktuelle Bearbeitung durch das Krankenhaus benötigt werden, gesondert zu speichern. Dies geschieht durch die Archivierung. Zur Erschließung der Akten ist im Krankenhausarchiv ein Nachweis zu führen, auf den andere Bereiche nicht direkt zugreifen dürfen. Dies wird u. a. durch die räumliche Abschottung des Archivs erreicht.

Nicht optimal fanden wir es allerdings, dass weder auf der Station noch im Archiv eine Auflistung des konkreten Akteninhaltes oder wenigstens eine Durchnummerierung der Dokumente vorgenommen wird. Dies führt dazu, dass das Archiv sich nicht in der Lage sieht, entsprechend dem Erforderlichkeitsprinzip nur die angeforderten Unterlagen aus einer Akte zu entsperren, sondern stets die gesamte Patientenakte herausgeben muss. Wir haben angeregt, zumindest für die künftig entstehenden Patientenakten eine weitergehende Erfassung des Akteninhaltes vorzunehmen.

Die Zusammenführung aller Daten eines Patienten aus verschiedenen Behandlungszeiträumen durch verschiedene Abteilungen in einer Gesamtakte im Archiv haben wir nur unter der Voraussetzung akzeptiert, dass beim Ausleihen wiederum eine Trennung nach den Fachabteilungen vorgenommen werden kann.

In unserem sechsten Tätigkeitsbericht[69] hatten wir Anforderungen an eine Entsperrung wegen eines medizinischen Sachzusammenhanges formuliert. Die Verantwortung für die Entsperrung lag danach im Wesentlichen bei der anfordernden Abteilung. Das Archiv hat lediglich sicherzustellen, dass eine Begründung im Sinne der Krankenhausdatenschutzverordnung vorliegt oder in Notfällen von der ausleihenden Station nachgereicht wird. Auf eine Sicherstellung der Begründung wird derzeit nicht ausreichend geachtet.

Die Regelungen in der Krankenhausdatenschutzverordnung zur Archivierung und Entsperrung gehen davon aus, dass keine automatische Entsperrung bei einer Wiederaufnahme erfolgen soll. Dementsprechend lässt es das IT-System des Krankenhauses nicht zu, dass die Mitarbeiterinnen der Patientenaufnahme eine Information darüber erhalten, ob ein Patient bereits in dem Krankenhaus behandelt wurde oder nicht.

[69] vgl. 6. Tätigkeitsbericht, 7.2.2.1 Archivierung von Patientenakten, insbesondere S. 111

8.2.3.7 Labor

Das Labor erhält von den Stationen einen Anforderungsschein mit patientenbezogenen Daten und Barcode sowie lediglich mit Barcode versehene Proben. Einzelne Stationen halten es für sicherer, auch auf den Proben handschriftlich Patientendaten zu ergänzen. Dies ist jedoch für das Labor nicht erforderlich. Im Gegenteil kann es sogar dazu führen, dass der Barcode nicht mehr zuverlässig abgelesen werden kann. Insoweit war die datenschutzgerechtere Vorgehensweise, die auf zusätzliche Angaben verzichtet, dem Krankenhaus auch aus haftungsrechtlichen Gründen dringend zu empfehlen.

Bei der Vergabe von Laborarbeiten an externe Einrichtungen werden wenige Patientendaten mitgeteilt. Auch insoweit haben wir empfohlen, über eine anonymere Gestaltung des Anforderungsscheines nachzudenken. Zumindest fordert die Krankenhausdatenschutzverordnung aber bei diesen Übermittlungen, dass der Patient auf eine geplante Übermittlung und sein Widerspruchsrecht dagegen hinzuweisen ist.

In Ausnahmefällen trägt das Labor in die Gerätelisten neben den Nummern der untersuchten Personen deren Namen ein. Damit soll bei Patienten mit extremen Werten eine bessere Plausibilitätskontrolle möglich sein. Wir haben das Krankenhaus darauf aufmerksam gemacht, dass diese Verfahrensweise bei Wartungs- oder Reparaturarbeiten dazu führen könnte, dass Patientendaten von Dritten zur Kenntnis genommen werden können. Personenbezogene Angaben sollten deswegen am besten gar nicht oder jedenfalls nur so in die Gerätelisten aufgenommen werden, dass sie einfach, aber sicher wieder entfernt werden können.

Der Leiter des Labors vertrat die Auffassung, dass er bei der namentlichen Meldung eines Krankheitserregers verpflichtet sei, auch die Anschrift des Hauptwohnsitzes des Patienten an das Gesundheitsamt mitzuteilen. Dies entspricht jedoch nicht dem Infektionsschutzgesetz. Dieses macht im Zusammenhang mit der Angabe der Adresse des Patienten durch den Zusatz „soweit die Angaben vorliegen“ deutlich, dass diese Angabe nicht zwingend ist. Wir haben deshalb empfohlen, auf Rückfragen bei der behandelnden Station zur Adresse des Patienten in diesen Fällen zu verzichten. Durch die parallele Meldepflicht der behandelnden Ärzte des Krankenhauses erhält das Gesundheitsamt dieses Datum auf jeden Fall.

8.2.3.8 Sozialer Dienst

Es entspricht den gesetzlichen Vorgaben, dass der Soziale Dienst, wenn er von einem hilfsbedürftigen Patienten erfahren hat, zunächst den Kontakt unmittelbar mit dieser Person sucht und nur dann, wenn der Patient eine Unter-

stützung wünscht, die Kommunikation mit der behandelnden Station, Kostenträgern oder sonstigen Stellen aufnimmt. Allerdings bewegen sich die Meldenden und der Soziale Dienst in einer datenschutzrechtlichen Grauzone, wenn der Soziale Dienst aufgrund des Hinweises einer anderen Person auf einen normalen geschäftsfähigen Patienten zugeht, ohne dass dieser selbst Unterstützung gefordert hatte.

Der Soziale Dienst erklärte, dass er für Angehörige Visitenkarten bei dem hilfebedürftigen Patienten hinterlasse. Notfalls nehme er jedoch auch Akteneinsicht in die Patientendokumentationen, um Angehörige ausfindig zu machen. Eine Akteneinsicht allein aus diesem Grund halten wir jedoch nicht für erforderlich. Die Klärung einer so scharf umrissenen Frage muss entweder mit Hilfe des Patienten oder anderer Mitarbeiter des Krankenhauses möglich sein. Allein dafür einen Einblick in sämtliche medizinische Dokumentationen zu eröffnen, erschiene unverhältnismäßig.

Der Soziale Dienst nimmt nicht an Chefarztvisiten teil, sondern macht eigene Rundgänge zu den hilfsbedürftigen Patienten. Wir haben diese am Erforderlichkeitsprinzip orientierte Verfahrensweise begrüßt. Zu den Besuchen des Sozialen Dienstes in den Patientenzimmern haben wir allerdings ausdrücklich darauf hingewiesen, dass dafür Sorge zu tragen ist, dass Patienten nicht dazu gedrängt werden, sich vor anderen (z. B. Zimmergenossen, Besuchern) zu offenbaren. Nicht unproblematisch ist es deshalb auch, dass sich die beiden Mitarbeiter des Sozialen Dienstes ein Zimmer teilen. Einzelgespräche mit Patienten sind nur möglich, wenn der andere Kollege den Raum verlässt. Jedem der beiden Mitarbeiter sollte ein Einzelzimmer zur Verfügung gestellt werden.

Derzeit werden die Dokumentationen des Sozialen Dienstes zwei Jahre lang im Arbeitsraum des Sozialen Dienstes aufbewahrt. Dies widerspricht den Regelungen der Krankenhausdatenschutzverordnung über die Sperrung und Archivierung im Krankenhausarchiv.

8.2.3.9 Innerorganisatorische Maßnahmen zum Datenschutz

Bei unserem ersten Besuch stellten wir fest, dass im Krankenhaus kein behördlicher Datenschutzbeauftragter bestellt war. Unsere Kritik daran führte zur Auswahl eines Mitarbeiters für diese Tätigkeit. Zugleich überlegte das Krankenhaus aber auch, diese Aufgabe zusätzlich noch durch einen externen Dienstleister erledigen zu lassen. Dies hätte jedoch dem Brandenburgischen Datenschutzgesetz widersprochen. In öffentlichen Stellen darf lediglich ein Bediensteter dieser oder einer anderen öffentlichen Stelle Datenschutzbeauftragter sein. Außerdem genügt für eine Daten verarbeitende Stelle ein einziger Datenschutzbeauftragter. Das Krankenhaus hat diesen Hinweis umgehend berücksichtigt.

Auch eine Dienstanweisung zum Datenschutz gab es nicht. Lediglich der Umgang mit PC's und Terminals war in einer Dienstanweisung geregelt. Das Krankenhaus hat zugesagt, umfassendere Dienstanweisungen zu erarbeiten.

Die Kontrolle einer öffentlichen Stelle durch den Landesdatenschutzbeauftragten soll zum einen datenschutzrechtliche Verbesserungen bewirken, zum anderen kann sie der betroffenen Stelle aber auch eine Bestätigung für datenschutzgerechte Verfahren sein.

Die Anbieter von Krankenhausinformationssystemen und Formularen sind zum Teil für einen unzureichenden Datenschutzstandard mit verantwortlich. In diesem Bereich deckten sich auffallend viele Mängel mit den Feststellungen bei der vorangegangenen Prüfung eines anderen Krankenhauses. Wir können allen Krankenhäusern daher nur empfehlen, an solche Angebote kritischer heranzugehen und ggf. vor einem Vertragsschluss unsere Stellungnahme einzuholen.

8.2.4 Landeskliniken: Regelmäßige Telefonüberwachung im Maßregelvollzug?

Eine Landesklinik installierte eine Telekommunikationsanlage, mit der Telefonate von Patienten im Maßregelvollzug nur nach Freischaltung durch das Klinikpersonal geführt werden können. Zum Einsatz sollen dabei Telefonkarten mit PIN-Nummern kommen. Der Patient kann die Telefonkarten aufladen und soll zukünftig per Knopfdruck den Kontostand abrufen können. Das Telefonkonto für die Karten wird auf einem Rechner geführt. Dazu werden Datum, Gesprächsdauer und die angerufene Telefonnummer gespeichert. Die Betroffenen erhalten darüber keinen Ausdruck; lediglich bei Beschwerden kann die Richtigkeit der Abbuchungen durch die Speicherungen notfalls überprüft werden.

Die Anlage ermöglicht Abhörmaßnahmen sowie die Aufzeichnung von Telefongesprächen. Auf eine Gesprächsüberwachung werden die Gesprächspartner durch ein akustisches Signal aufmerksam gemacht.

Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hatte die Auffassung vertreten, dass das Aufzeichnen und Speichern von Telefongesprächsinhalten unter engen Voraussetzungen nach §§ 24, 25 BbgPsychKG zulässig sei. Eine Speicherung der Telefonverbindungsdaten wollte es nach einer allgemeinen Datenverarbeitungsvorschrift in dem Gesetz immer dann zulassen, wenn die rechtmäßige Aufgabenerfüllung dies erfordere.

Wir vertreten demgegenüber die Auffassung, dass die spezielle Regelung zur Überwachung von Telefongesprächen sowohl den Gesprächsinhalt als auch die Verbindungsdaten betreffen kann, während die allgemeine datenschutzrechtliche Regelung im Brandenburgischen Psychisch-Kranken-Gesetz nicht auf die Besonderheiten der Telefonüberwachung abgestimmt ist. Das Mitschneiden eines Telefonats sehen wir jedoch nicht als von Vorschriften des Gesetzes gedeckt an.

Somit ist nach unserer Auffassung nur in Einzelfällen unter engen Voraussetzungen eine Telefonüberwachung im Maßregelvollzug zulässig. Dies schließt das regelmäßige Aufzeichnen von Verbindungsdaten aus. Eine pauschale Speicherung der Verbindungsdaten lässt sich auch nicht auf andere Vorschriften stützen. Wiederum lediglich im Einzelfall könnte nach der Telekommunikations-Datenschutzverordnung mit Einwilligung des betroffenen Patienten eine Speicherung erfolgen. Selbstverständlich dürfte dann die Möglichkeit des Telefonierens nicht nur nach dem Erklären einer solchen Einwilligung gewährt werden.

Im Strafvollzugsgesetz ist ausdrücklich bestimmt, dass die Entscheidung über die Einschränkung des Besuchsrechts und des Rechts auf Schriftwechsel und entsprechend für Ferngespräche und Telegramme jeweils dem Anstaltsleiter obliegen. Eine ähnliche Festlegung im Brandenburgischen Psychisch-Kranken-Gesetz hätten wir begrüßt. Diese Hinweise wurden bei der Novellierung des Psychisch-Kranken-Gesetzes jedoch nicht aufgegriffen.

Wir teilten dem Landesamt für Soziales und Versorgung mit, dass eine Telefonüberwachung durch die Bediensteten des Maßregelvollzugs nur in Einzelfällen unter den Voraussetzungen des Brandenburgischen Psychisch-Kranken-Gesetzes stattfinden dürfe und dass darunter auch lediglich ein Mithören, nicht aber ein Mitschneiden des Gespräches zu verstehen sei. Unabhängig davon ist die Landesklinik verpflichtet, bei Vorliegen einer richterlichen Anordnung Maßnahmen der Telefonüberwachung durch die Strafverfolgungsbehörden zu ermöglichen[70].

Das novellierte Brandenburgische Psychisch-Kranken-Gesetz geht zwar im Hinblick auf die Abhörbefugnisse im Maßregelvollzug über die Befugnisse für den Strafvollzug hinaus. Dennoch dürfen Bedienstete der Vollzugseinrichtung Telefonate von Patienten lediglich mithören, nicht aber aufzeichnen.

[70] s. dazu oben A 1.3

9 Landwirtschaft, Umweltschutz und Raumordnung

9.1 Neues Umweltinformationsgesetz

Der Bundesgesetzgeber hat mit dem am 3. August 2001 in Kraft getretenen novellierten Umweltinformationsgesetz nunmehr den europäischen Vorgaben Rechnung getragen[71] und damit zugleich die Zugangsrechte der Bürgerinnen und Bürger erweitert.

Umweltinformationen dürfen nicht weitergegeben werden, wenn schützenswerte private oder öffentliche Interessen dem entgegenstehen. Das neue Gesetz bestimmt jedoch, dass die nicht schützenswerten Informationen derselben Akte oder Datei offen zu legen sind.

Neu ist auch, dass das Umweltinformationsgesetz – weitergehend als das Akteneinsichts- und Informationszugangsgesetz – in „normalen“ Verwaltungsverfahren anwendbar ist. Strafrechtliche oder ordnungsbehördliche Ermittlungs- und Disziplinarverfahren sind ausgenommen. Hier besteht weiterhin kein Informationsanspruch.

Im Gegensatz zum bisherigen Rechtszustand ist jetzt die Ablehnung eines Antrags auf Zugang zu Umweltinformationen kostenlos. Die abschreckende Wirkung einer Gebührenpflicht auf mögliche Interessenten wird auch dadurch vermieden, dass die neue Umweltinformationskostenverordnung des Bundes die Möglichkeit eröffnet, von der Gebührenerhebung ganz abzusehen, wenn dies aus Gründen des öffentlichen Interesses oder der Billigkeit geboten ist.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hält eine Broschüre mit dem Text des novellierten Umweltinformationsgesetzes mit Kostenregelungen zum Versand bereit.

9.2 BSE – Landwirte und Wursthersteller bangen um ihren Namen

Die Rinderseuche BSE warf neben vielen anderen auch datenschutzrechtliche Fragen auf. Sollten beispielsweise die Namen von Wursthersstellern bekannt gegeben werden, die unzureichende Angaben darüber machten, ob ihre Erzeugnisse Rindfleisch enthalten? Wir hatten auch zu prüfen, ob Landwirte öffentlich genannt werden dürfen, deren Rinderbestand von BSE betroffen ist.

[71] s. Tätigkeitsbericht 1999, A 10.1

Brandenburg gehört zu den Bundesländern, in denen eine Information der Öffentlichkeit bei falsch deklarierten Wurstwaren nur unter ganz bestimmten Voraussetzungen zulässig ist. Falsch deklarierte Wurstwaren werden nach dem Lebensmittel- und Bedarfsgegenständegesetz des Bundes beanstandet, weil die Erzeugnisse mit zur Täuschung geeigneter Bezeichnung, Angaben, Aufmachungen bzw. Darstellungen in den Verkehr gebracht wurden. Die zuständige Behörde ist nach dem Brandenburgischen Ausführungsgesetz[72] berechtigt, bei begründetem Verdacht der Gefährdung von Leben und Gesundheit die Öffentlichkeit unter Angabe der Produktbezeichnung und des Produzenten zu warnen. Eine Warnung kann auch in anderen Fällen erfolgen, wenn ein besonderes öffentliches Interesse besteht. Der Hersteller oder Importeur ist zwar zu hören, soweit dies nicht die Erreichung des angestrebten Zwecks gefährdet. Von dieser Warnbefugnis wurde bisher jedoch kein Gebrauch gemacht.

Zu der Frage nach der öffentlichen Nennung der Landwirte, in deren Rinderbestand BSE aufgetreten ist, haben wir die Auffassung vertreten, dass mangels Rechtsgrundlage Landwirte im Falle des Auftretens von BSE in der Regel nicht öffentlich genannt werden dürfen.

Zwar ist der Ausbruch einer Seuche öffentlich bekannt zu machen (§ 30 Tierseuchengesetz). Die Veröffentlichung darf jedoch nur die Tatsache, dass und welche Seuche in welcher Gemeinde sowie die im Einzelfall getroffenen seuchenrechtlichen Maßnahmen umfassen. Eine namentliche Nennung der Landwirte könnte allenfalls in Betracht kommen, wenn es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist (§ 16 Abs. 1 b i. V. m. § 13 Abs. 2 d Brandenburgisches Datenschutzgesetz). Sollten im Einzelfall diese Tatbestandsvoraussetzungen erfüllt sein, wird der betroffene Landwirt den mit der Veröffentlichung seines Namens verbundenen Grundrechtseingriff hinnehmen müssen.

Dass Namen von Landwirten ohne Zutun öffentlicher Stellen bekannt werden, ist nicht auszuschließen, z. B. wenn in einer Gemeinde nur ein landwirtschaftlicher Betrieb ansässig ist. Soweit landwirtschaftliche Betriebe juristische Personen des Privatrechts sind, können sie sich dagegen ohnehin nicht auf das Brandenburgische Datenschutzgesetz berufen.

Es bleibt abzuwarten, ob das vom Bundesministerium für Verbraucherschutz angekündigte Verbraucherinformationsgesetz die Möglichkeit herstellerbezogener Warnmeldungen zugunsten der Verbraucher erweitern wird.

---

[72] Gesetz zur Ausführung des Lebensmittel- und Bedarfsgegenständegesetzes des Landes Brandenburg i. d. F. der Bekanntmachung v. 17.12.2001, GVBl. 2002 I S. 10

Eine öffentliche Nennung von Wurstherstellern und Landwirten ist bisher nur unter bestimmten rechtlichen Voraussetzungen im Einzelfall möglich.

9.3 Der neugierige Nachbar – Offenlegung von Daten im Bodenordnungsplan

Im Rahmen der Bekanntmachung des Bodenordnungsplanes fühlte sich ein Petent durch die Auflistung seines Namens und seiner Rechtsposition sowohl im Beteiligtenverzeichnis als auch im Teilnehmernachweis in seinem Recht auf informationelle Selbstbestimmung verletzt. Jeder am Bodenordnungsverfahren Beteiligte konnte auf diese Weise Name, Anschrift, Geburtsdatum und die jeweiligen Eigentumsverhältnisse anderer Beteiligter zur Kenntnis nehmen.

Bei der Bekanntgabe des Bodenordnungsplanes nach § 59 Landwirtschaftsanpassungsgesetz ist zu beachten, dass jeder Beteiligte nur die Informationen über das Bodenordnungsverfahren erhält, die ihn selbst etwas angehen. Im Fall des Petenten ist diese Maßgabe nicht in vollem Umfang eingehalten worden. Den Beteiligten hätte das vollständige Beteiligtenverzeichnis nicht zugänglich gemacht werden dürfen, weil sich hieraus schutzwürdige Informationen über die Rechtsstellung von (beschränkt) dinglich Berechtigten ableiten lassen.

Das Ministerium für Landwirtschaft, Umwelt und Raumordnung hat den Fall zum Anlass genommen, die Ämter allgemein auf die Einhaltung des Brandenburgischen Datenschutzgesetzes und im besonderen darauf hinzuweisen, dass das Beteiligtenverzeichnis den Beteiligten nicht zugänglich zu machen ist. Danach erhält der Teilnehmer eines Bodenordnungsverfahrens nach § 56 i. V. m. § 64 Landwirtschaftsanpassungsgesetz gem. § 59 Abs. 3 Flurbereinigungsgesetz einen (nur) ihn betreffenden Auszug aus dem Bodenordnungsplan. Dieser beinhaltet – außer dem Textteil – einen Teilnehmernachweis, Nebenbeteiligtennachweis, Wertermittlungsnachweis, Abfindungsnachweise sowie die Bodenordnungskarten. Keinesfalls werden, so teilte uns das Ministerium mit, einem Teilnehmer die im Grundbuch eingetragenen Belastungen oder die Abfindungsnachweise (Ausgleiche und Entschädigungen) eines anderen Teilnehmers zur Kenntnis gegeben.

Im Bodenordnungsverfahren ist darauf zu achten, dass bei der Bekanntgabe des Bodenordnungsplanes den Beteiligten nicht die vollständigen Beteiligtenverzeichnisse zugänglich gemacht werden dürfen.

10 Finanzen

10.1 Bleibt die eigene Steuerakte ein Geheimnis?

Ein Steuerpflichtiger beantragte Einsicht seiner eigenen Steuerakte. Das Finanzamt lehnte seinen Antrag unter Hinweis auf die §§ 91 und 364 Abgabenordnung (AO) ab.

Das Finanzamt hat den Antrag insoweit richtig beschieden, als ein Akteneinsichtsanspruch aus der Abgabenordnung tatsächlich nicht herzuleiten ist. Allerdings ist das Brandenburgische Datenschutzgesetz (§ 18 BbgDSG) anwendbar. Ein Anspruch auf Akteneinsicht bzw. Auskunft gegenüber Behörden ist inzwischen nicht nur auf Grund der Datenschutzgesetze und der EG-Datenschutzrichtlinie (vgl. dort Artikel 12) so weitgehend anerkannt, dass es im Interesse eines gleichmäßigen Datenschutzes in allen Bereichen nicht mehr vertretbar ist, ihn dem Steuerpflichtigen gegenüber der Finanzverwaltung von vornherein vollständig vorzuenthalten. Wir haben das Finanzamt zudem auf Artikel 11 Abs. 1 Satz 1 der Landesverfassung und die Charta der Grundrechte der Europäischen Union hingewiesen, die in Artikel 8 Satz 3 festlegt, dass jede Person das Recht hat, Auskunft über die sie betreffenden erhobenen Daten zu erhalten.

Der Bundesgesetzgeber bleibt daneben aufgefordert, die Abgabenordnung um die verfassungsrechtlich gebotenen datenschutzrechtlichen Regelungen zu ergänzen.

Die Abgabenordnung sieht einen Akteneinsichtsanspruch für den Betroffenen nicht vor. Dennoch sollte die Finanzverwaltung gerade auch vor dem Hintergrund der EU-Datenschutzrichtlinie und der Grundrechte-Charta der Europäischen Union Informationen aus der „eigenen“ Steuerakte zugänglich machen.

10.2 Fragebogen für das steuerliche Absetzen von PC

Um die berufliche Nutzung eines privaten Personalcomputers steuerlich berücksichtigen zu können, erhielt ein Steuerpflichtiger vom Finanzamt einen Fragebogen zugesandt, mit dem er aufgefordert wurde, einen Ausdruck des Inhaltsverzeichnisses der Festplatte mit allen Unterverzeichnissen beizufügen.

Das Finanzamt ist hier zu weit gegangen. Nach § 93 Abs. 1 Satz 1 Abgabenordnung (AO) und dem ergänzend heranzuziehenden § 12 Brandenburgisches Datenschutzgesetz (BbgDSG) hat der Steuerpflichtige dem Finanzamt

die erforderlichen Auskünfte zu erteilen. Unseres Erachtens wird der Grundsatz der Erforderlichkeit hier nicht gewahrt.

Die Darstellung der Verzeichnisse ist nicht geeignet, den Umfang der beruflichen und privaten Nutzung des PC festzustellen. Die Namen der Verzeichnisse sind frei wählbar und lassen keinerlei Rückschlüsse auf die Art und den Umfang der in ihnen vorhandenen Dateien und Anwendungen zu. Es wäre für den Steuerpflichtigen ohne Weiteres möglich, auch private Verzeichnisse so zu benennen, dass sie einen beruflich genutzten Eindruck erwecken. Hinzu kommt, dass der Steuerpflichtige sämtliche privat genutzten Dateien auch auf mobilen Datenträgern (Diskette, CD-ROM usw.) speichern könnte, sodass auf der Festplatte neben den für den Betrieb des PC notwendigen Dateien nur noch Verzeichnisse gespeichert wären, die aus beruflichem Anlass angelegt wurden.

Darüber hinaus ist der Ausdruck aller Verzeichnisse auch nicht verhältnismäßig, da der Steuerpflichtige u. U. auch sensible persönliche Informationen mit der geforderten Übersicht gegenüber dem Finanzamt preisgeben würde. Der Zweck der Feststellung der beruflichen Nutzung eines privaten PC kann solche weit gehenden Eingriffe in das Recht auf informationelle Selbstbestimmung nicht rechtfertigen.

Dem Finanzamt haben wir empfohlen, auf die generelle Anforderung eines Ausdruckes aller auf der Festplatte gespeicherten Verzeichnisse zu verzichten. Die zuständige Oberfinanzdirektion hat dazu mitgeteilt, dass das Finanzamt die Anforderungen an die Nachweisführung/Glaubhaftmachung deutlich reduziert hat. Nur wenn Zweifel an dem vom Steuerpflichtigen benannten Umfang der beruflichen Nutzung bestehen, beabsichtigt das Finanzamt, Nachweise vom Steuerpflichtigen anzufordern. Dazu soll dann ausnahmsweise auch die Vorlage von Verzeichnissen der Festplatte dienen.

Die Datenerhebung durch die Finanzämter ist nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich, geeignet und angemessen ist. Auskünfte über sämtliche auf einem privat und beruflich genutzten PC vorhandenen Verzeichnisse erfüllen diese Kriterien nicht.

10.3 „Vollstreckungsbehörde“ im Absenderstempel

Ein Bürger fühlte sich „an den Pranger gestellt“ und fürchtete zugleich eine gesellschaftliche Diskriminierung, weil er von der Stadtverwaltung eine Postsendung mit dem Absenderstempel „Vollstreckungsbehörde Stadtkasse“ erhielt.

Der betroffenen Stadtverwaltung haben wir zu bedenken gegeben, dass ein solcher Absenderstempel Rückschlüsse auf die persönlichen Verhältnisse des Adressaten zulässt. Der Bürger sah sich zu Recht in seinen Persönlichkeitsrechten verletzt. Bei der Versendung dieser Post kann nicht ausgeschlossen werden, dass Dritte (Postbedienstete, Nachbarn) unberechtigter Weise Kenntnis hiervon erlangen. Dies bedeutet einen Eingriff in das Persönlichkeitsrecht des Empfängers. Aus diesem Grund haben wir der Stadtverwaltung geraten, eine neutrale Absenderangabe ohne den Zusatz „Vollstreckungsbehörde“ zu wählen. Diese Absenderangabe kann um ein Sachbearbeiter- oder Stellenzeichen ergänzt werden, das den Rücklauf von unzustellbaren Schreiben innerhalb der Stadtverwaltung sicherstellt.

Weil nicht ausgeschlossen werden kann, dass Post in die Hände Dritter gelangt, sind die Verwaltungen gehalten, eine neutrale Absenderangabe zu wählen.

10.4 Auskunftsersuchen im bargeldlosen Zahlungsverkehr

Sind Sparkassen berechtigt oder verpflichtet, im Rahmen des bargeldlosen Zahlungsverkehrs Namen und Anschriften der Kunden, deren Zahlungen nicht erfolgten, an Händler bzw. Inkasso-Unternehmen herauszugeben?

Grundsätzlich sollten Daten immer beim Betroffenen erhoben werden, sodass es zunächst Sache des Händlers wäre, die Daten bei seinen Kunden selbst zu erheben. Bei den derzeit auf dem Markt befindlichen gängigen Verfahren ermächtigt der Kunde beim Zahlen mit der EC-Karte allerdings regelmäßig seine Bank, im Falle der Nichteinlösung Namen und Anschrift dem Händler mitteilen zu dürfen.

Dieses Verfahren ist aus datenschutzrechtlicher Sicht der direkten Erhebung durch den Händler vorzuziehen, da es dem Prinzip der Datenvermeidung und Datensparsamkeit nach § 3 a Bundesdatenschutzgesetz (BDSG) besser Rechnung trägt. So ist sichergestellt, dass der Händler nur dann personenbezogene Daten seiner Kunden erhält, wenn er seine Forderungen nicht einziehen kann. Würde er hingegen gezwungen, bei jeder Zahlung mittels EC-Karte Name und Anschrift des Kunden zu erheben, würde er eine Reihe von personenbezogenen Daten auf Vorrat speichern, die er in den meisten Fällen nie benötigen wird. Die notwendige Transparenz der Verarbeitung seiner personenbezogenen Daten kann durch die Einwilligung des Kunden hergestellt werden.

Eine Verpflichtung der Sparkasse, Daten des Kunden an den Händler zu übermitteln, lässt sich dem Datenschutzrecht hingegen nicht entnehmen.

Diese könnte nur durch entsprechende vertragliche Vereinbarungen zwischen Händler, Bank und Kunden begründet werden.

Die Kreditinstitute sind im bargeldlosen Zahlungsverkehr nur mit Einwilligung des Kunden berechtigt, deren Namen und Anschrift an Händler herauszugeben.

Teil B

Akteneinsicht und Informationszugang

Das Grundrecht aller Bürgerinnen und Bürger auf Zugang zu amtlichen Unterlagen wird zunehmend in Europa und allmählich auch in der Bundesrepublik Deutschland zumindest auf der Ebene der Rechtssetzung anerkannt. Damit wird ein wichtiger Schritt in Richtung auf mehr Transparenz der öffentlichen Verwaltungen getan, den das Land Brandenburg vor vier Jahren mit der Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes vollzogen hat. Rechtliche Regelungen allein verändern aber eine Verwaltungskultur erst dann, wenn sie mit Leben erfüllt werden. Das geschieht zunehmend.

1 Entwicklung des Informationsrechts

1.1 Europa

Seit dem 3. Dezember 2001 ist die Verordnung des Europäisches Parlaments und des Rates in Kraft, die den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission regelt[73]. Diese Verordnung entfaltet unmittelbare Rechtswirkung in allen Mitgliedstaaten, sodass auch jeder in Deutschland und in Brandenburg sich auf diese Verordnung berufen kann. Adressaten sind zwar in erster Linie die europäischen Institutionen, deren Dokumente grundsätzlich allgemein zugänglich gemacht werden müssen. Die Europäische Kommission hat hierzu einen Leitfaden für Bürger entwickelt, der auch im Internet abgerufen werden kann und helfen soll, die umfangreichen Informationsbestände der EU-Kommission zu erschließen[74].

Auf diese Europäische Transparenzverordnung können sich Bürgerinnen und Bürger in Deutschland auch gegenüber deutschen Behörden berufen, wenn EU-Dokumente dort vorliegen und eingesehen werden sollen. Die Verordnung verpflichtet die Mitgliedstaaten und ihre Behörden nur in den Fällen, in denen unklar ist, ob das betreffende Dokument verbreitet werden muss oder nicht verbreitet werden darf, die europäische Institution zu konsultieren, von der das Dokument stammt. In allen Fällen, in denen derartige Dokumente zweifelsfrei zugänglich gemacht werden können, hat der Bürger einen direkten Anspruch auf Einsicht gegenüber der deutschen Dienststelle (Artikel 5 der Verordnung). Das nationale Recht und damit auch das Brandenburgische Akteneinsichts- und Informationszugangsgesetz können in solchen Fällen nicht

[73] Verordnung (EG) Nr. 1049/2001 v. 30.5.2001, ABlEG L 145/43

[74] Der Leitfaden ist abgedruckt in Dokumente zu Datenschutz und Informationsfreiheit 2001, B

dazu herangezogen werden, den Zugang auszuschließen. Allerdings enthält die Verordnung ihrerseits eine Reihe von Ausnahmeregelungen, die schutzwürdige öffentliche und private Geheimhaltungsinteressen sichern sollen.

Auch der Europäische Gerichtshof hat im Berichtszeitraum erneut die Bedeutung des Transparenzgrundsatzes hervorgehoben, indem er eine Entscheidung des Rates für nichtig erklärte, mit der einem Mitglied des Europäischen Parlaments der Zugang zu einem Bericht über Waffenausfuhren verweigert wurde[75]. Der Gerichtshof hat betont, dass der Öffentlichkeit ein möglichst umfassender Zugang zu Ratsdokumenten zu eröffnen ist und jede Ausnahme von diesem Recht eng ausgelegt werden muss. Insbesondere darf der Zugang bei teilweise geheimhaltungsbedürftigen Unterlagen nicht pauschal verweigert, sondern muss insoweit gewährt werden, als kein gerechtfertigtes Geheimhaltungsbedürfnis besteht.

Auch das Europäische Parlament hat in einer Entschließung die Bedeutung des Transparenzgrundsatzes gerade in Situationen betont, in denen ein Bürger versucht, Auskünfte über die Beeinflussung der Entscheidungsfindung der Europäischen Kommission zu erhalten. Im konkreten Fall hatte diese es abgelehnt, die Namen von Verbandsvertretern mitzuteilen, die an einem offiziellen Gespräch mit der Kommission teilgenommen hatten. Das Europäische Parlament hat in Übereinstimmung mit dem Europäischen Bürgerbeauftragten festgestellt, dass der Datenschutz nicht für Zwecke des unlauteren Wettbewerbes oder der heimlichen Beeinflussung von Gremien der Gemeinschaft missbraucht werden darf; das Parlament hat dem zukünftigen Europäischen Datenschutzbeauftragten vorgeschlagen, Muster für Verhaltensregeln mit dem Ziel auszuarbeiten, die Respektierung der Rechte der Verbraucher auf Datenschutz zu gewährleisten, und Normen festzulegen, um den beschriebenen Missbrauch des Datenschutzes zu verhindern[76]. Nach Auffassung des Europäischen Parlaments sollte kein Datenschutz in Anspruch genommen werden, wenn Personen z. B. in einer öffentlichen Funktion tätig sind, während sie an öffentlicher Beschlussfassung auf Grund ihrer eigenen Initiative beteiligt sind oder während sie versuchen, eine solche Beschlussfassung zu beeinflussen[77].

---

[75] Urteil vom 6.12.2001 – C 353/99 P-(Rat der Europäischen Union/Hautala)

[76] Entschließung des Europäischen Parlaments v. 11.12.2001 zu dem Sonderbericht des Europäischen Bürgerbeauftragten in der Beschwerde 713/98/IJH (A5-0423/2001)

[77] vgl. hierzu auch den Vortrag von Gill, Zugang zu Dokumenten der EU – aus der Praxis des Europäischen Bürgerbeauftragten, beim Internationalen Symposium zu Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union, Oktober 2001, Potsdamer Materialien zu Akteneinsicht und Informationszugang, Bd. 2, 179 ff., 199 f.

1.2 Bundesrepublik Deutschland

Das Bundesinnenministerium hat im Berichtszeitraum den Entwurf für ein Informationsfreiheitsgesetz des Bundes im Internet veröffentlicht und dazu ein Diskussionsforum eingerichtet. Das Ministerium beabsichtigt dem Vernehmen nach weiterhin, im Frühjahr 2002 einen Kabinettsbeschluss über den Entwurf herbeizuführen und ihn noch vor der Bundestagswahl in den Bundestag einzubringen. Allerdings werden von anderen Bundesressorts zunehmend Einwände geltend gemacht.

Das Bundesministerium für Verbraucherschutz hat daneben die Vorlage des Entwurfs für ein Verbraucherinformationsgesetz angekündigt, das auf Grund der BSE-Krise und dem Ausbruch der Maul- und Klauenseuche Informationsrechte der Verbraucherinnen und Verbraucher stärken soll. In erster Linie soll der Zugang zu Informationen bei Lebensmittelüberwachungs-, Veterinäruntersuchungs- und Gewerbeaufsichtsämtern auf Bundes-, Länder- und Gemeindeebene verbessert werden. Auch sollen die Behörden das Recht erhalten, von sich aus die Öffentlichkeit über Produkte zu informieren, bei denen eine erhebliche Überschreitung von Grenzwerten festgestellt wurde oder gegen verbraucherschützende Vorschriften verstoßen worden ist. Dabei soll auch die namentliche Nennung von Unternehmen zugelassen werden, die riskante Produkte in den Handel bringen. Diese Initiative ist zu begrüßen. Der Staat kann sich gerade bei Informationen, die für die Gesundheit der Bevölkerung wesentlich sind, nicht darauf beschränken, sie für Interessierte bereitzuhalten; vielmehr hat der Staat insoweit eine „Bringschuld“ und kann zur aktiven Veröffentlichung solcher Daten verpflichtet sein. Schutzwürdige private Interessen der Produzenten wie Betriebs- und Geschäftsgeheimnisse müssen gegenüber dem öffentlichen Informationsinteresse sorgfältig abgewogen werden.

Auf Länderebene sind in zahlreichen Landtagen Gesetzentwürfe und Initiativen für die Verabschiedung von Informationsfreiheitsgesetzen eingebracht worden. Am ersten Januar 2002 trat im bevölkerungsreichsten Bundesland Nordrhein-Westfalen ein weiteres Informationsfreiheitsgesetz in Kraft[78]. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat bei einer Anhörung des Ausschusses für Innere Verwaltung und Verwaltungsstrukturreform des Nordrhein-westfälischen Landtages über die in Brandenburg gesammelten Erfahrungen berichtet. Das Nordrhein-westfälische Informationsfreiheitsgesetz ist ähnlich wie das Akteneinsichts- und Informationszugangsgesetz angelegt, geht in Teilen aber darüber hinaus. Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen ist jetzt auch Beauftragte für das Recht auf Information.

[78] GVBl. NRW 2001 S. 806

Zu weiteren Gesetzentwürfen und Initiativen ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Innenausschuss des Landtages Sachsen-Anhalt und im Ausschuss für Verfassungsfragen des Niedersächsischen Landtages angehört worden.

Für die Entwicklung des Informationszugangsrechts bedeutsam ist schließlich die Einführung des „in camera-Verfahrens“ im Verwaltungsprozess, die durch die Änderung der Verwaltungsgerichtsordnung am 1. Januar 2002 wirksam geworden ist[79]. Entsprechend einer Forderung des Bundesverfassungsgerichts aus dem Jahre 1999[80] ist die Verwaltungsgerichtsordnung in der Weise modifiziert worden, dass bei einer Verweigerung der Vorlage von Urkunden oder Akten auf Grund der Sperrerklärung einer obersten Landesbehörde, die möglich ist, wenn das Bekannt werden dieser Unterlagen dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde oder sie sonst geheimhaltungsbedürftig sind, das Oberverwaltungsgericht darüber zu entscheiden hat, ob die Verweigerung der Aktenvorlage zulässig ist. Dieses Verfahren unterliegt den Vorschriften des materiellen Geheimschutzes, sodass das Gericht „in camera“, also ohne Beteiligung desjenigen, der die Vorlage der Unterlagen verlangt, deren Geheimhaltungsbedürftigkeit prüft. Durch diese für das deutsche Prozessrecht neue Verfahrensform wird der Rechtschutz des Bürgers erheblich verbessert. Auch die Berufung auf die Staatswohlklausel oder Geheimhaltungsvorschriften zur Verweigerung von Informationen unterliegt nunmehr einer unabhängigen gerichtlichen Überprüfung.

1.3 Brandenburg

Der Landesbeauftragte hat im Berichtszeitraum auf Grund der in den ersten drei Jahren seit Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes gesammelten Erfahrungen eine Novellierung dieses Gesetzes vorgeschlagen[81] und bei den Fraktionen des Landtages um Unterstützung für diese Vorschläge geworben. Ein entsprechender Gesetzentwurf[82] wurde im Plenum des Landtages ohne Überweisung in die Ausschüsse abgelehnt[83]. Die Landesregierung hatte zuvor in ihrer Stellungnahme zum Tätigkeitsbericht 2000 des Landesbeauftragten zu erkennen gegeben, dass sie die Notwendigkeit zur Novellierung des Akteneinsichts- und Informationszugangsgesetzes nicht prinzipiell verneint, einen entsprechenden Bedarf aber

[79] Gesetz zur Bereinigung des Rechtsmittelrechts im Verwaltungsprozess v. 20.12.2001, BGBl. I S. 3987

[80] vgl. dazu Tätigkeitsbericht 1999, B 1.2

[81] vgl. Tätigkeitsbericht 2000, B 4

[82] Eingebracht von der Fraktion der PDS. Drs. 3/3376 sowie Plenarprotokoll 3/44 v. 25.10.2001

[83] Plenarprotokoll 3/44 v. 25.10.2001

erst nach Verabschiedung eines Bundesinformationszugangsgesetzes prüfen wolle[84].

Der Landesbeauftragte wird seine Vorschläge auf Grund der in der Praxis gesammelten Erfahrungen fortschreiben und dabei auch die Rechtsentwicklung in den anderen Bundesländern und auf Bundesebene berücksichtigen. Brandenburg hat seit 1998 eine Vorreiterrolle im Bereich des allgemeinen Informationszugangsrechts in Deutschland. Es sollte möglichst zeitnah die hier gesammelten praktischen Erfahrungen dazu nutzen, um den Anschluss an die Entwicklung des Informationszugangsrechts in anderen Bundesländern und im Bundesrecht, etwa beim Zugang zu Umweltinformationen, zu halten.

2 Umsetzung des Akteneinsichts- und Informationszugangsgesetzes

2.1 Eingaben und Anfragen beim Landesbeauftragten

Das Akteneinsichts- und Informationszugangsgesetz (AIG) ist nunmehr seit über drei Jahren in Kraft. Wie unterscheiden sich die aktuellen Eingaben beim Landesbeauftragten von den Beschwerden aus der Anfangszeit des Gesetzes?

Die Zahl der Beschwerden zum Umgang der Behörden mit dem Informationszugang bewegte sich im Berichtsjahr etwa auf dem Niveau des Vorjahres, während es im zweiten und dritten Jahr des In-Kraft-Tretens des Gesetzes einen erheblichen Anstieg der Eingaben zu verzeichnen gab. Ebenfalls zugenommen hat im Vergleich zu den ersten beiden Jahren der Erfolg der Eingaben beim Landesbeauftragten. Dies bedeutet, dass wir in einer zunehmenden Zahl von Fällen festgestellt haben, dass die Akteneinsicht zu Unrecht verweigert, aufgrund unserer Intervention schließlich aber doch Einsicht gewährt wurde.

Während zwei Drittel der Beschwerden von Bürgerinnen und Bürgern eingereicht wird, stammt jede fünfte Eingabe von Bürgerinitiativen, die sich gerade im kommunalen und regionalen Rahmen politisch engagieren und für diese Arbeit Informationen der Verwaltung benötigen. Ungebrochen ist die Entwicklung hinsichtlich der Behörden, über die Beschwerden eingereicht werden: Waren zunächst fast genauso viele oberste Landesbehörden wie andere Verwaltungen betroffen, haben sich die uns bekannten problematischen Fälle bei den Ministerien mittlerweile stark reduziert. Wie bereits im Vorjahr betreffen drei Viertel aller Eingaben den Umgang von Gemeinden, Ämtern, Städten und Landkreisen mit dem Akteneinsichts- und Informationszugangsgesetz.

[84] Drs. 3/2984

Betrachtet man die einzelnen Fachbereiche, so fallen weiterhin die Bauakten ins Auge. Die Häufigkeit der Beschwerden und Anfragen zu diesem Thema hat im Berichtszeitraum zwar etwas abgenommen, liegt aber mit etwa 40 Prozent aller Eingaben noch immer sehr hoch. Dies dürfte auch daran liegen, dass sich der Umgang mit personenbezogenen Daten hier recht kompliziert gestaltet und noch Unsicherheiten bestehen. Angelegenheiten der kommunalen Selbstverwaltung sowie der Bereich der Vermögens- und Grundstücksverwaltung stellten einen zunehmenden Schwerpunkt des Einsichtsinteresses dar. Die Umweltverwaltung hingegen ist immer weniger Gegenstand von Beschwerden zum Akteneinsichts- und Informationszugangsgesetz. Dies dürfte auch daran liegen, dass hier das Umweltinformationsgesetz als speziellere und damit vorrangige Rechtsnorm bereits einen allgemeinen Anspruch auf Informationszugang vorsieht.

Während in den Vorjahren nur selten Probleme mit der Erhebung von Kosten für den Informationszugang an uns herangetragen wurden, beträgt der Anteil der Eingaben, die ausschließlich die Kostenerhebung zum Inhalt haben, im Berichtsjahr bereits ein Zehntel. Dies ist durch das In-Kraft-Treten der Akteneinsichts- und Informationsgebührenordnung im April 2001 begründet. Da diese Verordnung nicht für Aufgaben der kommunalen Selbstverwaltung gilt, haben einige Kommunen seit April eigene Gebührensatzungen für die Akteneinsicht erlassen, die ebenfalls Anlass für Anfragen und Beschwerden gaben.

Die Entwicklung der vergangenen Jahre zeigt einerseits die zunehmende Routine in der Anwendung des Akteneinsichts- und Informationszugangsgesetzes, offenbart aber auch kritische Punkte wie z.B. den Umgang mit personenbezogenen Daten in Bauakten oder die Erhebung von Kosten für den Informationszugang.

2.2 Gebührenerhebung durch Kommunen nur mit Satzung

Drei Jahre nach Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes hat die Landesregierung im April 2001 die Gebührenordnung für die Akteneinsicht erlassen. Manchen Gebührenbescheiden mangelt es dennoch an einer eindeutigen Rechtsgrundlage.

Die Akteneinsichts- und Informationszugangsgebührenordnung der Landesregierung vom 2. April 2001 gilt nur für die Akteneinsicht nach dem Akteneinsichts- und Informationszugangsgesetz. Für den Informationszugang nach anderen Rechtsgrundlagen werden nach speziellen Kostenvorschriften Gebühren erhoben. Auch gilt die Gebührenordnung nicht für Aufgaben der kommunalen Selbstverwaltung. Eine Gemeinde, eine kreisfreie Stadt oder ein

Landkreis können Kosten nur dann erheben, wenn dies in einer Satzung vorgesehen ist.

Viele Kommunen haben in ihren allgemeinen Verwaltungsgebührensatzungen keine Regelung zur Akteneinsicht vorgesehen. Eine solche kann zwar in eine bestehende Satzung eingefügt werden, jedoch ist hier darauf zu achten, dass sich die Kostenerhebung nicht ausschließlich am Verwaltungsaufwand orientieren darf, sondern das angemessene Verhältnis zum Grundrecht auf Akteneinsicht zu wahren hat. Das bedeutet, dass der Verwaltungsaufwand nicht nach einheitlichen Zeitsätzen (z.B. 30,- DM pro halbe Stunde) abgerechnet werden darf.

Alternativ zum Rückgriff auf eine bereits bestehende, allgemeine Gebührensatzung können Kommunen auch separate Satzungen zur Kostenerhebung für die Akteneinsicht erlassen.

Die Anwendung der Akteneinsichts- und Informationszugangsgebührenordnung der Landesregierung durch die Kommunen ist aber auch bei kommunalen Selbstverwaltungsangelegenheiten möglich, wenn eine Satzung deren Heranziehung regelt. Diese Alternative dürfte für alle Beteiligten am übersichtlichsten sein. So wird vermieden, dass eine Kommune – je nachdem, ob es sich bei der zur Einsicht beantragten Akte um eine kommunale Selbstverwaltungsaufgabe oder um eine Landes- bzw. Weisungsaufgabe handelt – für dieselbe Leistung Kosten in unterschiedlicher Höhe verlangt.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird im Laufe dieses Jahres detaillierte Hinweise zur Anwendung der Gebührenordnung veröffentlichen.

Die Gebührenordnung der Landesregierung gilt für Angelegenheiten außerhalb der kommunalen Selbstverwaltung. Für den Informationszugang bei Selbstverwaltungsaufgaben dürfen Kosten nur aufgrund einer kommunalen Satzung erhoben werden. Diese hat bei der Bemessung der Gebührenhöhe ein angemessenes Verhältnis zwischen dem Verwaltungsaufwand und dem Einsichtsrecht zu berücksichtigen.

2.3 Bürgerberatung als Einnahmequelle?

Als sich herausstellte, dass die zur Einsicht beantragte Akte personenbezogene Daten Dritter enthielt, informierte die Stadt den Antragsteller ordnungsgemäß über die Möglichkeit, die Zustimmung der Betroffenen einzuholen. Bereits für diese Beratungsleistung erhob sie Gebühren in Höhe von 50,- DM.

Das Akteneinsichts- und Informationszugangsgesetz sieht verschiedene Beratungs- und Unterstützungsleistungen vor. So hat die Behörde beispielsweise den Antragsteller zu unterstützen, wenn ihm Angaben zur hinreichenden Bestimmung des Antrages fehlen, den Antrag an die zuständige Stelle weiterzuleiten und den Antragsteller hierüber zu unterrichten oder, wie hier geschehen, ihn darüber zu informieren, dass er von der Behörde die Einholung der Zustimmung betroffener Dritter verlangen kann. In bestimmten Ausnahmefällen – siehe hierzu § 4 Abs. 2 letzter Satz sowie § 5 Abs. 2 Nr. 3 Akteneinsichts- und Informationszugangsgesetz – hat sie auch das Einsichtsinteresse des Antragstellers zu erfragen, um eine Abwägung mit dem öffentlichen oder privaten Geheimhaltungsinteresse vornehmen zu können.

Bei diesen Unterstützungspflichten handelt es sich um Leistungen, die der Gewährung oder Ablehnung der Akteneinsicht voraus gehen. Sie stellen noch keine Entscheidung in der Sache dar, sondern sind lediglich als Zwischenschritt zu werten, ohne die eine rechtmäßige Weiterbearbeitung des Antrages nicht möglich ist. Die Erhebung von Gebühren kommt erst in Frage, wenn eine Entscheidung über den Antrag getroffen wird. Die Bearbeitung des Einsichtsbegehrens ist als ein einheitlicher Lebenssachverhalt zu betrachten, der insgesamt nur einmal einen Gebührentatbestand erfüllen kann. Auf keinen Fall kann bereits jeder Zwischenschritt mit Gebühren belegt werden. Die Stadt hat unserer Empfehlung, den Gebührenbescheid aufzuheben, entsprochen.

Gebühren für die Akteneinsicht können lediglich für die abschließende Entscheidung über den Antrag, keinesfalls aber für Zwischenschritte und Beratungsleistungen erhoben werden.

2.4 Öffentliche Auftragsvergabe – Transparenz oder Geheimhaltung?

Ein Kreistag beriet in nicht öffentlicher Sitzung die Angebote verschiedener Unternehmen, die sich um eine zu vergebende Leistung beworben haben. Wie kann die Öffentlichkeit nachvollziehen, unter welchen Kriterien die Beauftragung eines der Anbieter erfolgt ist?

Das Akteneinsichts- und Informationszugangsgesetz sieht die Ablehnung eines Einsichtsantrages für Vorgänge vor, die in nicht öffentlicher Sitzung beraten oder beschlossen worden sind. Allerdings ist der Vorgang offen zu legen, wenn das Interesse an der Einsichtnahme das entgegenstehende öffentliche Interesse überwiegt. Voraussetzung dafür, dass eine Abwägung erforderlich wird, ist das Vorliegen eines öffentlichen Geheimhaltungsinteresses. Im Falle einer Auftragsvergabe dürfte die Sitzung des Kreistages vor allem zum Schutz der Betriebs- und Geschäftsgeheimnisse der Anbieter, nicht aber aus

Gründen des öffentlichen Wohls, unter Ausschluss der Öffentlichkeit stattgefunden haben. Demnach können auch keine öffentlichen Interessen geltend gemacht werden, die einer Einsichtnahme entgegenstehen. Vielmehr liegt es im öffentlichen Interesse, dass die Auftragsvergabe so transparent wie möglich erfolgt.

Die vollständige Offenlegung der Angebote scheitert jedoch am Interesse der anbietenden Unternehmen, die in Vergabeakten regelmäßig vorhandenen Betriebs- und Geschäftsgeheimnisse zu schützen. Schließlich können bereits Kenntnisse über Detailkalkulationen und ähnliche geschäftsinterne Informationen möglichen Konkurrenten Wettbewerbsvorteile verschaffen. Das Akteneinsichts- und Informationszugangsgesetz sieht vor, dass über den Schutz der Betriebs- und Geschäftsgeheimnisse hinaus sämtliche Angaben mit Unternehmensbezug nicht ohne Zustimmung der betroffenen Firmen offen gelegt werden können. An Stelle der hier wenig Erfolg versprechenden Einholung der Zustimmung sollte sich die Akten führende Stelle auf die Vorschriften zur Aussonderung schutzbedürftiger Angaben konzentrieren. Eine solche Aussonderung erfolgt so lange, bis der Unternehmensbezug nicht mehr zu erkennen ist. Möglicherweise bleiben dann im Ergebnis lediglich bestimmte Rubriken, Leistungs- oder Preisangebote übrig. Die Anbieter sind dann anonym zu kennzeichnen, beispielsweise als „Anbieter 1“ etc. Die wichtigsten Informationen, nämlich darüber, nach welchen Kriterien der Zuschlag erteilt wurde, können so vom Antragsteller nachvollzogen werden.

Auch Vergabeakten sind nach dem Akteneinsichts- und Informationszugangsgesetz grundsätzlich einsehbar. Ein öffentliches Interesse an der Geheimhaltung der Vergabepraxis besteht in der Regel nicht. Bei der Offenlegung ist allerdings darauf zu achten, dass schutzbedürftige Unternehmensdaten nicht bekannt gegeben werden. Ein Schema zum Umgang mit Unternehmensdaten befindet sich in der Anlage.

2.5 Anonymisierung schutzbedürftiger Angaben

Ein Anwohner, der die Berechnung der Beiträge für den Ausbau der Straße kontrollieren wollte, interessierte sich für die Beiträge der anderen Anwohner, da er vermutete, dass diese teilweise bei der Erhebung der Abgaben ausgelassen worden seien. Die Summe der Beiträge beabsichtigte er, mit der Rechnung der Straßenbaufirma zu vergleichen. Beide Informationen unterliegen jedoch grundsätzlich den Ausnahmebestimmungen des Akteneinsichts- und Informations-zugangsgesetzes.

2.5.1 Personenbezogene Daten

Bei der Information, welche Anwohner wie viel Beiträge gezahlt haben, handelt es sich um personenbezogene Daten, die nicht ohne Zustimmung der Betroffenen offen gelegt werden können. Die Einholung der Zustimmung bei allen Betroffenen stellt für die Verwaltung einen erheblichen Aufwand dar; zudem ist sie für den Antragsteller, falls auch nur ein Nachbar die Offenlegung verweigert, nicht unbedingt zweckdienlich. Dies bedeutet jedoch nicht, dass die Herausgabe der Informationen von vornherein abzulehnen ist.

Die Aussonderung der schutzbedürftigen personenbezogenen Daten kann in diesem Fall zwar nicht durch eine einfache Schwärzung bestimmter Angaben erfolgen. Vielmehr ist es aber möglich, dem Antragsteller beispielsweise eine Flurkarte vorzulegen, auf der die Flurstücke markiert sind, für die Beiträge erhoben wurden. Eine parallele Auflistung der Quadratmeterzahlen für jedes Grundstück – ohne Bezug zu den einzelnen Flurstücken und möglichst ohne deren tatsächliche Reihenfolge – erlaubt es, festzustellen, ob die Beitragserhebung nach dem Gleichheitsgrundsatz erfolgt ist.

2.5.3 Unternehmensdaten

Im Falle der Straßenbaufirma ging es dem Anwohner vor allem darum, sich anhand der Rechnung über die Ausgaben der Gemeinde zu informieren, die der Beitragserhebung zu Grunde lagen. Dies kann möglicherweise bereits mit Hilfe von Haushaltsunterlagen geschehen. Für die Einsicht in die Rechnung ist entweder die Identität des Unternehmens zu schwärzen oder – wenn dem Antragsteller diese Informationen nicht genügen – dessen Anhörung vorzunehmen bzw. Zustimmung einzuholen.

Das Akteneinsichts- und Informationszugangsgesetz schützt unternehmensbezogene Daten bereits dann, wenn sie nach dem Willen des Unternehmens geheim zu halten sind. Während in anderen Rechtsgebieten Unternehmensdaten nur als Betriebs- und Geschäftsgeheimnisse gelten, wenn das Unternehmen auch ein schutzwürdiges Interesse an deren Geheimhaltung hat, genügt hier bereits der Wunsch einer Firma, die Daten nicht herauszugeben – auch wenn ein objektives Schutzinteresse überhaupt nicht zu erkennen ist.

Durch die Aufbereitung behördlicher Informationen können der Aufwand für die Verwaltung verringert und gleichzeitig das Einsichtsinteresse des Antragstellers befriedigt werden. Zum Umgang mit Unternehmensdaten siehe auch Anlage 4.

2.6 Wer vertritt eine Bürgerinitiative?

Das Mitglied einer Bürgerinitiative beantragte in deren Namen Einsicht in die Unterlagen zu einer Gemeindeeingliederung. Der Landkreis forderte den Antragsteller daraufhin auf, eine Vertretungsbefugnis vorzulegen. Da es für die Organisationsform von Bürgerinitiativen jedoch – anders als beispielsweise für eingetragene Vereine – keine formalen Voraussetzungen gibt, konnte eine solche Befugnis nicht beigebracht werden.

Das Akteneinsichts- und Informationszugangsgesetz gilt auch für Bürgerinitiativen und Verbände. Nach § 9 Abs. 2 AIG können Anträge auf Akteneinsicht nur durch den Vorstand oder einen Bevollmächtigten gestellt werden. In Zweifelsfällen ist die Vertretungsbefugnis nachzuweisen. Die ausdrückliche Erwähnung von Bürgerinitiativen und Verbänden durch den Gesetzgeber hebt deren Recht auf politische Mitgestaltung und Informationszugang in besonderer Weise hervor. Der Nachweis der Vertretungsbefugnis soll daher nicht die rechtliche Legitimation zur Antragstellung nachweisen, sondern vielmehr sicherstellen, dass die Behörde über einen konkreten Adressaten des Bescheides zur Akteneinsicht verfügt.

Nur ein eingetragener Verein oder ein Verband verfügt über eine formale Struktur bzw. Rechtsform, die es ermöglicht, einen Verwaltungsakt an ihn als juristische Person zu richten. Nur hier kann es sinnvoll sein, den Nachweis einer Vertretungsbefugnis zu verlangen.

Im Gegensatz dazu sind Bürgerinitiativen durch eine lockere Organisationsform gekennzeichnet. Ein Verwaltungsakt entfaltet keine Wirkung gegenüber einer solchen Initiative, sondern gegenüber ihren Mitgliedern als natürlichen Personen. Ein Bescheid zur Akteneinsicht richtet sich stets an die im Namen der Interessengemeinschaft Antrag stellende Person und verpflichtet im Regelfall nur diese auch hinsichtlich der Kosten. Auf das Einholen einer Vertretungsbefugnis von einer Bürgerinitiative ist daher zu verzichten. Sofern die Behörde jedoch einen Ansprechpartner benötigt, sollte sie das Einverständnis des Antragstellers einholen, als Adressat der mit der Akteneinsicht in Zusammenhang stehenden Verwaltungsakte zur Verfügung zu stehen. Ihm muss deutlich gemacht werden, dass er für die Bürgerinitiative ggf. auch die anfallenden Kosten trägt.

Von einer Bürgerinitiative kann keine Vertretungsbefugnis verlangt werden, solange sie nicht z.B. als Verein eingetragen ist. Um eine Ansprechperson für den Bescheid zur Akteneinsicht zu haben, kann die Behörde jedoch den Antragsteller auffordern, zu erklären, die Verantwortung für die Initiative zu übernehmen.

2.7 Auch das Datenschutzgesetz ermöglicht Akteneinsicht

Ein Architekt interessierte sich für die Bauzeichnungen, die ein Bauherr zwecks Genehmigung eingereicht hat. Er war selbst eine Zeit lang für diesen Bauherren tätig, bis dieser einen anderen Architekten beauftragte. Der Antragsteller vermutet nun, dass sein Nachfolger die ursprünglichen Entwürfe übernommen und damit gegen Urheberrecht verstoßen habe. Die Zeichnungen geben auch Auskunft über die Vermögensverhältnisse des Bauherrn und stellen somit ein personenbezogenes Datum dar. Auf welcher Rechtsgrundlage kommt eine Akteneinsicht in Frage?

Ein Antrag auf Informationszugang, der nach dem Akteneinsichts- und Informationszugangsgesetz (AIG) geprüft wird, bezieht sich auf allgemeine Informationen, die bei der Behörde vorhanden sind. Diese einzusehen ist ein individuelles Recht, für dessen Wahrnehmung es keines berechtigten oder rechtlichen Interesses bedarf. Ziel einer solchen Akteneinsicht sind nicht die personenbezogenen Angaben, sondern die übrigen Informationen. Befinden sich neben den begehrten Informationen auch personenbezogene Daten Dritter in der Akte, dürfen diese nur unter bestimmten Voraussetzungen eingesehen werden. § 5 Abs. 2 letzter Satz AIG sieht vor, dass die Bestimmungen des § 16 des Brandenburgischen Datenschutzgesetzes (BbgDSG) keine Anwendung finden. Dadurch wird klargestellt, dass bei einem Anspruch auf Einsicht in personenbezogene Akten die Datenübermittlung aufgrund des Akteneinsichts- und Informationszugangsgesetzes und nicht des Datenschutzgesetzes erfolgt. Der Anspruch auf Aktenseinsicht kann nicht durch die engeren Bestimmungen des Datenschutzgesetzes wieder eingeschränkt werden.

§ 16 BbgDSG enthält nur die Befugnis der Behörde, personenbezogene Daten an Dritte oder an Stellen außerhalb des öffentlichen Bereiches zu übermitteln. Hieraus lässt sich kein individueller Rechtsanspruch der Antrag stellenden Person, sondern lediglich das Recht auf eine Entscheidung nach pflichtgemäßem Ermessen ableiten. Unter anderem ist die Übermittlung der Daten nur zulässig, wenn der Auskunft Begehrende ein rechtliches Interesse geltend macht und kein Grund zur Annahme besteht, dass das Geheimhaltungsinteresse des Betroffenen überwiegt. Die Behörde hat also die beiderseitigen Interessen gegeneinander abzuwägen. Im Unterschied zur Akteneinsicht auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes wird hier explizit die Übermittlung der personenbezogenen Daten (eigene oder fremde Bauzeichnungen) beantragt. Die Vorschrift ist spezieller als das Akteneinsichts- und Informationszugangsgesetz und daher in diesem Fall vorrangig anzuwenden.

Der Antragsteller hatte im vorliegenden Fall vermutlich bereits weit gehend Kenntnis von den personenbezogenen Daten des Bauherrn. Ihm ging es da-

rum, festzustellen, ob eine Klage gegen diesen oder den zweiten Architekten Erfolg versprechend sein könnte. Er machte also ein rechtliches Interesse geltend und hatte damit eine stärkere Stellung als jemand, der ohne weitere Begründung Akteneinsicht verlangt. Der Übermittlung der Zeichnungen durch die Behörde dürften daher keine überwiegenden Geheimhaltungsinteressen entgegenstehen. Die Anwendung des Akteneinsichts- und Informationszugangsgesetzes hätte in diesem Fall zu dem widersinnigen Ergebnis geführt, dass die Behörde den Antrag auf Informationszugang ohne eigenen Entscheidungsspielraum hätte ablehnen müssen, wenn die Betroffenen ihr nicht zugestimmt hätten, obwohl der Antragsteller ein rechtliches Interesse geltend gemacht hat.

Wird die Akteneinsicht beantragt, um explizit an personenbezogene Daten zu gelangen, so ist deren Übermittlung durch die Behörde nach einer Interessenabwägung auf der Grundlage des § 16 Brandenburgisches Datenschutzgesetz möglich, soweit ein rechtliches Interesse an der Einsicht geltend gemacht wird. Richtet sich das Einsichtsinteresse jedoch auf andere Informationen, die sich nicht in erster Linie auf personenbezogene Angaben in den Unterlagen beziehen, greifen die Vorschriften des Akteneinsichts- und Informationszugangsgesetzes.

2.8 Der Grund für die Akteneinsicht ist Sache des Antragstellers

Eine Stadtverwaltung verlangt, dass ein Antragsteller, der sich für die Niederschriften öffentlicher Sitzungen der Stadtverordnetenversammlung interessiert, ein berechtigtes Interesse darlegt.

Das Akteneinsichts- und Informationszugangsgesetz (AIG)gewährt ein voraussetzungsloses Recht auf Akteneinsicht. Es kommt also nicht darauf an, dass ein Antragsteller ein irgendwie geartetes Interesse geltend macht. Ein solches Offenbarungsinteresse darf lediglich in zwei Ausnahmefällen erfragt werden. So wird Akteneinsicht gewährt, wenn das Interesse an der Einsichtnahme das entgegenstehende öffentliche Interesse überwiegt (§ 4 Abs. 2 AIG). Informationen können auch zugänglich gemacht werden, wenn nach § 5 Abs. 2 Nr. 3 AIG das Offenbarungsinteresse im Hinblick auf den Zweck der politischen Mitgestaltung das Geheimhaltungsinteresse einer betroffenen Person überwiegt. Um in diesen beiden Fällen eine Abwägung vornehmen zu können, muss die Akten führende Stelle Kenntnis vom Einsichtsinteresse des Antragstellers haben. Ihm ist nach § 6 Abs. 1 Satz 4 AIG Gelegenheit zu dessen Darlegung innerhalb von zwei Wochen zu geben. In allen anderen Fällen ist die Verwaltung nicht berechtigt, den Antragsteller zu fragen, weshalb er sich für die Akten interessiert.

Auf Niederschriften von Sitzungen der Stadtverordnetenversammlung, die ohnehin öffentlich stattgefunden haben, trifft keine der beiden Ausnahmeregelungen zu. Weder sind private Belange berührt, noch liegt ein schützenswertes öffentliches Interesse vor. Wir haben die Stadtverwaltung daher aufgefordert, nur im gesetzlich vorgesehenen Rahmen eine Interessensdarlegung zu verlangen.

Die Behörde darf einen Antragsteller nur nach dem Grund für sein Einsichtsinteresse fragen, wenn das Akteneinsichts- und Informationszugangsgesetz eine Abwägung zwischen Einsichts- und Geheimhaltungsinteresse vorsieht.

2.9 Informationszugang im Kommunalrecht

Ein Antragsteller interessiert sich für die Beschlüsse der Gemeindevertretung, für eine Abwassergebührensatzung sowie für verschiedene Protokolle der Sitzungen der Gemeindevertretung. Die Gemeinde übersendet die gewünschten Unterlagen und lässt sich die entstandenen Kopier- und Versandkosten erstatten. Im Zusammenhang mit dem vom Antragsteller in Zweifel gezogenen Kostenbescheid hatten wir die Frage zu klären, auf welcher Rechtsgrundlage die einzelnen Unterlagen zugänglich gemacht werden.

Unterlagen einer Gemeinde oder eines Landkreises fallen grundsätzlich unter das Akteneinsichts- und Informationszugangsgesetz. Allerdings gilt auch hier, dass Rechtsvorschriften, die bereichsspezifische Regelungen zum Informationszugang durch einen unbeschränkten Personenkreis vorsehen, Vorrang haben. Die Gemeinde- und die Landkreisordnung enthalten teilweise solche Vorschriften.

Nach § 49 Abs. 5 Gemeindeordnung sind Beschlüsse der Gemeindevertretung in ortsüblicher Weise bekannt zu machen. Für Beschlüsse des Kreistages gilt die gleich lautende Vorschrift des § 33 Abs. 5 Landkreisordnung. Die Veröffentlichung geschieht in der Regel durch Aushang oder Abdruck in Amtsblättern. Eine derartige Veröffentlichung steht dem Recht des Antragstellers, eine Fotokopie der Beschlüsse zu erhalten, jedoch nicht entgegen.

Nach den gleichlautenden §§ 5 Abs. 6 der Gemeinde- und der Landkreisordnung besteht für jedermann ein Recht auf Einsicht in Satzungen bzw. auf Erhalt von Abschriften gegen Kostenerstattung.

Rechtsgrundlage für die Kostenerhebung für die Fertigung und den Versand der Fotokopien sowohl der Beschlüsse als auch der Satzungen ist in der Regel eine allgemeine Verwaltungsgebührensatzung der Kommune.

Der Zugang zu den Niederschriften (Protokollen) der Sitzungen der kommunalen Vertretungen richtet sich nach den Vorschriften des Akteneinsichts- und Informationszugangsgesetzes, da weder die Gemeinde-, noch die Landkreisordnung hierzu Regelungen enthalten. Da es sich hier um Angelegenheiten der kommunalen Selbstverwaltung handelt, können Kosten nur erhoben werden, wenn eine Satzung dies vorsieht[85].

Die Einsicht in Satzungen und die Veröffentlichung von Beschlüssen der kommunalen Vertretungen sind auf der Grundlage der Gemeinde- bzw. Landkreisordnung zu bearbeiten. Niederschriften von Sitzungen der Gemeinde- bzw. Stadtverordnetenvertretung oder des Kreistages werden nach dem Akteneinsichts- und Informationszugangsgesetz offen gelegt.

2.10 Wenn's ums Geld geht: Fiskalisches Verwaltungshandeln

Ein Inhaber eines Erbbaurechtes beabsichtigte, das von ihm bebaute Grundstück vom Land Brandenburg zu erwerben. Zur Ermittlung des Kaufpreises hat die zuständige Finanzbehörde Bezug auf ein in der Nähe liegendes, ähnliches Grundstück genommen, für das ein Wertgutachten vorliegt. Die vom Kaufinteressenten beantragte Einsicht in dieses Gutachten wurde unter Angabe wettbewerbsrechtlicher Gründe abgelehnt.

Das Akteneinsichts- und Informationszugangsgesetz gilt für die Grundstücks- und Vermögensverwaltung ebenso wie für alle anderen brandenburgischen Behörden, Einrichtungen und Kommunen. Der Anspruch auf Akteneinsicht erstreckt sich auf Informationen, die bei der Behörde vorhanden sind – das Gesetz unterscheidet hier nicht zwischen hoheitlichen und fiskalischen Aufgaben. Wettbewerbsrecht, also beispielsweise das Gesetz gegen den unlauteren Wettbewerb, kommt hier nicht zur Anwendung.

Der Staat befindet sich beim fiskalischen Verwaltungshandeln zwar in einem gleichrangigen Verhältnis zum Bürger (beide sind insofern Wirtschaftsteilnehmer), ist aber dennoch an öffentlich-rechtliche Regelungen gebunden. Insbesondere die Bindung an die Grundrechte – also auch an das Informationszugangsrecht, das auf der Landesverfassung beruht – aber auch andere Vorschriften wie beispielsweise die Landeshaushaltsordnung sind zu beachten. Dies hat unter anderem zum Ziel, die Kontrolle der öffentlichen Hand beim Umgang mit Steuergeldern zu gewährleisten und dient somit auch der Korruptionsprävention. Durch die Wahl der Rechtsreform – hier also die pri-

[85] s. oben B 2.2

vatrechtliche Tätigkeit – kann sich der Staat nicht der Verpflichtung zum transparenten Handeln entziehen.

Soweit sich aus den Unterlagen ein Schutzbedarf ergibt, sind die Bestimmungen des § 5 Abs. 1 Nr. 3 Akteneinsichts- und Informationszugangsgesetz heranzuziehen. Ob Betriebs- und Geschäftsgeheimnisse vorliegen, richtet sich jedoch nicht wie bei Unternehmen nach dem Willen der Behörde[86]. Vielmehr muss diese begründen, dass ein objektives Geheimhaltungsinteresse für das Gutachten vorliegt. Die Schutzwürdigkeit richtet sich danach, ob es sich tatsächlich um eine Wettbewerbssituation handelt. Außerdem ist zu fragen, welcher Schaden im Falle einer Offenlegung einträte. Im Falle des Wertgutachtens ist jedoch weder eine Konkurrenzsituation, noch ein potenzieller Schaden zu erkennen. Wir haben die Behörde deshalb aufgefordert, das Gutachten auf der Grundlage des Akteneinsichts- und Informationszugangsgesetz offen zu legen.

Betätigt sich die öffentliche Hand wirtschaftlich, hat sie ihr Handeln genauso offen zu legen wie bei hoheitlichen Tätigkeiten. Die Transparenz beim Umgang mit Steuergeldern trägt dazu bei, das Vertrauen der Bürger zu stärken und der Gefahr der Korruption zu begegnen.

2.11 Wenn Verwaltung und Bürger sich misstrauen

Nachdem ein Antragsteller nach erhaltener Akteneinsicht öffentlich behauptete, die Unterlagen nie gesehen zu haben, war der betroffene Landkreis nicht in der Lage, den Gegenbeweis anzutreten. Nun müssen dort die Antragsteller schriftlich bestätigen, dass und in welche Akten sie Einsicht genommen haben. Unter Hinweis auf diese Problematik hat eine Behörde daraufhin die Übersendung von Fotokopien verweigert.

Die Behörde kann vom Antragsteller verlangen, die Einsichtnahme in die beantragten Unterlagen zu bestätigen. Dem Antragsteller ist auf Verlangen eine Kopie der Bestätigung zur Verfügung zu stellen. So wird sichergestellt, dass beide Seiten im Bedarfsfall nachweisen können, wer was wann gesehen hat. Diese Praxis sollte allerdings auf Ausnahmefälle beschränkt bleiben, wenn beispielsweise die Akteneinsicht strittig war oder erst nach dem Einlegen von Rechtsmitteln gewährt wurde.

Wird unter Bezugnahme auf § 7 AIG die Übermittlung von Vervielfältigungen beantragt, stellt sich das Problem, dass der Antragsteller die Durchführung des Informationszugangs nicht in derselben Weise bestätigen kann wie bei der Einsicht in die Originalunterlagen vor Ort. Dennoch darf sein Recht auf

[86] s. oben B 2.4

Fotokopien durch die Notwendigkeit der Bestätigung ihres Erhalts nicht eingeschränkt werden. Wir haben der Behörde empfohlen, das von ihr entwickelte Formular, auf dem die Durchführung der Akteneinsicht bestätigt wird, entsprechend zu erweitern. Wird die Übersendung von Kopien beantragt, sollte das Formular behördlicherseits ausgefüllt und dem Antragsteller mit der Bitte, es zu unterschreiben, zugesandt werden. Eine Kopie des von der Behörde ausgefüllten Formulars kann zusammen mit dem Absendevermerk bis zum Eingang des unterzeichneten Schreibens zur Vorgangsakte genommen werden. Dies genügt für den Nachweis, dass die Kopien übersandt wurden.

Die Behörde hat das Bestätigungsformular sowie die Dienstanweisung zur Akteneinsicht daraufhin geändert und dem Antragsteller die gewünschten Kopien übersandt.

In Ausnahmefällen kann die Bestätigung der Durchführung der Akteneinsicht durch den Antragsteller notwendig sein. Dies darf dem Recht auf den Erhalt von Fotokopien jedoch nicht entgegenstehen.

2.12 Interessante Altakten – Akteneinsicht und Archivrecht

Das Akteneinsichts- und Informationsgesetz erlaubt einem unbeschränkten Personenkreis den Zugang zu den aktuellen Akten der öffentlichen Verwaltung. Werden diese Akten von der Verwaltung nicht mehr benötigt, sind sie dem Landesarchiv zur Verfügung zu stellen. Die Nutzung des Landesarchivs wiederum richtet sich nach dem Brandenburgischen Archivgesetz (BbgArchivG) und erlaubt eine Nutzung des Archivguts durch die Allgemeinheit erst nach Ablauf von zehn Jahren nach der Entstehung der Unterlagen. Paradoxes Ergebnis: Ehemals zugängliche Akten werden, nachdem sie für die laufende Verwaltung keinen Gebrauchswert mehr haben, erst einmal zu „Verschlusssachen".

Sowohl das Archivrecht als auch das Recht auf Akteneinsicht ermöglichen den Zugang zu Informationen öffentlicher Stellen, um so letztlich auch das Verwaltungshandeln transparent zu machen. Allerdings ist das Archivrecht sehr viel älter als das Akteneinsichtsrecht. Es stammt aus einer Zeit, in der der Zugang zu Akten die Ausnahme war und allenfalls für Verfahrensbeteiligte ermöglicht wurde. Daher galt für alle Akten, auch solche, die nicht in erster Linie personenbezogene Daten enthielten, eine generelle Sperrfrist, während derer keine Einsicht gewährt wurde. Durch die Schaffung des Akteneinsichts- und Informationszugangsgesetzes ist die Ausnahme zur Regel geworden. In dem Moment aber, in dem die Unterlagen nicht mehr benötigt werden, sind sie dem Landesarchiv anzubieten. Werden sie dort angenommen, unterliegen sie nicht mehr dem Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes, sondern dem des Archivgesetzes mit der Folge, dass

ehemals frei zugängliche Unterlagen gemäß § 10 Abs.1 BbgArchivG einer generellen zehnjährigen Sperrfrist unterliegen und damit unzugänglich werden. Unter der Voraussetzung, dass sowohl das Akteneinsichts- und Informationszugangsgesetz als auch das Brandenburgische Archivgesetz den Erhalt und die freie Nutzung von Informationen aus den Akten der öffentlichen Verwaltung gewährleisten sollen, ergibt sich daraus ein Wertungswiderspruch: Jemand, der voraussetzungslos in eine Akte Einsicht genommen hat, hat nunmehr aufgrund einer Sperrfrist keinerlei Zugriff mehr und muss auch nach deren Ablauf noch ein berechtigtes Interesse an der Einsicht glaubhaft machen. Am besten aufzulösen wäre dieser Wertungswiderspruch durch eine Änderung des Archivrechts dahingehend, dass für alle Unterlagen, die nach dem Akteneinsichts- und Informationszugangsgesetz zugänglich waren oder wären, keine Sperrfrist gilt.

Bereits jetzt ist das Brandenburgische Archivgesetz so anzuwenden, dass Akten, in die schon im Verwaltungsvollzug Einsicht gewährt worden ist, auch vor Ablauf der archivrechtlichen Sperrfristen zugänglich zu machen sind. Denn diese Akten waren der Öffentlichkeit bereits zugänglich (§ 10 Abs. 7 BbgArchivG). Darauf hat auch das Ministerium des Innern in seinen Ersten Hinweisen zum AIG hingewiesen[87].

Das nebeneinander geltende Recht auf Akteneinsicht und das Recht der Nutzung öffentlicher Archive kann bei der Beurteilung der Zugriffsmöglichkeit auf Informationen zu gegensätzlichen Ergebnissen führen. Unter Berücksichtigung der verfassungsrechtlich verankerten Informationsfreiheit sollte jedoch unbeschränkt Einblick in solche archivierten Unterlagen gewährt werden, die schon im Verwaltungsvollzug nach dem AIG offengelegt worden sind.

3 Offenlegung von Verwaltungsvorschriften

3.1 Sind die Regeln zur Gefangenenverpflegung geheim?

Ein Mitarbeiter einer Hamburger Gefangenenzeitung, der in einem anderen Bundesland eine Haftstrafe verbüßte, bat das Ministerium der Justiz und für Europaangelegenheiten zunächst vergeblich, ihm Einsicht in die Verwaltungsvorschriften zur Gefangenenverpflegung in Brandenburg zu gewähren. Schließlich wandte er sich an uns.

Auf das Akteneinsicht- und Informationszugangsrecht kann sich jeder Mensch berufen, auch wenn er kein Bürger des Landes Brandenburg ist oder hier keinen Wohnsitz hat. Verwaltungsvorschriften enthalten weder personenbezogene Daten noch Betriebs- oder Geschäftsgeheimnisse, sodass ihrer

[87] Ziff. 1.5 der Ersten Hinweise v. 17.7.1998, ABl. S. 842

Offenlegung jedenfalls keine schutzwürdigen privaten Interessen entgegenstehen. Denkbar ist zwar, dass überwiegende öffentliche Interessen es gebieten, bestimmte Verwaltungsvorschriften zumindest in Teilen nicht zur Einsicht freizugeben. Das ist jedoch bei verwaltungsinternen Regelungen zur Gefangenenverpflegung offenkundig nicht der Fall.

Wir konnten beim Ministerium der Justiz und für Europaangelegenheiten – wenn auch erst nach geraumer Zeit – erreichen, dass dem Petenten Kopien der Vorschriften aus der Geschäftsanweisung für die Wirtschaftsverwaltung der Justizvollzugsanstalten, die die Verpflegung der Gefangenen berühren, übersandt wurden.

Auf das Akteneinsichts- und Informationszugangsgesetz können sich auch Personen berufen, die nicht in Brandenburg leben. Weder private noch öffentliche Interessen rechtfertigen es, Verwaltungsvorschriften über die Verpflegung von Strafgefangenen unter Verschluss zu halten.

3.2 Transparenz als Beitrag zum Abbau von Normen und Standards

Gesetze und Verordnungen bedürfen zu ihrer Wirksamkeit der Verkündung im Gesetz- und Verordnungsblatt. Daneben gibt es eine Vielzahl von Vorschriften, die die Verwaltung sich selbst als „Binnenrecht" gegeben hat und mit denen vor allem die Ministerien das Verwaltungshandeln zu steuern versuchen. Nur ein Teil dieses Binnenrechts wird vom Ministerium der Justiz und für Europaangelegenheiten veröffentlicht[88].

Das „Binnenrecht" der Verwaltung (Verwaltungsvorschriften, Runderlasse, Allgemeine Verfügungen) hat mittlerweile einen so großen Umfang, dass das Ministerium des Innern sich im Dezember 2001 veranlasst sah, die Aufhebung von 40 bis 50 Prozent dieser Erlasse für das I. Quartal 2002 anzukündigen, weil ein Großteil der Vorschriften z. B. im Meldewesen inzwischen überflüssig geworden sei. Soweit Verwaltungsvorschriften, Runderlasse und Allgemeine Verfügungen nicht offensichtlich obsolet geworden sind, haben die Bürgerinnen und Bürger einen Anspruch, ihren Inhalt zu kennen. Diese Vorschriften haben nämlich nicht nur interne Bedeutung für die Verwaltung, sondern alle Bürgerinnen und Bürger können sich gegenüber der Verwaltung und vor den Verwaltungsgerichten nach dem Gleichbehandlungsgrundsatz der Verfassung darauf berufen, dass Verwaltungsbehörden sich an das selbst gesetzte Binnenrecht in der Regel halten und nur bei Vorliegen sachlicher Gründe oder bei einer generellen Änderung der Verwaltungspraxis davon abweichen dürfen.

[88] Fundstellennachweis für Verwaltungsvorschriften (Stand: 31.12.2000), ABl I/2001 v. 16.3.2001

Es besteht kein Zweifel, dass sich der verfassungsrechtliche Anspruch auf Akteneinsicht auch auf Verwaltungsvorschriften und anderes Binnenrecht der Verwaltung erstreckt[89], soweit nicht gesetzliche Geheimhaltungsgründe im Einzelfall dagegen sprechen. Die Verwaltung sollte aber darüber hinaus die von ihr selbst gesetzten Regeln über das eigene Handeln nicht erst auf Nachfrage offen legen, sondern den Bürgerinnen und Bürgern von sich aus zur Verfügung stellen.

Der Landesbeauftragte hat sich deshalb an den Ausschuss für Verwaltungsoptimierung mit dem Vorschlag gewandt, die Staatskanzlei möge sich dafür einsetzen, dass alle obersten Landesbehörden angehalten werden, die von ihnen erlassenen Verwaltungsvorschriften möglichst im Internet zu publizieren. Soweit dies nicht bis zu einem bestimmten festzulegenden Zeitpunkt geschieht, sollten die verwaltungsinternen Regelungen außer Kraft treten.

Verwaltungsvorschriften sollten generell veröffentlicht werden und für Interessenten leicht zugänglich sein. Davon könnten nur solche Vorschriften ausgenommen bleiben, bei denen ein überwiegendes öffentliches Interesse an der Geheimhaltung besteht. Mit einem solchen Vorgehen würde gleichzeitig dem Gebot der Transparenz des Verwaltungshandelns im Rechtsstaat und dem Ziel eines zunehmenden Abbaus von Normen und Standards Rechnung getragen.

4 Informationszugang für Abgeordnete

Ein Landtagsabgeordneter richtete eine Kleine Anfrage an die Landesregierung, mit der er Auskunft über Werbemaßnahmen der Berlin-Brandenburg Flughafen Holding GmbH begehrte. Die Landesregierung teilte dem Abgeordneten hierzu mit, dass sie über keine eigenen Unterlagen oder Kenntnisse zu seinen Fragen verfüge. Die Flughafen Holding, an der das Land zu 37,5 % beteiligt ist, habe detaillierte Angaben zu den Fragen des Abgeordneten unter Hinweis auf ihre Geschäftsgeheimnisse und darauf verweigert, dass über Einzelheiten der Werbeaktionen mit den Vertragspartnern Stillschweigen vereinbart worden sei[90]. Der Abgeordnete wandte sich daraufhin an den Landesbeauftragten und bat um Überprüfung der Antwort.

Der Anspruch von Abgeordneten des Landtages auf Auskunft und Vorlage von Akten nach Artikel 56 der Landesverfassung war bereits in der Vergangenheit Gegenstand von Anfragen beim Landesbeauftragten für das Recht

89 s. oben B 3.1

90 Antwort auf die Kleine Anfrage 1150, Drs. 3/3094

auf Akteneinsicht[91]. Landtagsabgeordnete haben einen Anspruch auf Informationszugang gegen alle Behörden und Dienststellen des Landes, der gegenüber der Landesregierung oder dem Landesrechnungshof geltend zu machen ist. Das Landesverfassungsgericht hat wiederholt festgestellt, dass die Funktion des Parlaments in hohem Maße davon abhängt, dass die Abgeordneten die Möglichkeit erhalten, ihre Kontrollfunktion wahrzunehmen, was wiederum unmittelbar von der Eröffnung des Zugangs zu Informationen lebt[92].

Bei der Beantwortung Kleiner Anfragen ist die Landesregierung deshalb grundsätzlich befugt, in das Grundrecht auf informationelle Selbstbestimmung von Privatpersonen im erforderlichen Umfang einzugreifen, wenn sonst die parlamentarische Kontrolle nicht ausgeübt werden kann. Lediglich bei Informationen aus dem höchstpersönlichen Bereich ist eine Auskunft zu verweigern. Die personenbezogenen Informationen sind in einem geeigneten Verfahren (z. B. durch schriftliche Beantwortung gegenüber dem Fragesteller oder mündliche Auskunftserteilung in nicht öffentlicher Ausschusssitzung) mitzuteilen. Gleiches gilt, wenn die Anfrage des Abgeordneten sich auf unternehmensbezogene Informationen bezieht. Soweit die Landesregierung über solche Informationen verfügt, hat sie diese dem Fragesteller selbst dann offen zu legen, wenn es sich um Betriebs- und Geschäftsgeheimnisse eines Unternehmens handelt, das vollständig im Eigentum des Landes steht. Das gilt zumindest insoweit, als die Ausübung der parlamentarischen Kontrollrechte sonst vereitelt würde. Den Geheimhaltungsinteressen eines Unternehmens kann durch die nicht öffentliche Form der Beantwortung gegenüber dem schweigepflichtigen Abgeordneten Rechnung getragen werden, so dass es in aller Regel nicht gerechtfertigt ist, dem Abgeordneten die Information vorzuenthalten.

In dem konkreten Fall bestand die zusätzliche Schwierigkeit, dass die Landesregierung nicht über die zur Beantwortung der Kleinen Anfrage erforderlichen Informationen verfügte und zudem das Land nur einer von mehreren Gesellschaftern der Berlin-Brandenburg Flughafen Holding GmbH ist. Die von dieser Gesellschaft geltend gemachten Gründe zur Verweigerung der verlangten Auskünfte hätten eine Auskunftsverweigerung durch die Landesregierung, soweit sie über die Informationen selbst verfügt hätte, nicht gerechtfertigt. Das Ministerium für Wirtschaft hat deshalb zu Recht das Ministerium der Finanzen gebeten, im Rahmen ihrer Zuständigkeit für die Verwaltung der Landesbeteiligungen zu prüfen, ob das Land Brandenburg eine gesellschaftsrechtliche Möglichkeit hat, die Geschäftsführung der Holding um die erbetene Auskunft zu bitten. Die Landesregierung ist nach Artikel 56 der Landesver-

[91] vgl. Tätigkeitsbericht 1998, B 5

[92] Urteile vom 20.6.1996 (VfGBbg 3/96) und vom 20.11.19997 (VfGBbg 16/97)

fassung gehalten, alles im Rahmen des Gesellschaftsrechts Mögliche zu unternehmen, um den Abgeordneten die erbetenen Auskünfte zu erteilen.

Das Beispiel macht deutlich, welche – bei der gegenwärtigen politischen Diskussion um die Landesbeteiligungen wenig beachteten – zusätzlichen Probleme der parlamentarische Kontrolle bei der Realisierung des Auskunftsanspruchs von Abgeordneten auftreten können.

Da dieser Auskunfts- und Aktenvorlageanspruch sich nur an Behörden und Dienststellen des Landes richtet, kann er zwar gegenüber Oberbürgermeistern und Landräten geltend gemacht werden, soweit diese als untere Landesbehörden handeln. Im Übrigen und gegenüber den Gemeinden hat der Abgeordnete wie jede Bürgerin und jeder Bürger die Rechte nach dem Akteneinsichts- und Informationszugangsgesetz.

Die Landesregierung ist verpflichtet, Anfragen von Abgeordneten des Landtages zu landeseigenen Unternehmen umfassend zu beantworten. Betriebs- und Geschäftsgeheimnisse sind durch die Form der Beantwortung zu sichern und rechtfertigen es nur in seltenen Fällen, dem Abgeordneten die Information vorzuenthalten. Bei Beteiligungen des Landes an privaten Unternehmen muss das zuständige Ressort alle gesellschaftsrechtlichen Möglichkeiten ausschöpfen, um die gewünschte Information bereitstellen zu können.

Teil C

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Die Anforderungen an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sind im vergangenen Jahr – auch auf Grund der aktuellen Ereignisse – stark angestiegen. Gerade in einer Zeit, in der die Sicherheitsbehörden angesichts neuer Bedrohungen von - lange Zeit ungenutzten - Befugnissen wie der zur Rasterfahndung Gebrauch machen und zudem zusätzliche, weiter gehende gesetzliche Befugnisse erhalten, wächst die Bedeutung einer unabhängigen Datenschutzkontrolle. Dennoch blieb die Ausstattung des Landesbeauftragten im Wesentlichen unverändert. Mittelfristig wird sie jedoch den deutlich gestiegenen Anforderungen angepasst werden müssen.

Im Berichtszeitraum haben wir damit begonnen, die Altakten der jetzt zehn Jahre bestehenden Dienststelle des Landesbeauftragten zu archivieren, also die Originalakten auszusondern und die Ergebnisse der Vorgangsbearbeitung in anonymisierter Form für die Dienststelle nutzbar zu machen.

Im laufenden Jahr wird es möglich sein, mit zusätzlich vom Landtag bewilligten Mitteln die Internetpräsenz des Landesbeauftragten neu und bürgerfreundlicher zu gestalten. Angesichts der beschränkten Ressourcen, die ihm zur Verfügung stehen, muss der Landesbeauftragte das Internet verstärkt zur Öffentlichkeitsarbeit und zur Bereitstellung von Informationen für die Bürgerinnen und Bürger wie auch für die Verwaltung nutzen.

Zur Frage des Standortes der Dienststelle bekräftigt der Landesbeauftragte seinen Standpunkt, dass diese Bürgerbehörde ihren Sitz in der Landeshauptstadt erhalten sollte. Zu diesem Zweck hat er sich an den Präsidenten des Landtages mit der Bitte gewandt, sich bei den bevorstehenden Entscheidungen für einen Neubau des Brandenburgischen Landtages dafür einzusetzen, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht seinen endgültigen Dienstsitz im neuen Parlament erhält.

2 Zusammenarbeit mit dem Landtag

Der Tätigkeitsbericht 2000 wurde im Berichtszeitraum im Innenausschuss des Landtages eingehend erörtert, wobei die Beratungen hierüber im Berichtszeitraum nicht mehr abgeschlossen werden konnten. Der Ausschuss für

Inneres hat sich bei dieser Gelegenheit auch mit der vom Landesbeauftragten erneut aufgeworfenen Frage nach der noch immer ausstehenden Datenschutzordnung für den Landtag nach § 2 Abs. 1 a Brandenburgisches Datenschutzgesetz befasst und seinen Vorsitzenden beauftragt, den Präsidenten um eine Mitteilung zum Sachstand in dieser Angelegenheit zu bitten. Zudem hat der Landesbeauftragte gegenüber dem Ausschuss für Gesundheit und Soziales Stellung zum Entwurf zur Änderung des Psychisch-Kranken-Gesetzes genommen.

3 Kooperation mit anderen Institutionen

3.1 Zusammenarbeit mit Datenschutzbeauftragten und Aufsichtsbehörden

Im vergangenen Jahr fanden unter dem Vorsitz der nordrhein-westfälischen Landesbeauftragten für den Datenschutz, Bettina Sokol, zwei turnusmäßige Konferenzen der Datenschutzbeauftragten des Bundes und der Länder in Düsseldorf und Münster statt. Auf einer Sonderkonferenz beschäftigten sich die Datenschutzbeauftragten ausschließlich mit den Auswirkungen der Terroranschläge am 11. September 2001. Die zahlreichen bei diesen Konferenzen gefassten Entschließungen sind in dem gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit veröffentlichten Band „Dokumente zu Datenschutz und Informationsfreiheit 2001“ enthalten, den wir auf Wunsch versenden. Im Jahr 2002 geht der Vorsitz der Datenschutzkonferenz auf den Landesbeauftragten für den Datenschutz Rheinland-Pfalz, Prof. Dr. Walter Rudolf, über.

Der Landesbeauftragte für Datenschutz und Akteneinsicht hat zur Vorbereitung der Datenschutzkonferenzen den Arbeitskreis Medien im Berichtszeitraum zu je einem Treffen in Potsdam und in Düsseldorf einberufen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat auf Vorschlag des Landesbeauftragten ein Arbeitspapier zu Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen beschlossen[93]. Zu diesem Thema hat er auch einen Vortrag bei der XXII. Internationalen Datenschutzkonferenz in Paris im September 2001 gehalten. Zudem hat der Landesbeauftragte die Bundesländer in der Gruppe der Europäischen Datenschutzbeauftragten nach Artikel 29 der EG-Datenschutzrichtlinie in Brüssel vertreten.

Die Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich verlief auch im Berichtszeitraum konstruktiv, es konnten

[93] Dokumente zu Datenschutz und Informationsfreiheit 2001, A.IV.2

jedoch auf Grund von organisatorischen Veränderungen im Ministerium des Innern nicht die in der Vergangenheit üblichen regelmäßigen Koordinationsgespräche durchgeführt werden.

Dagegen entwickelte sich die Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit weiterhin positiv. Neben regelmäßigen Arbeitstreffen der Dienststellenleitungen wurden auch auf Arbeitsebene die Prüfvorhaben miteinander abgestimmt und gemeinsame Kontrollen wie etwa im Bereich des Rundfunks durchgeführt.

3.2 Zusammenarbeit mit Informationsbeauftragten

Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID) hat unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit in Berlin getagt und sich mit aktuellen Problemen des Informationszugangs in Deutschland und Europa beschäftigt. Es wurde festgelegt, dass der Vorsitz in der Arbeitsgemeinschaft halbjährlich wechselt. Nach dem Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein übernimmt mit Wirkung vom 1. Februar 2002 die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen den Vorsitz in der Arbeitsgemeinschaft, die seit dem 1. Januar 2002 zugleich für die Informationsfreiheit in ihrem Bundesland zuständig ist.

4 Internationales Symposium „Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union“

Informationsfreiheit und Datenschutz sind seit Verabschiedung der Europäischen Grundrechte-Charta wesentliche Bestandteile der entstehenden Europäischen Verfassung und gehören damit auch zu den Regelungen, die die beitrittswilligen Staaten Mittel- und Osteuropas in ihre Rechtsordnungen aufzunehmen haben. Zugleich können sich aber auch die bisherigen Mitgliedsländer der Europäischen Union die Erfahrungen zu Nutze machen, die etwa in Ungarn mit dem ersten in Europa verabschiedeten Informationszugangs- und Datenschutzgesetz gemacht worden sind. Die bevorstehende Erweiterung der Europäischen Union ist deshalb keine Einbahnstraße in west-östlicher Richtung. Brandenburg bieten sich daher aufgrund seiner geografischen Lage in den nächsten Jahren besondere Chancen.

Wir haben diesen Prozess zum Thema unseres Internationalen Symposiums **„Informationsfreiheit und Datenschutz in der Erweiterten Europäischen Union“** gemacht, das am 8. und 9. Oktober 2001 gemeinsam mit der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik e.V. in Potsdam veranstaltet wurde. Expertinnen und Experten aus Mittel- und Osteuropa tauschten während der Konferenz ihre

Erfahrungen mit Fachleuten aus Brandenburg, der Bundesrepublik Deutschland und Institutionen der Europäischen Union aus.

Neben internationalen Gästen nahmen vor allem Verantwortliche für den Datenschutz und den Informationszugang aus brandenburgischen Verwaltungen, aber auch Beschäftigte der privaten Wirtschaft sowie von Nicht-Regierungs-Organisationen an der Veranstaltung teil. Ebenso wie interessierte Bürgerinnen und Bürger erfuhren sie von ganz unterschiedlichen Problemen und Erfolgen in den einzelnen Staaten und brachten die spezifisch brandenburgischen Erfahrungen – insbesondere mit dem Recht auf Informationszugang – in die Diskussion ein.

Schwerpunkte waren der Datenschutz und die Medienberichterstattung, der Datenschutz bei Finanztransaktionen, Electronic Government und der Informationszugang als Dienstleistung der europäischen und deutschen Verwaltung. Die Vorträge, die auf dem Symposium gehalten wurden, können aus unserem Internet-Angebot abgerufen werden. Wir stellen auch auf Anfrage gerne eine gedruckte Version zur Verfügung.

5 Öffentlichkeitsarbeit

5.1 Aktuelle Publikationen des Landesbeauftragten

In diesem Jahr hat der Landesbeauftragte verschiedene Gesetzestexte erstmals herausgegeben. So ist das neue Bundesdatenschutzgesetz, dessen Bestimmungen auch für brandenburgische Unternehmen gelten, jetzt bei uns erhältlich. Auch das Umweltinformationsgesetz, das die Anspruchsgrundlage für den allgemeinen Zugang zu behördlichen Umweltinformationen darstellt, wurde neu in unsere Reihe „Brandenburgisches Informationsgesetzbuch“ aufgenommen. Beide Gesetzestexte ergänzen das bereits seit Längerem in dieser Reihe verfügbare Brandenburgische Datenschutzgesetz sowie das Akteneinsichts- und Informationszugangsgesetz, das wir in einer Neuauflage zusammen mit der dazugehörigen Landesgebührenordnung publiziert haben und Interessierten gerne zur Verfügung stellen.

Viele Behörde und Kommunen im Land Brandenburg bemühen sich um eine bürgerfreundliche Verwaltung und richten zentrale Service-Stellen ein. Bürgerinnen und Bürger finden dort unter anderem durch Broschüren und Veröffentlichungen verschiedener öffentlicher und nicht öffentlicher Stellen erste Informationen. Gerne stellen wir Faltblätter, die eine übersichtliche Einführung in die Themen „Datenschutz“ und „Informationszugang“ bieten, auch in größeren Mengen für die Auslage in allgemein zugänglichen Räumen zur Verfügung.

5.2 Der Landesbeauftragte auf dem Brandenburg-Tag

Auf dem Marktplatz in Luckau standen der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht sowie seine Mitarbeiterinnen und Mitarbeiter im September allen Besucherinnen und Besuchern des Brandenburg-Tages für Informationen zur Verfügung. Wie bereits im Vorjahr in Frankfurt (Oder) nutzten zahlreiche Interessierte die Gelegenheit, Fragen zu ihren Grundrechten auf Datenschutz und Informationszugang zu stellen.

So erkundigten sich viele, wie es sein kann, dass Unternehmen ihre Adresse für Werbezwecke nutzen und sich so der Briefkasten mit unerwünschter Post füllt, andere interessierten sich dafür, welche ihrer Daten von den Meldeämtern weitergegeben werden dürfen und wie sie dies verhindern können. Von großem Interesse war auch die Frage, was zu tun ist, um in Akten der Gemeinde oder des Landkreises einzusehen. Für umfangreichere Beratungen konnten auch individuelle Termine mit uns vereinbart werden.

Der Landesbeauftragte wird auch auf dem Brandenburg-Tag 2002 in Neuruppin wieder präsent sein. Wir freuen uns auf ein ebenso reges Interesse und ähnlich intensive Diskussionen wie im zurückliegenden Jahr.

Kleinmachnow, den 13. März 2002

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht

Anlagen

Anlage 1

Rede des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, vor dem Landtag Brandenburg am 24. Januar 2001 zum Tätigkeitsbericht 1999

Herr Präsident,

sehr geehrte Damen und Herren,

Datenschutz und Informationszugang sind Grundrechte, die unsere Landesverfassung als einzige in Deutschland gemeinsam garantiert und die zu achten ständige Aufgabe der Behörden in Brandenburg ist.

Der Landesbeauftragte ist zur Wahrung dieser Grundrechte vom Landtag gewählt worden. Die Verantwortung für die Einhaltung der gesetzlichen Bestimmungen zu Datenschutz und Akteneinsicht liegt allerdings bei den Leitern der öffentlichen Stellen des Landes, der Ämter und Gemeinden. Ich betone dies deshalb, weil ich regelmäßig dem Missverständnis begegne, der Landesbeauftragte oder die behördlichen Datenschutzbeauftragten hätten den Datenschutz zu gewährleisten. Datenschutz und Verwaltungstransparenz sind vielmehr in jeder brandenburgischen Behörde „Chefsache“, und wo sie dies noch nicht sind, sollten sie es werden.

Unser Tätigkeitsbericht 1999 ist mit der Stellungnahme der Landesregierung eingehend im Innenausschuss behandelt worden. Dafür, dass dies in sachlicher Form geschehen ist, bin ich den Mitgliedern des Ausschusses dankbar, auch wenn sie nicht in allen Punkten meinen Argumenten gefolgt sind.

Ausländerfeindlichkeit und Gewaltbereitschaft nehmen in unserem Land in erschreckender Weise zu. Sie richten sich zum Teil auch gegen die rechtsstaatliche Verfassung. Um dem zu begegnen, müssen alle rechtlichen Möglichkeiten der Polizei, der Strafverfolgungsbehörden wie auch des Verfassungsschutzes ausgeschöpft werden. Aber selbst die Feinde des Rechtsstaats dürfen nur mit den Mitteln des Rechtsstaats, das heißt auch unter strikter Beachtung der zugelassenen Wege der Datenerhebung und -nutzung bekämpft werden. Erst wenn diese nicht ausreichen sollten, wofür ich bisher keine Anhaltspunkte sehe, sollte über mögliche Änderungen nachgedacht werden.

Das Internet wird zu einem immer wichtigeren Medium. Es fördert die Zugänglichkeit von Informationen und den internationalen Austausch von Ideen. Ich begrüße deshalb die Initiative der Landesregierung, um möglichst bald alle Schulen mit Internet-Anschlüssen auszustatten. Ebenso wichtig ist es aber, den Schülern wie auch den Lehrern eine entsprechende Medienkompetenz zu vermitteln, damit die Chancen des weltweiten Netzes genutzt werden können, ohne die Risiken - auch in datenschutzrechtlicher Hinsicht - zu unterschätzen. Es bedarf hier einer nachhaltigen Anstrengung aller beteiligten Stellen, um das Bewusstsein für die Notwendigkeit und Möglichkeit des Selbstschutzes im Netz zu wecken. Ohne dieses Bewusstsein wird die Nutzung der neuen Medien stets von einem gravierenden Vertrauensverlust bedroht sein.

Akteneinsicht dient der Herstellung von Transparenz in der öffentlichen Verwaltung. Dass die Verwaltung transparenter werden muss, zeigen zwei aktuelle Beispiele:

Der BSE-Skandal führt gegenwärtig zu verstärkten Forderungen nach mehr Transparenz bei der Nahrungsmittel-Herstellung. Das betrifft auch die Tätigkeit der Behörden, die den gesundheitlichen Verbraucherschutz zu überwachen haben. Bereits vor 20 Jahren konnten britische Journalisten in den USA die Ergebnisse der Kontrollen amerikanischer Behörden bei solchen britischen Betrieben einsehen, deren Erzeugnisse in die USA exportiert werden sollten. Weil die britischen Behörden keine Akteneinsicht gewähren mussten, waren deren Kontrollergebnisse zuvor nie publik geworden. Das Beispiel zeigt, dass es bald auch international keine Inseln der Intransparenz mehr geben wird. Brandenburg, dessen Produkte über die Landesgrenzen hinweg verkauft werden, ist erfreulicherweise schon seit fast drei Jahren keine solche Insel mehr. Möglicherweise stärkt das auch das Vertrauen der Verbraucher in die brandenburgischen Produkte. Transparenz könnte so zum Standortvorteil werden.

Die Zunahme der Korruptionskriminalität hat dazu geführt, dass zu Beginn dieses Jahres eine eigene Schwerpunktstaatsanwaltschaft in Brandenburg gebildet worden ist. Die Stadt Cottbus erwägt die Berufung eines Anti-Korruptionsbeauftragten. Größtmögliche Transparenz in der Verwaltung kann den Kampf gegen die Korruption unterstützen. Eine Behörde, die sich darauf einstellt, dass ihre Akten und Dateien jederzeit von interessierten Bürgern eingesehen werden können, ist zwar nicht völlig gefeit gegen Korruption, aber sie erschwert Bestechungsversuche damit zusätzlich.

Als unabhängige Kontrollinstanz hat der Landesbeauftragte Verstöße gegen den Datenschutz und das Recht auf Akteneinsicht festzustellen und gegebe-

nenfalls zu beanstanden. Diese Aufgabe wird er auch weiterhin verantwortungsbewusst wahrnehmen. Das kann bedeuten, dass der Landesbeauftragte festgestellte Mängel öffentlich macht. Ich verstehe meine Aufgabe darüber hinaus auch in der Weise, dass ich der Verwaltung im Rahmen des Möglichen konstruktive Empfehlungen zu geben habe, wie sie ihre legitimen Ziele in gesetzeskonformer Weise erreichen kann. Die Verwaltung ist gut beraten, diese Empfehlungen aufzugreifen.

Herzlichen Dank für Ihre Aufmerksamkeit.

Anlage 2

Entwurf

für ein Gesetz zur Änderung des Akteneinsichts- und Informationszugangsgesetzes und des Verwaltungsverfahrensgesetzes für das Land Brandenburg

Vorbemerkung

Seit März 1998 ist das Brandenburgische Akteneinsichts- und Informationszugangsgesetz (AIG) in Kraft, mit dem das Grundrecht nach Artikel 21 Abs. 4 der Landesverfassung konkretisiert wird. Zum ersten Mal in der Bundesrepublik konnten in den zurückliegenden fast drei Jahren Erfahrungen mit einem allgemeinen verfahrensunabhängigen Informationszugangsrecht für alle Bürgerinnen und Bürger gesammelt werden. Zudem haben inzwischen zwei weitere Bundesländer (Berlin und Schleswig-Holstein) ebenfalls Informationsfreiheitsgesetze in Kraft gesetzt. Schließlich ist die neuere Rechtsprechung des Europäischen Gerichtshofes zum Umweltinformationsrecht auch bei allgemeinen Informationszugangsrechten zu berücksichtigen.

Die praktischen Erfahrungen des Landesbeauftragten und die Weiterentwicklung des Informationszugangsrechtes in Deutschland und in Europa lassen es angezeigt erscheinen, dass Brandenburgische Akteneinsichts- und Informationszugangsgesetz zu novellieren und in verfassungskonformer Weise weiterzuentwickeln.

A. In folgenden sechs zentralen Punkten werden Änderungen des Akteneinsichts- und Informationszugangsgesetzes und des Verwaltungsverfahrensgesetzes vorgeschlagen:

1. Art. 1 Erstes Gesetz zur Änderung des Akteneinsichts- und Informationszugangsgesetzes

1.1 § 1 wird wie folgt gefasst:

„Aufgabe

Aufgabe dieses Gesetzes ist es, dem Einzelnen, Bürgerinitiativen und Verbänden die Wahrnehmung ihres Grundrechts auf Akteneinsicht und

Informationszugang zu ermöglichen, soweit dem nicht überwiegende öffentliche oder private Interessen nach den §§ 4 und 5 entgegenstehen.“

BEGRÜNDUNG:

Entsprechend § 1 des Brandenburgischen Datenschutzgesetzes sollte auch in das Akteneinsichts- und Informationszugangsgesetz eine Festlegung des Normzwecks aufgenommen werden, die Bezug auf die verfassungsrechtliche Gewährleistung in Art. 21 der Landesverfassung nimmt.

1.2 § 2 Abs. 5 wird gestrichen.

BEGRÜNDUNG:

Der bisherige Ausschluss der Anwendbarkeit des AIG in laufenden Verfahren hat sich nicht bewährt. Er führt vielmehr dazu, dass ein Großteil des Verwaltungshandelns Bestimmungen unterliegt, die den Informationszugang nur sehr restriktiv zulassen. Dies ist mit dem verfassungsrechtlich garantierten Grundrecht auf voraussetzungslosen Informationszugang kaum zu vereinbaren. Zugleich führt das geltende Recht zu dem merkwürdigen Ergebnis, dass vor Beginn eines Verwaltungsverfahrens jede Person Akteneinsicht ohne Begründung verlangen kann, nach Beginn eines solchen Verfahrens jedoch nur die daran Beteiligten und diese auch nur insoweit, als die Kenntnis der Akten zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 29 Abs. 1 Satz 1 Verwaltungsverfahrensgesetz - VwVfG -).

Aus diesem Grund wird vorgeschlagen, das AIG auch in laufenden Verwaltungsverfahren anzuwenden und zugleich den Verfahrensbeteiligten eine voraussetzungslose Einsicht bei gleichzeitiger Wahrung berechtigter Geheimhaltungsinteressen (z.B. Datenschutz, Betriebs- und geschäftsgeheimnisse) zu ermöglichen (s. dazu unten A 2). Auf diese Weise würde ein einheitliches, gleichermaßen hohes Transparenzniveau innerhalb und außerhalb von Verwaltungsverfahren sichergestellt.

Das gerichtliche Verfahrensrecht ist im Übrigen bundesgesetzlich geregelt (Verwaltungsgerichtsordnung, Strafprozessordnung, Zivilprozessordnung) und geht dem AIG ohnehin vor. Insofern ist die bisherige Regelung des § 4 Abs. 5 AIG überflüssig.

1.3 § 5 wird wie folgt neu gefasst:

„Schutz privater Interessen

(1) Ein Recht auf Akteneinsicht besteht nicht, soweit

1. personenbezogene Daten offenbart werden und dem schutzwürdige Belange der Betroffenen entgegenstehen, ohne dass das Offenbarungsinteresse des Antragstellers das Interesse der Betroffenen an der vertraulichen Behandlung der Information überwiegt,

2. ein Betriebs- und Geschäftsgeheimnis offenbart würde, ohne dass das Offenbarungsinteresse des Antragstellers das schutzwürdige Interesse des Unternehmens an der Wahrung des Betriebs- und Geschäftsgeheimnisses überwiegt oder das Unternehmen der Offenbarung zugestimmt hat.

§ 4 Abs. 2 gilt entsprechend.

(2) Der Offenbarung personenbezogener Daten stehen schutzwürdige Belange der Betroffenen in der Regel nicht entgegen, soweit diese zustimmen oder sich aus der Akte ergibt, dass

1. die Betroffenen an einem Verwaltungsverfahren oder einem sonstigen Verfahren beteiligt sind,

2. eine gesetzlich vorgeschriebene Erklärung abgegeben oder eine Anzeige, Anmeldung, Auskunft oder vergleichbare Mitteilung durch die Betroffenen gegenüber einer Behörde erfolgt ist,

3. gegenüber dem Betroffenen überwachende oder vergleichbare Verwaltungstätigkeiten erfolgt sind,

4. die Betroffenen Eigentümer, Pächter, Mieter oder Inhaber eines vergleichbaren Rechts sind,
5. die Betroffenen als Gutachter, sachverständige Personen oder in vergleichbarer Weise eine Stellungnahme abgegeben haben

und durch diese Angaben mit Ausnahme von

- Namen,
- Titel, akademischem Grad,
- Geburtsdatum,
- Beruf, Branchen- oder Geschäftsbezeichnung,
- innerbetrieblicher Funktionsbezeichnung,
- Anschrift,
- Rufnummer

nicht zugleich weitere personenbezogene Daten offenbart werden.

Satz 1 gilt auch, wenn die Betroffenen im Rahmen eines Arbeits- oder Anstellungsverhältnisses oder als Vertreter oder Vertreterin oder Organ einer juristischen Person an einem Verwaltungsverfahren beteiligt sind, die Mitteilungen machen oder die Verwaltungstätigkeit ihnen gegenüber in einer solchen Eigenschaft erfolgt. § 16 des Brandenburgischen Datenschutzgesetzes findet keine Anwendung."

§ 5 Abs. 3 bleibt unverändert.

BEGRÜNDUNG:

Gegenwärtig regelt das Akteneinsichts- und Informationszugangsgesetz das Verhältnis zwischen Informationszugangsrecht einerseits und Recht auf informationelle Selbstbestimmung andererseits in der Weise, dass der Zugang zu personenbezogenen Daten ohne Zustimmung der (datenschutzrechtlich) Betroffenen grundsätzlich ausgeschlossen ist. Nur in zwei Fällen lässt das Gesetz Ausnahmen von diesem Verbot zu, wenn im Einzelfall im Hinblick auf den Zweck der politischen Mitgestaltung das Offenbarungsinteresse des Antragstellers das Geheimhaltungsinteresse der betroffenen Person überwiegt oder wenn es sich um Daten von Amtsträgern handelt, die an Verwaltungsvorgängen beteiligt sind.

Diese Regelung erscheint vor dem Hintergrund der brandenburgischen Landesverfassung, in der sowohl das Informationszugangsrecht als auch das Recht auf Datenschutz Grundrechtsqualität haben, als zu restriktiv. Der Gesetzgeber hat bisher nicht in ausreichendem Maße praktische Konkordanz zwischen diesen beiden Grundrechten hergestellt, sondern räumt im Regelfall dem Recht auf Datenschutz gegenüber dem Recht auf Informationszugang den Vorrang ein. In der Praxis führt diese Regelung häufig dazu, dass die Verwaltung den Zugang zu Informationen verweigern muss, weil personenbezogene Daten betroffener Bürger in den Verwaltungsvorgängen enthalten sind. Diese materiell-rechtliche Regelung wird noch verschärft durch die verfahrensrechtliche Vorschrift in § 6 Abs. 5 AIG, wonach die Zustimmung Dritter nur auf Verlangen des Antragstellers einzuholen ist und als verweigert gilt, wenn sie innerhalb von zwei Monate nach Aufforderung durch die aktenführende Behörde nicht vorliegt. In der Praxis versäumen es die aktenführenden Behörden zudem häufig, die Antragsteller darauf hinzuweisen, dass sie die Einholung der Zustimmung der betroffenen Bürger verlangen können.

Der Gesetzgeber sollte demgegenüber in einem novellierten Akteneinsichts- und Informationszugangsgesetz eine differenziertere Abwägung zwischen den Grundrechten auf Informationszugang und Datenschutz vornehmen, um eine praktische Konkordanz zwischen diesen prinzipiell gleichwertigen Verfassungsgewährleistungen zu erzielen. Ausgangspunkt für diese ausgewogene Regelung ist die mehrfach vom Bundesverfassungsgericht getroffene Feststellung, dass das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine“ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Viele Informationen, auch soweit sie personenbezogen sind, stellen ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen zugeordnet werden kann. Das Grundgesetz und die brandenburgische Landesverfassung haben die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Derartige Beschränkungen bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 65, 1, 43 f.).

Auch wenn es angesichts der modernen Datenverarbeitung keine belanglosen personenbezogenen Daten gibt, ist der Schutz des Grundrechts auf informationelle Selbstbestimmung innerhalb der Privatsphäre im engeren Sinne intensiver als im Bereich der Sozialsphäre, in der der Gesetzgeber einen weiteren Spielraum hat. Der strikte Vorrang der Berufs- und besonderen Amtsgeheimnisse nach § 4 Abs. 3 AIG bleibt unverändert bestehen. Dagegen sind personenbezogene Daten über Bürgerinnen und Bürger mit stärkerem Sozialbezug, insbesondere solche, die durch die Kontaktaufnahme mit der Verwaltung und die Beteiligung an Verwaltungsverfahren entstehen, nicht in vergleichbarer Weise schutzwürdig. Eine derartige Regelung würde es zuverlässiger ausschließen, dass - wie in der Vergangenheit zum Teil geschehen - der Datenschutz als Vorwand zur Informationsverweigerung benutzt wird.

Mit der Formulierung „Ein Recht auf Akteneinsicht besteht nicht, soweit...“ wird der Verwaltung abweichend vom bisher geltenden Recht ein gewisser Ermessenspielraum eröffnet.

Zugleich ist durch die Formulierung „in der Regel“ in Abs. 2 des neuen § 5 sichergestellt, dass nicht ausnahmslos in allen Fällen die in dieser Vorschrift genannten personenbezogenen Daten von der Verwaltung offen gelegt werden dürfen. Soweit im Einzelfall selbst in diesen Fällen schutzwürdige Belan-

ge der Betroffenen dem Informationszugang entgegenstehen, ist er zu verweigern. Insgesamt würde die vorgeschlagene Aufnahme einer Liste mit Regelfallbeispielen in das Gesetz das Informationszugangsrecht der Bürgerinnen und Bürger stärken, ohne das Grundrecht auf Datenschutz der Betroffenen in unverhältnismäßiger Weise einzuschränken. Zugleich ist die neue Regelung durch ein höheres Maß an Normenklarheit gekennzeichnet.

Der Schutz geistigen Eigentums und insbesondere das Urheberrecht, die nach geltendem Recht zur Ablehnung von Akteneinsichtsanträgen zwingen, stehen nach richtiger Auffassung nicht dem Informationszugang, sondern nur der unkontrollierten Vervielfältigung und Weitergabe von urheberrechtlich geschützten Informationen entgegen. Das zeigt auch ein Blick auf die Rechtslage in anderen Ländern der Europäischen Union mit Informationsfreiheitsgesetzgebung[1]. Der ausdrückliche Verweis auf den Urheberrechtsschutz hat außerdem keine praktische Bedeutung in der Gesetzesanwendung erlangt. Falls es zu Konflikten in diesem Bereich kommen sollte, würde das Urheberrechtsgesetz des Bundes ohnehin Vorrang vor dem AIG haben. Im Interesse einer schlankeren und übersichtlicheren gesetzlichen Regelung sollte § 5 Abs. 1 Nr. 2 deshalb gestrichen werden.

Der Schutz von unternehmensbezogenen Angaben ist im geltenden Recht nicht angemessen geregelt. Zum einen ist in § 5 Abs. 1 Nr. 3 eine Definition der Betriebs- und Geschäftsgeheimnisse übernommen worden, die es praktisch in das Belieben des betroffenen Unternehmens stellt, ob eine Information geheim zu halten ist oder nicht. Das einzige objektive Kriterium, nämlich das schutzwürdige Interesse des Unternehmens an der Geheimhaltung ist nämlich durch das Wort „oder“ statt des sonst üblicherweise verwandten „und“ praktisch irrelevant geworden. Richtigerweise muss die aktenführende Stelle in jedem Fall, also gerade auch dann, wenn ein Unternehmen eine Information geheim gehalten wissen will, selbständig überprüfen, ob an deren Geheimhaltung ein schutzwürdiges Interesse besteht. Diese Bewertung ist ihrerseits justitiabel. Das geltende AIG lässt diese Handhabung aber nicht zu, sondern überlässt den Unternehmen das letzte Entscheidungsrecht darüber, ob Informationen in behördlichen Unterlagen geheim zu halten sind oder nicht. Hinzu kommt, dass das geltende Recht von einer verfassungsrechtlich problematischen Asymmetrie im Verhältnis zwischen dem Schutz personenbezogener Daten einerseits und dem Schutz von Unternehmensdaten andererseits gekennzeichnet ist. Während personenbezogene Daten ausnahmsweise im Einzelfall im Hinblick auf den Zweck der politischen Mitgestaltung offen gelegt werden dürfen, wenn das Offenbarungsinteresse das Geheimhaltungsinteresse überwiegt, ist eine solche Möglichkeit bei unternehmens-

[1] Vgl. Grünbuch der EU-Kommission „Informationen des öffentlichen Sektors - eine Schlüsselressource für Europa, Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft“ KOM(98) 585 endg.; Ratsdok. 5580/99; BR-Drs. 93/99

bezogenen Daten im Gesetz generell nicht vorgesehen. Dies führt zu einem verfassungsrechtlich nicht vertretbaren erhöhten Schutz von unternehmensbezogenen Daten im Vergleich zu personenbezogenen Daten.

1.4 In § 6 Abs. 1 werden die Sätze 2 und 4 ersatzlos gestrichen.

§ 6 Abs. 3 wird wie folgt neu gefasst:

„Kommt die Akten führende Stelle bei der Prüfung eines Antrags auf Akteneinsicht zu der Auffassung, dass der Offenbarung von personenbezogenen Daten oder Betriebs- oder Geschäftsgeheimnissen keine schutzwürdigen Belange Betroffener entgegenstehen, oder dass der Gewährung der Akteneinsicht zwar schutzwürdige Belange Betroffener entgegenstehen, das Informationsinteresse aber gegenüber dem Interesse der Betroffenen an der Geheimhaltung überwiegt, so hat sie den Betroffenen Gelegenheit zu geben, sich innerhalb von drei Wochen zu den für die Entscheidung erheblichen Tatsachen zu äußern. Die Entscheidung ist auch den Betroffenen bekannt zu geben. Gegen die Entscheidung können die Betroffenen Widerspruch einlegen. Die Akteneinsicht darf erst nach Eintritt der Bestandskraft der Entscheidung gegenüber den Betroffenen oder zwei Wochen nach Anordnung der sofortigen Vollziehung, die auch den Betroffenen bekannt zu geben ist, gewährt werden."

Der bisherige § 6 Abs. 5 Satz 2 wird zum Satz 3 und wie folgt gefasst:

„Liegt innerhalb von drei Wochen nach Aufforderung durch die Akten führende Behörde eine Zustimmung Betroffener zur Offenbarung personenbezogener Daten nicht vor, gilt die Zustimmung als verweigert; liegt die Zustimmung einer Behörde nach § 4 Abs.1 Nr.2 oder eines Unternehmens nach § 5 Abs.1 Nr.2 innerhalb dieser Frist nicht vor, gilt sie als erteilt."

BEGRÜNDUNG:

Die Streichung in § 6 Abs.1 ist redaktioneller Natur (Folgeänderung).

Die Neufassung des § 6 Abs. 3 beruht auf praktischen Erfahrungen des Landesbeauftragten mit Fällen der Akteneinsicht, in denen Betroffene Rechtsbehelfe gegen die Erteilung der Akteneinsicht angekündigt, aber nicht eingelegt haben und Rechtsunsicherheit darüber bestand, ob Akteneinsicht vor Eintritt der Bestandskraft gewährt werden darf. Zudem soll die neue Vorschrift die Anhörung Betroffener (Personen und Unternehmen) in allen Fällen der not-

wendigen Abwägung zwischen dem Informationsinteresse und dem Geheimhaltungsinteresse eindeutig regeln.

Die Änderung in § 6 Abs. 5 beruht auf folgender Überlegung:

Die bisher vorgesehene 2-Monatsfrist, innerhalb derer die Zustimmung Dritter einzuholen ist, verzögert den Informationszugang unverhältnismäßig. Damit die Akten führende Stelle innerhalb der zu § 6 Abs.6 AIG (neu - s. unten Ziffer 1.5) vorgeschlagenen regelmäßigen Frist von einem Monat über den Antrag auf Akteneinsicht entscheiden kann, muss die Zustimmungsfrist entsprechend kürzer sein.

Das geltende Gesetz sieht eine fingierte Zustimmungsverweigerung in dem Fall vor, dass die Zustimmung innerhalb der Frist nicht vorliegt. Dies entspricht dem datenschutzrechtlichen Grundsatz, dass Schweigen nicht als Zustimmung zur Verarbeitung personenbezogener Daten gewertet werden darf. Insofern soll die Verweigerungsfiktion bei der Offenlegung personenbezogener Daten beibehalten werden. Nicht gerechtfertigt ist diese gesetzliche Fiktion aber bei der Offenlegung von unternehmensbezogenen Informationen (Betriebs- und Geschäftsgeheimnissen) und bei der Beteiligung anderer Behörden. Hier ist vielmehr - wie auch sonst im kaufmännischen Rechtsverkehr - eine Zustimmungsfiktion angemessener. Vergleichbare Regelungen finden sich auch in § 111 Abs. 3 Satz 2 GWB (für Betriebs- und Geschäftsgeheimnisse) und in § 11 Satz 3 der Neunten Verordnung zur Durchführung des Bundesimmissionsschutzgesetzes (zur Beteiligung anderer Behörden).

1.5 In § 6 wird folgender neuer Absatz 6 angefügt:

> „Über den Antrag ist sobald wie möglich, spätestens jedoch einen Monat nach seinem Eingang bei der Akten führenden Behörde zu entscheiden."

BEGRÜNDUNG:

Dieser Änderungsvorschlag ist von zentraler Bedeutung. Das AIG sieht eine Bearbeitungsfrist bisher nicht vor. Darin liegt eine wesentliche Schwäche des Gesetzes, wie die praktische Erfahrung in Brandenburg zeigt. Viele Akten führende Stellen berücksichtigen die Bedeutung der Aktualität von Informationen bei der Gesetzesanwendung nicht ausreichend. Zwar sieht das geltende Umweltinformationsgesetz noch eine 2-Monatsfrist vor, der Vorschlag zur Neufassung der Europäischen Umweltinformationsrichtlinie enthält jedoch eine Halbierung dieser Frist. Nach kanadischem Bundesrecht beträgt die Frist einen Monat, nach dem amerikanischen Freedom of Information Act beträgt die Frist im Regelfall 20 Arbeitstage.

1.6 Es wird folgender neuer § 7 a eingefügt:

„Veröffentlichungspflichten, Aktenführung

(1) Akten führende Behörden i. S. d. § 2 haben Verzeichnisse zu führen, die geeignet sind, die Aktenordnung und den Aktenbestand sowie den Zweck der geführten Akten erkennen zu lassen. Diese Verzeichnisse sind in allgemein verständlicher Weise zu veröffentlichen. Entsprechendes gilt für Verwaltungsvorschriften , die von der Akten führenden Behörde erlassen worden sind. Möglichkeiten der Veröffentlichung in elektronischer Form sind entsprechend dem Stand der Technik zu berücksichtigen.

(2) Die Akten führenden Behörden treffen geeignete organisatorische Vorkehrungen, damit Informationen, die nach § 4 und 5 nicht eingesehen werden können, möglichst ohne unverhältnismäßigen Aufwand von einsehbaren Informationen abgetrennt werden können."

BEGRÜNDUNG:

Die Verwaltung sollte dazu verpflichtet werden, Aktenpläne und -verzeichnisse zu führen und zu veröffentlichen. Dies würde den Antragstellern die Beurteilung ermöglichen, zu welchen Themen die Behörde überhaupt Akten führt und ob ein Antrag auf Akteneinsicht Erfolg verspricht. Das Gleiche gilt für Verwaltungsvorschriften, die die Akten führende Behörde erlassen hat. Aktenpläne und -verzeichnisse müssten als Wegweiser in verständlicher Form für die Bürgerinnen und Bürger veröffentlicht werden.

Zugleich würde eine solche Vorschrift die Verwaltung von Einzelanträgen entlastet, was insbesondere die Erfahrungen mit dem Electronic Freedom of Information Act in den USA zeigen. Das brandenburgische Akteneinsichts- und Informationszugangsgesetz würde auf dieses Weise „internetfähig".

Außerdem sollte die Aktenführung und Datenverarbeitung entsprechend § 4 Abs. 5 des Brandenburgischen Datenschutzgesetzes und § 15 des Schleswig-Holsteinischen Informationsfreiheitsgesetzes so organisiert werden, dass eine Trennung von einsichtsfähigen Informationen einerseits und nicht einsichtsfähigen (z. B. geheimhaltungsbedürftigen) Informationen andererseits ohne großen Aufwand erfolgen kann.

2. Art. 2 Gesetz zur Änderung des Verwaltungsverfahrensgesetzes für das Land Brandenburg

§ 29 wird wie folgt gefasst:

„Akteneinsicht

(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten. Satz 1 gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung. Soweit nach den §§ 17 und 18 eine Vertretung stattfindet, haben nur die Vertreter Anspruch auf Akteneinsicht.

(2) Die Regelungen der §§ 4 und 5 des Akteneinsichts- und Informationszugangsgesetzes gelten entsprechend.

(3) (unverändert)

(4) Für Nichtbeteiligte gilt das Akteneinsichts- und Informationszugangsgesetz.

(5) § 72 Abs. 1 ist mit der Maßgabe anzuwenden, dass die Regelungen des Akteneinsichts- und Informationszugangsgesetzes uneingeschränkt auch im Planfeststellungsverfahren gelten."

BEGRÜNDUNG:

Die vorgeschlagene Regelung dient der Harmonisierung der Akteneinsichtsrechte innerhalb und außerhalb des Verwaltungsverfahrens (s. o. Ziff. 1.2).

B. Auch in einer Reihe von Detailfragen legt die praktische Erfahrung mit dem ersten deutschen Informationszugangsgesetz Änderungen nahe[2]:

1. In § 2 Abs. 4 wird das Wort „hoheitlicher" durch das Wort „ihrer" ersetzt.

BEGRÜNDUNG:

Das AIG gilt bisher für Private nur dann, wenn eine öffentliche Stelle sich ihrer zur Erledigung hoheitlicher Aufgaben bedient. Im Zusammenhang mit der verstärktem Privatisierung im Bereich der öffentlichen Verwaltung werden jedoch Unternehmen zunehmend mit der Erfüllung von Verwaltungsaufgaben

[2] Alle Paragraphen ohne Zusatz sind solche des AIG.

betraut, die nicht zwingend hoheitlich sind. In der Praxis werden aber auch nicht-hoheitliche Verwaltungsaufgaben Privaten übertragen. Die vorgeschlagene Gesetzesänderung soll bewirken, dass die Einsehbarkeit von Unterlagen nicht nach der Rechtsform der Akten führenden Stelle, sondern nach dem Charakter der zu erledigenden Aufgabe zu beurteilen ist. Eine Flucht der Verwaltung in privatrechtliche Formen der Aufgabenerfüllung darf nicht zur Absenkung des verfassungsrechtlich vorgeschriebenen Transparenzniveaus führen. Zwar handelt es sich bei vielen dieser Aufgaben um Angelegenheiten, bei deren Erledigung die Unternehmen im Wettbewerb stehen. Der Schutz von Unternehmensdaten ist jedoch in § 5 AIG ausreichend geregelt.

2. Es wird folgender neuer § 2 Abs. 5 eingefügt:

   „Soweit Akten führende Stellen nach den Absätzen 1 oder 4 um Zustimmung zur Offenbarung von Unterlagen solcher Stellen gebeten werden, die nicht dem Anwendungsbereich dieses Gesetzes unterfallen, haben sie dieses Gesetz anzuwenden."

BEGRÜNDUNG:

Da es zunehmend auch in anderen Bundesländern Informationszugangsgesetze gibt, entsteht ein Problem, das bei der Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes wegen seiner damaligen Singularität noch nicht auftreten konnte. Öffentliche Stellen des Landes Brandenburg können von Stellen anderer Bundesländer oder des Bundes um Zustimmung zur Offenbarung dort vorliegender Akten gebeten werden, soweit sie Angaben und Mitteilungen öffentlicher Stellen des Landes Brandenburg enthalten . In diesem Fall darf die brandenburgische Stelle ihre Zustimmung nicht ohne weiteres verweigern, sondern muss hierbei die Maßstäbe des Akteneinsichts- und Informationszugangsgesetzes zugrunde legen. Akten und Unterlagen aus Brandenburg verlieren ihre Einsichtsfähigkeit nicht dadurch, dass sie Bestandteil von Akten in solchen Bundesländern oder Verwaltungen werden, für die ebenfalls Informationsfreiheitsgesetze gelten.

3. In § 4 wird die Überschrift wie folgt geändert:

   „Schutz öffentlicher Interessen"

   In § 4 Abs. 1 werden die Worte „Der Antrag auf Akteneinsicht ist abzulehnen, wenn" ersetzt durch die Worte „Ein Recht auf Akteneinsicht besteht nicht, soweit"

BEGRÜNDUNG:

Durch diese Änderung soll der Akten führenden Stelle ein gewisser Ermessensspielraum eröffnet werden, der bisher nicht besteht. Vor dem Hintergrund des Grundrechts aus Artikel 21 Abs. 4 der Landesverfassung erscheint es als problematisch, die in § 4 Abs. 1 genannten öffentlichen Interessen stets zwingend dem Recht auf politische Mitgestaltung überzuordnen. Gleiches gilt auch für die in Absatz 2 genannten Geheimhaltungsinteressen. Der Verwaltung bleibt nach der vorgeschlagenen Neufassung die Möglichkeit, in allen Fällen des bisherigen § 4 (Absätze 1 und 2) die Akteneinsicht nach einer fehlerfreien Ausübung ihres Ermessens zu verweigern, in Einzelfällen kann sie aber dem verfassungsrechtlichen Informationszugangsrecht den Vorrang einräumen.

Im Übrigen wird durch die Einfügung des Wortes „soweit“ klargestellt, dass stets eine differenzierende Entscheidung über den Antrag auf Akteneinsicht erforderlich ist.

4. In § 4 Abs.1 Nr. 5 werden die Worte „oder die der Aufsicht über eine andere Stelle dienen“ gestrichen.

BEGRÜNDUNG:

Aufsichtsakten geben Aufschluss darüber, welche Beanstandungen eine Aufsicht führende Stelle gegenüber der beaufsichtigten Stelle trifft oder weshalb sie von Beanstandungen absieht, welche Fragen zur Ermittlung des Sachverhalts gestellt wurden und wie die beaufsichtigte Behörde reagiert hat. Dies pauschal geheim zu halten ist nicht gerechtfertigt. Das Gesetz enthält eine Vielzahl anderer Ausnahmevorschriften, die den Schutz überwiegender öffentlicher Interessen ausreichend sicherstellen. Der Aufsichtsprozess an sich bedarf eines solchen Schutzes nicht. Das zeigen auch die praktischen Erfahrungen, die der Landesbeauftragte für das Recht auf Akteneinsicht mit Bürgereingaben gemacht hat. Es würde vielmehr das Vertrauen der Bürgerinnen und Bürger in eine effektiv arbeitende Aufsicht erhöhen, wenn die entsprechenden Akten prinzipiell zugänglich wären und nicht stärker geheimgehalten würden als andere Verwaltungsvorgänge.

5. In § 4 Abs. 2 werden die Worte „Der Antrag auf Akteneinsicht soll abgelehnt werden,“ gestrichen. § 4 Abs. 2 Nr.1 wird § 4 Abs. 1 Nr. 6 und wie folgt gefasst:

„6. soweit sich der Inhalt der Akten auf den nicht-abgeschlossenen Prozess der Willensbildung innerhalb von und zwischen Behörden oder Verwaltungseinrichtungen bezieht, wenn durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg bevorstehender behördlicher Maßnahmen gefährdet würde; dies gilt nicht für die Ergebnisse von abgeschlossenen Verfahrenshandlungen eines Verwaltungsverfahrens, die für die Entscheidung verbindlich sind, insbesondere Ergebnisse von Beweiserhebungen und Stellungnahmen; „

6. § 4 Abs. 2 Nr. 2 wird § 4 Abs. 1 Nr. 7 und wie folgt gefasst:

„7. soweit sich der Inhalt der Akten auf Vorgänge bezieht, die nach § 44 der Gemeindeordnung oder § 38 der Landkreisordnung in nicht öffentlicher Sitzung zu beraten oder zu beschließen sind oder in nicht öffentlicher Sitzung beraten oder beschlossen worden sind.“

BEGRÜNDUNG:

Der behördliche Entscheidungsprozess sollte nur solange von der Akteneinsicht ausgenommen sein, wie er noch nicht abgeschlossen ist und soweit ein Bekanntwerden des Akteninhalts behördliche Maßnahmen konterkarieren würde.

Für eine darüber hinausgehende Ausnahmevorschrift, wie sie der bisherige § 4 Abs. 2 Nr. 2 AIG enthält, besteht daneben kein Bedarf, denn die Akteneinsicht kann den Erfolg bevorstehender behördlicher Maßnahmen immer nur dann gefährden, wenn zugleich der behördliche Entscheidungsprozess betroffen ist. Stattdessen sollte der bisher in § 4 Abs. 2 Nr. 1 zweiter Halbsatz geregelte Fall der nach Kommunalrecht in nicht öffentlicher Sitzung zu behandelnden Vorgänge geregelt werden.

7. § 4 Abs. 2 Nr. 3 wird gestrichen.

BEGRÜNDUNG:

Die Einsicht in nicht-abgeschlossene Schriftstücke oder Entwürfe wird ausreichend bereits durch die (modifizierte) Ziffer 1 in § 4 Abs. 2 geregelt. Eines zusätzlichen Schutzes „nicht abgeschlossener Schriftstücke“ oder vorbereitender Arbeiten bedarf es deshalb nicht.

8. In § 4 Abs. 2 werden die Worte „es sei denn, dass das Interesse an der Einsichtnahme das entgegenstehende öffentliche Interesse im Einzelfall überwiegt“ ersetzt durch die Worte

   „und wenn das öffentliche Interesse an der Geheimhaltung das Interesse an der Einsichtnahme im Einzelfall überwiegt.“

BEGRÜNDUNG:

Das bisher geltende Regel-Ausnahme-Verhältnis soll zu Gunsten der Akteneinsicht verändert werden. Die Ablehnung der Akteneinsicht sollte in Zukunft nur noch die Ausnahme in den Fällen des § 4 Abs. 2 sein. Dies würde der Voraussetzungslosigkeit des Einsichtsanspruches besser Rechnung tragen, während es bisher notwendig war, dass der Antragsteller sein überwiegendes Einsichtsinteresse darlegt, um die Verwaltung trotz entgegenstehender öffentlicher Interessen ausnahmsweise zur Einsichtsgewährung zu veranlassen.

9. § 4 Abs. 2 Nr. 4 wird zu § 4 Abs. 1 Nr. 8.
   § 4 Abs. 3 wird zu § 4 Abs. 2.

BEGRÜNDUNG:

Auch bei den hier genannten öffentlichen Geheimhaltungsinteressen besteht nach der vorgeschlagenen Neufassung ein Ermessensspielraum der Verwaltung.

10. In § 6 Abs. 1 wird folgender neuer Satz 8 angefügt:

    „Der Antragsteller ist im Ablehnungsbescheid auf sein Recht nach § 11 Abs. 2 Satz 1 hinzuweisen.“

BEGRÜNDUNG:

Wird Akteneinsicht abgelehnt, so ist den Antrag stellenden Bürgerinnen und Bürgern häufig nicht bekannt, dass sie - unabhängig von der Möglichkeit, förmliche Rechtsbehelfe einzulegen - das Recht haben, den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht anzurufen. Eine entsprechende Hinweispflicht gilt bereits für die Verfassungsschutzbehörde nach § 12 Abs. 3 Satz 2 des Brandenburgischen Verfassungsschutzgesetzes.

11. § 6 Abs. 3 Satz 2 wird gestrichen.

BEGRÜNDUNG:

Die Vorschrift ist entbehrlich, da der Schutz von Betriebs- und Geschäftsgeheimnissen neu geregelt wird. Sie hat im übrigen in der Vergangenheit auch keine praktische Bedeutung erlangt hat.

12. In § 6 Abs. 5 wird folgender neuer Satz 2 eingefügt:

„Der Antragsteller ist auf diese Möglichkeit hinzuweisen."

BEGRÜNDUNG:

Die Behörde ist nur dann zur Einholung der Zustimmung Dritter verpflichtet, wenn der Antragsteller sie dazu auffordert. An diesem Grundsatz soll nichts geändert werden. Allerdings ist diese Möglichkeit häufig nicht bekannt und die Erfahrungen des Landesbeauftragten zeigen, dass die Verwaltung auch kein Interesse daran hat, ohne eine rechtliche Verpflichtung die Antragsteller auf diese Möglichkeit hinzuweisen. Häufig werden Verweigerungen der Akteneinsicht durch die Akten führenden Stellen pauschal damit begründet, dass eine Zustimmung Dritter nicht vorliege, ohne dass der Versuch unternommen wurde, sie einzuholen. Diese Praxis sollte der Gesetzgeber beenden.

13. § 6 Abs. 5 Satz 3 wird gestrichen.

BEGRÜNDUNG:

Die Vorschrift hatte bisher in der Praxis keine Bedeutung. Sie könnte zudem missverstanden werden als Einladung zu „Blankettverweigerungen".

14. In § 6 Abs. 5 wird folgender neuer Satz 4 angefügt:

„Angaben zur Person des Antragstellers dürfen bei der Einholung der Zustimmung Dritter nur mit Einverständnis des Antragstellers offenbart werden."

BEGRÜNDUNG:

Das Gesetz regelt bisher nicht die Frage, ob die Akten führende Stelle bei der Einholung der Zustimmung Dritter die Identität des Antragstellers preisgeben darf. Zum Teil geschieht dies routinemäßig, obwohl dazu kein Erfordernis besteht und der Antragsteller sein Einverständnis auch nicht erklärt hat. Durch die vorgeschlagene Regelung würde klargestellt, dass dieses Einverständnis erforderlich ist. Wird es verweigert, kann der Dritte (Betroffener, Unternehmen, Behörden) seinerseits die Erteilung der Zustimmung von der Offenlegung der Identität des Antragstellers abhängig machen.

15. In § 6 wird folgender neuer Absatz 7 angefügt:

„Lehnt die Akten führende Behörde die Akteneinsicht unter Berufung auf § 4 Abs. 1 Nrn. 3 - 5 oder § 4 Abs. 2 ab, so hat sie dem Antragsteller mitzuteilen, zu welchem Zeitpunkt eine Einsichtnahme voraussichtlich erfolgen kann."

BEGRÜNDUNG:

Die genannten Ausnahmetatbestände rechtfertigen es nur vorübergehend, das Grundrecht auf Informationszugang einzuschränken. Die Verwaltung sollte verpflichtet werden, den Antragstellern mitzuteilen, wann ihr Informationsinteresse voraussichtlich befriedigt werden kann.

16. § 7 wird wie folgt gefasst:

„Art und Weise der Gewährung des Akteneinsichtsrechts"

„Der Anspruch auf Akteneinsicht wird vorbehaltlich der in § 6 Abs. 2 und § 8 geregelten Ausnahmen durch Gewährung der Einsicht in die Originaldokumente erfüllt. Auf Verlangen des Antragstellers ist das Akteneinsichtsrecht durch

1. Übermittlung von Vervielfältigungen,
2. Verweis auf Dokumentationen und Veröffentlichungen der zuständigen Behörde,
3. elektronische Post,
4. Zurverfügungstellung von Informationsträgern in sonstiger Weise

zu gewähren, soweit sie die begehrten Informationen enthalten. Die Akten führende Behörde ist nicht verpflichtet, einem Verlangen des Antragstellers nach Satz 2 zu entsprechen, wenn hierfür im Einzelfall ge-

wichtige Gründe bestehen, die sie darzulegen hat. Das Recht auf Einsicht in die Originalunterlagen bleibt davon unberührt."

BEGRÜNDUNG:

Die geltende Fassung des Gesetzes, insbesondere der bisherige Satz 1 des § 7 wird in der Praxis von den Behörden häufig als Begründung dafür herangezogen, dass die Aushändigung von Fotokopien generell abgelehnt wird. Zum Teil wird sogar die Auffassung vertreten, das Gesetz lasse die Aushändigung von Fotokopien nur zu, wenn die Behörde dies vorschlägt und die Antragsteller dem zustimmen. Nach der Rechtsprechung des Bundesverwaltungsgerichts zum Umweltinformationsgesetz (Urteil vom 06.12.1996 - 7C64/95 -) hat der Informationsinteressent zwar kein Wahlrecht hinsichtlich des Formats, in dem ihm die gewünschte Information zur Verfügung zu stellen ist, andererseits ist das Auswahlermessen der Akten führenden Stelle jedoch stark eingeschränkt, so dass häufig nur eine Entscheidung, nämlich die Zurverfügungstellung von Fotokopien, ermessensfehlerfrei ist. Lediglich wenn gewichtige, von der Verwaltung darzulegende Gründe dagegen sprechen, dem Verlangen des Antragstellers nachzukommen, ist eine Ablehnung rechtmäßig. Dabei wird die Verwaltung auch abzuwägen haben, ob es kostengünstiger ist, dem Antragsteller gegen Auslagenerstattung auch eine größere Anzahl von Fotokopien zur Verfügung zu stellen oder ihm stattdessen einen oder sogar mehrere Bedienstete als unterstützende „Erklärungshelfer" zur Verfügung zu stellen, während er Einsicht in die Originalunterlagen nimmt (so ausdrücklich das Bundesverwaltungsgericht in der zitierten Entscheidung).

17. § 10 Abs. 1 Satz 3 wird wie folgt gefasst:

„Mit dieser Maßgabe bleiben Kostenregelungen in anderen Rechtsvorschriften unberührt."

In § 10 wird Abs. 3 gestrichen.

BEGRÜNDUNG:

Die Regelung des § 10 Abs. 3 ist insofern überflüssig, als in § 10 Abs. 1 Satz 3 ohnehin andere Kostenregelungen unberührt bleiben. Zudem kann der gesonderte Verweis auf das Kommunalabgabengesetz zu dem Fehlschluss verleiten, bei der Anwendung des Kommunalabgabengesetzes könnten stets kostendeckende Gebühren erhoben werden. Stattdessen muss der Grundsatz des § 10 Abs. 1 Satz 2 (Proportionalität) aus verfassungsrechtlichen Gründen auch dann gelten, wenn die Gemeinden und Gemeindeverbände in

Angelegenheiten der Selbstverwaltung über Akteneinsichtsanträge zu entscheiden haben. Dem trägt die vorgeschlagene Neufassung des § 10 Abs. 1 Satz 3 Rechnung.

18. Folgender neuer § 10 Abs. 3 wird angefügt:

    „Der Antragsteller ist vor der Durchführung der Akteneinsicht über die Höhe der Kosten zu informieren."

BEGRÜNDUNG:

Der Antragsteller soll rechtzeitig beurteilen können, wie hoch die Kosten der erstrebten Akteneinsicht sein werden. Dies dient seiner Information und ersetzt nicht den eigentlichen Gebührenbescheid.

19. Es wird folgender neuer § 10 Abs. 4 eingefügt:

    „Auf die Erhebung von Kosten ist zu verzichten, wenn die Akteneinsicht im öffentlichen Interesse liegt oder zum Zweck der politischen Mitgestaltung erfolgt."

BEGRÜNDUNG:

Während z. B. die Einsicht in Bauakten zu privaten Zwecken durchaus eine Erhebung von Kosten rechtfertigt, sollte die Einsicht zu Zwecken der demokratischen Beteiligung und politischen Mitgestaltung im engeren Sinne (vgl. Art. 21 der Landesverfassung) - ebenso wie die Teilnahme an Wahlen - kostenfrei sein.

20. § 11 Abs. 2 Satz 2 wird wie folgt gefasst:

    „Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat die Befugnisse nach § 23, 25 und 26 des Brandenburgischen Datenschutzgesetzes."

BEGRÜNDUNG:

Der Landesbeauftragte für das Recht auf Akteneinsicht sollte ebenso wie der Landesbeauftragte für den Datenschutz auch dann tätig werden können, wenn ihm keine entsprechende Beschwerde vorliegt. Dies würde zu einer ef-

fektiveren Wahrung des Grundrechts auf Informationszugang in der Brandenburgischen Verwaltung beitragen.

Anlage 3

Text des Akteneinsichts- und Informationszugangsgesetzes unter Berücksichtigung der Änderungsvorschläge des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

§ 1 Aufgabe

Aufgabe dieses Gesetzes ist es, dem Einzelnen, Bürgerinitiativen und Verbänden die Wahrnehmung ihres Grundrechts auf Akteneinsicht und Informationszugang zu ermöglichen, soweit dem nicht überwiegende öffentliche oder private Interessen nach den §§ 4 und 5 entgegenstehen.

§ 2 Anwendungsbereich

(1) Das Akteneinsichtsrecht besteht gegenüber Behörden und Einrichtungen des Landes im Sinne des Zweiten Abschnitts des Landesorganisationsgesetzes sowie gegenüber Gemeinden und Gemeindeverbänden.

(2) Das Akteneinsichtsrecht besteht gegenüber den in § 1 Abs. 2 des Landesorganisationsgesetzes genannten Stellen nur, soweit sie Verwaltungsaufgaben erledigen. Gegenüber Forschungsanstalten, zentralen Forschungseinrichtungen, Schulen und Prüfungseinrichtungen besteht das Einsichtsrecht nur, soweit sie nicht im Bereich von Forschung, Lehre, Unterricht und Prüfung tätig werden.

(3) Das Akteneinsichtsrecht besteht gegenüber Behörden und Verwaltungseinrichtungen des Landes und der Gemeinden und Gemeindeverbände, deren Zuständigkeitsbereich sich auch auf andere Bundesländer erstreckt, nur, soweit sich deren Akten ausschließlich auf das Land Brandenburg beziehen.

(4) Soweit sich die aktenführende Behörde zur Erledigung ihrer Aufgaben Privater bedient, besteht das Akteneinsichtsrecht gegenüber den privaten Stellen.

(5) Soweit Akten führende Stellen in Brandenburg um Zustimmung zur Offenbarung von Akteninhalten außerhalb des Geltungsbereichs dieses Gesetzes gebeten werden, haben sie dieses Gesetz zugrunde zu legen.

§ 3 Begriffsbestimmung

Akten im Sinne dieses Gesetzes sind alle schriftlich, elektronisch, optisch, akustisch oder auf andere Weise aufgezeichneten Unterlagen, soweit diese ausschließlich amtlichen oder dienstlichen Zwecken dienen. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil des Vorgangs sind und spätestens nach dessen Abschluss vernichtet werden.

§ 4 Schutz öffentlicher Interessen

(1) Ein Recht auf Akteneinsicht besteht nicht, soweit

1. das Bekanntwerden des Akteninhalts die Landesverteidigung oder die internationalen Beziehungen des Bundes oder eines anderen Landes berühren würde oder die Beziehungen des Landes zu anderen Staaten oder zwischenstaatlichen Einrichtungen, zur Europäischen Union, zum Bund oder zu den Ländern beeinträchtigen könnte,

2. durch das Bekanntwerden des Akteninhalts Angaben und Mitteilungen öffentlicher Stellen, die nicht dem Anwendungsbereich dieses Gesetzes unterfallen, ohne deren Zustimmung offenbart würden,

3. sich der Inhalt der Akten auf Beratungen der Landesregierung oder Arbeiten zu ihrer Vorbereitung bezieht,

4. das Bekanntwerden des Akteninhalts Belange der Strafverfolgung und -vollstreckung, der Gefahrenabwehr oder andere Belange der inneren Sicherheit beeinträchtigen könnte oder eine erhebliche Gefahr für die öffentliche Sicherheit verursachen könnte,

5. durch die Gewährung von Akteneinsicht Inhalte von Akten offenbart würden, die eine Behörde zur Durchführung eines Gerichtsverfahrens, eines strafrechtlichen oder disziplinarrechtlichen Ermittlungsverfahrens oder eines Bußgeldverfahrens erstellt hat, oder die ihr aufgrund des Verfahrens zugehen.

6. soweit sich der Inhalt der Akten auf den nicht-abgeschlossenen Prozess der Willensbildung innerhalb von und zwischen Behörden oder Verwaltungseinrichtungen bezieht, wenn durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg bevorstehender behördlicher Maßnahmen gefährdet würde; dies gilt nicht für die Ergebnisse von abgeschlossenen Verfahrenshandlungen eines Verwaltungsverfahrens, die für die Entscheidung verbindlich sind, insbesondere Ergebnisse von Beweiserhebungen und Stellungnahmen;

7. soweit sich der Inhalt der Akten auf Vorgänge bezieht, die in § 44 der Gemeindeordnung oder § 38 der Landkreisordnung in nicht öffentlicher Sitzung zu beraten oder zu beschließen sind oder in nicht öffentlicher Sitzung beraten oder beschlossen worden sind.

8. wenn die ordnungsgemäße Erfüllung der Aufgaben der öffentlichen Stelle erheblich beeinträchtigt würde,

und wenn das öffentliche Interesse an der Geheimhaltung das Interesse an der Einsichtnahme im Einzelfall überwiegt.

(2) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 5 Schutz privater Interessen

(1) Ein Recht auf Akteneinsicht besteht nicht, soweit

1. personenbezogene Daten offenbart werden und dem schutzwürdige Belange der Betroffenen entgegenstehen, ohne dass das Offenbarungsinteresse des Antragstellers das Interesse der Betroffenen an der vertraulichen Behandlung der Information überwiegt,

2. ein Betriebs- und Geschäftsgeheimnis offenbart würde, ohne dass das Offenbarungsinteresse des Antragstellers das schutzwürdige Interesse des Unternehmens an der Wahrung des Betriebs- und Geschäftsgeheimnisses überwiegt oder das Unternehmen einer Offenbarung zugestimmt hat.

§ 4 Abs. 2 gilt entsprechend.

(2) Der Offenbarung personenbezogener Daten stehen schutzwürdige Belange der Betroffenen in der Regel nicht entgegen, soweit diese zustimmen oder sich aus der Akte ergibt, dass

1. die Betroffenen an einem Verwaltungsverfahren oder einem sonstigen Verfahren beteiligt sind,
2. eine gesetzlich oder behördlich vorgeschriebene Erklärung abgegeben oder eine Anzeige, Anmeldung, Auskunft oder vergleichbare Mitteilung durch die Betroffenen gegenüber einer Behörde erfolgt ist,

3. gegenüber dem Betroffenen überwachende oder vergleichbare Verwaltungstätigkeiten erfolgt sind,

4. die Betroffenen Eigentümer, Pächter, Mieter oder Inhaber eines vergleichbaren Rechts sind,

5. die Betroffenen als Gutachter, sachverständige Personen oder in vergleichbarer Weise eine Stellungnahme abgegeben haben

und durch diese Angaben mit Ausnahme von

- Namen,
- Titel, akademischem Grad,
- Geburtsdatum,
- Beruf, Branchen- oder Geschäftsbezeichnung,
- innerbetrieblicher Funktionsbezeichnung,
- Anschrift,
- Rufnummer

nicht zugleich weitere personenbezogene Daten offenbart werden.

Satz 1 gilt auch, wenn die Betroffenen im Rahmen eines Arbeits- oder Anstellungsverhältnisses oder als Vertreter oder Vertreterin oder Organ einer juristischen Person an einem Verwaltungsverfahren beteiligt sind, die Mitteilungen machen oder die Verwaltungstätigkeit ihnen gegenüber in einer solchen Eigenschaft erfolgt. § 16 des Brandenburgischen Datenschutzgesetzes findet keine Anwendung.

(3) Bei Einsicht in die Akten ist auch die Offenbarung der Mitwirkung eines Amtsträgers an Verwaltungsvorgängen oder sonstigem hoheitlichem Handeln sowie dessen Namens, Titels, akademischen Grades, der innerdienstlichen Funktionsbeschreibung, der dienstlichen Anschrift und Rufnummer zulässig, es sei denn, der Offenbarung stehen schutzwürdige Belange des Amtsträgers entgegen.

§ 6 Durchführung der Akteneinsicht

(1) Der Antrag auf Akteneinsicht muss hinreichend bestimmt sein. Der Antrag ist schriftlich an die aktenführende Behörde zu richten. Sofern dem Antragsteller Angaben zur hinreichenden Bestimmung seines Antrages fehlen, ist er von der öffentlichen Stelle zu beraten und zu unterstützen. Wird ein Antrag bei einer unzuständigen Stelle gestellt, so ist diese verpflichtet, den Antrag unverzüglich an die zuständige Stelle weiterzuleiten und den Antragsteller hierüber zu unterrichten. Eine Ablehnung des Antrages ist von der aktenführenden Behörde schriftlich zu begründen. Der Antragsteller ist im Ablehnungsbescheid auf sein Recht nach § 11 Abs. 2 Satz 1 hinzuweisen.

(2) Soweit der Schutz der in den §§ 4 und 5 genannten öffentlichen und privaten Belange durch Aussonderung von Aktenteilen oder Einzeldaten gewährleistet werden kann, ist dem Antragsteller der übrige Teil der Akte zugänglich zu machen. Ist die Aussonderung mit einem unverhältnismäßig hohen Aufwand verbunden, besteht nur ein Recht auf Auskunftserteilung.

(3) Kommt die Akten führende Stelle bei der Prüfung eines Antrags auf Akteneinsicht zu der Auffassung, dass der Offenbarung von personenbezogenen Daten oder Betriebs- oder Geschäftsgeheimnissen keine schutzwürdigen Belange Betroffener entgegenstehen, oder dass der Gewährung der Akteneinsicht zwar schutzwürdige Belange Betroffener entgegenstehen, das Informationsinteresse aber gegenüber dem Interesse der Betroffenen an der Geheimhaltung überwiegt, so hat sie den Betroffenen Gelegenheit zu geben, sich innerhalb von drei Wochen zu den für die Entscheidung erheblichen Tatsachen zu äußern. Die Entscheidung ist auch den Betroffenen bekannt zu geben. Gegen die Entscheidung können die Betroffenen Widerspruch einlegen. Die Akteneinsicht darf erst nach Eintritt der Bestandskraft der Entscheidung gegenüber den Betroffenen oder zwei Wochen nach Anordnung der sofortigen Vollziehung, die auch den Betroffenen bekannt zu geben ist, gewährt werden.

(4) Der Antrag kann abgelehnt werden, wenn der Antragsteller bereits über die begehrten Informationen verfügt oder sich diese in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann oder wenn der Antrag zum Zweck der Vereitelung oder Verzögerung von Verwaltungshandlungen erfolgt.

(5) Soweit die Akteneinsicht von der Zustimmung Dritter abhängig ist, ist auf Verlangen des Antragstellers die Zustimmung einzuholen. Der Antragsteller ist auf diese Möglichkeit hinzuweisen. Liegt innerhalb von drei Wochen nach Aufforderung durch die aktenführende Behörde eine Zustimmung Betroffener zur Offenbarung personenbezogener Daten nicht vor, gilt die Zustimmung als verweigert. Liegt die Zustimmung einer Behörde nach § 4 Abs.1 Nr.2 oder eines Unternehmens nach § 5 Abs.1 Nr.2 innerhalb dieser Frist nicht vor, gilt sie als erteilt. Angaben zur Person des Antragstellers dürfen bei der Einholung der Zustimmung Dritter nur mit Einverständnis des Antragstellers offenbart werden.

(6) Über den Antrag ist sobald wie möglich, spätestens jedoch einen Monat nach seinem Eingang bei der Akten führenden Behörde zu entscheiden.

(7) Lehnt die Akten führende Behörde die Akteneinsicht unter Berufung auf § 4 Abs. 1 Nrn. 3 - 5 oder § 4 Abs. 2 ab, so hat sie dem Antragsteller mitzu-

teilen, zu welchem Zeitpunkt eine Einsichtnahme voraussichtlich erfolgen kann.

§ 7 Art und Weise der Gewährung des Akteneinsichtsrechts

(1) Der Anspruch auf Akteneinsicht wird vorbehaltlich der in § 6 Abs. 2 und § 8 geregelten Ausnahmen durch Gewährung der Einsicht in die Originaldokumente erfüllt. Auf Verlangen des Antragstellers ist das Akteneinsichtsrecht auch durch

1. Übermittlung von Vervielfältigungen,

2. Verweis auf Dokumentationen und Veröffentlichungen der zuständigen Behörde,

3. elektronische Post,

4. Zurverfügungstellung von Informationsträgern in sonstiger Weise

zu gewähren, soweit sie die begehrten Informationen enthalten. Die Akten führende Behörde ist nicht verpflichtet, einem Verlangen des Antragstellers nach Satz 2 zu entsprechen, wenn hierfür im Einzelfall gewichtige Gründe bestehen, die sie darzulegen hat. Das Recht auf Einsicht in die Originalunterlagen bleibt davon unberührt.

§ 7aVeröffentlichungspflichten, Aktenführung

(1) Akten führende Behörden i. S. d. § 2 haben Verzeichnisse zu führen, die geeignet sind, die Aktenordnung und den Aktenbestand sowie den Zweck der geführten Akten erkennen zu lassen. Diese Verzeichnisse sind in allgemein verständlicher Weise zu veröffentlichen. Entsprechendes gilt für Verwaltungsvorschriften, die von der Akten führenden Behörde erlassen worden sind. Möglichkeiten der Veröffentlichung in elektronischer Form sind entsprechend dem Stand der Technik zu berücksichtigen.

(2) Die Akten führenden Behörden treffen geeignete organisatorische Vorkehrungen, damit Informationen, die nach § 4 und 5 nicht eingesehen werden können, möglichst ohne unverhältnismäßigen Aufwand abgetrennt werden können.“

§ 8 Gleichförmige Anträge und Beschränkung auf Auskunftserteilung

(1) Das Akteneinsichtsrecht ist auf Auskunftserteilung beschränkt, wenn mehr als 50 Anträge vorliegen, die auf die gleichen Informationen gerichtet sind,

und die Auskunft auch ohne den Informationsträger verständlich ist. Abweichend von Satz 1 kann auch bei weniger als 50 Anträgen die Informationsgewährung auf Auskunftserteilung beschränkt werden, wenn die Gewährung von Akteneinsicht mit einem unverhältnismäßig hohen Aufwand verbunden wäre.

(2) Bei Anträgen, die von mehr als 50 Personen auf Unterschriftslisten unterzeichnet oder in Form vervielfältigter gleichlautender Texte eingereicht worden sind (gleichförmige Anträge), gelten die §§ 17 und 19 des Brandenburgischen Verwaltungsverfahrensgesetzes entsprechend.

§ 9 Informationsrecht für Bürgerinitiativen und Verbände zur Beeinflussung öffentlicher Angelegenheiten

(1) Dieses Gesetz findet entsprechend Anwendung auf Bürgerinitiativen und Verbände zur Beeinflussung öffentlicher Angelegenheiten im Sinne des Artikels 21 Abs. 3 der Verfassung des Landes Brandenburg, soweit sie ihr Recht auf Information geltend machen.

(2) Anträge nach Absatz 1 können nur durch den Vorstand oder einen besonders hierzu Bevollmächtigten gestellt werden. In Zweifelsfällen ist gegenüber der Behörde die Vertretungsbefugnis nachzuweisen.

§ 10 Kosten

(1) Für Amtshandlungen, die aufgrund dieses Gesetzes vorgenommen werden, werden Kosten (Gebühren und Auslagen) erhoben. Die Gebühren sind so zu bemessen, dass zwischen dem Verwaltungsaufwand einerseits und dem Recht auf Akteneinsicht andererseits ein angemessenes Verhältnis besteht. Mit dieser Maßgabe bleiben Kostenregelungen in anderen Rechtsvorschriften unberührt.

(2) Die Landesregierung wird ermächtigt, im Benehmen mit dem Ausschuss für Inneres des Landtages die Gebührentatbestände und die Höhe der Gebühren durch Rechtsverordnung (Gebührenordnung) zu bestimmen.

(3) Der Antragsteller ist vor der Durchführung der Akteneinsicht über die Höhe der Gebühr zu informieren.

(4) Auf die Erhebung von Kosten ist zu verzichten, wenn die Akteneinsicht im öffentlichen Interesse liegt oder zum Zweck der politischen Mitgestaltung erfolgt.

§ 11 Landesbeauftragter für das Recht auf Akteneinsicht

(1) Zur Wahrung des Grundrechts auf Akteneinsicht und Informationszugang wird ein Landesbeauftragter für das Recht auf Akteneinsicht bestellt. Diese Aufgabe wird von dem Landesbeauftragten für den Datenschutz wahrgenommen. Die Wahl und die Rechtsstellung des Landesbeauftragten richten sich nach den §§ 22 und 23 des Brandenburgischen Datenschutzgesetzes. Der Landesbeauftragte führt die Amts- und Funktionsbezeichnung „Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht“ in männlicher oder weiblicher Form.

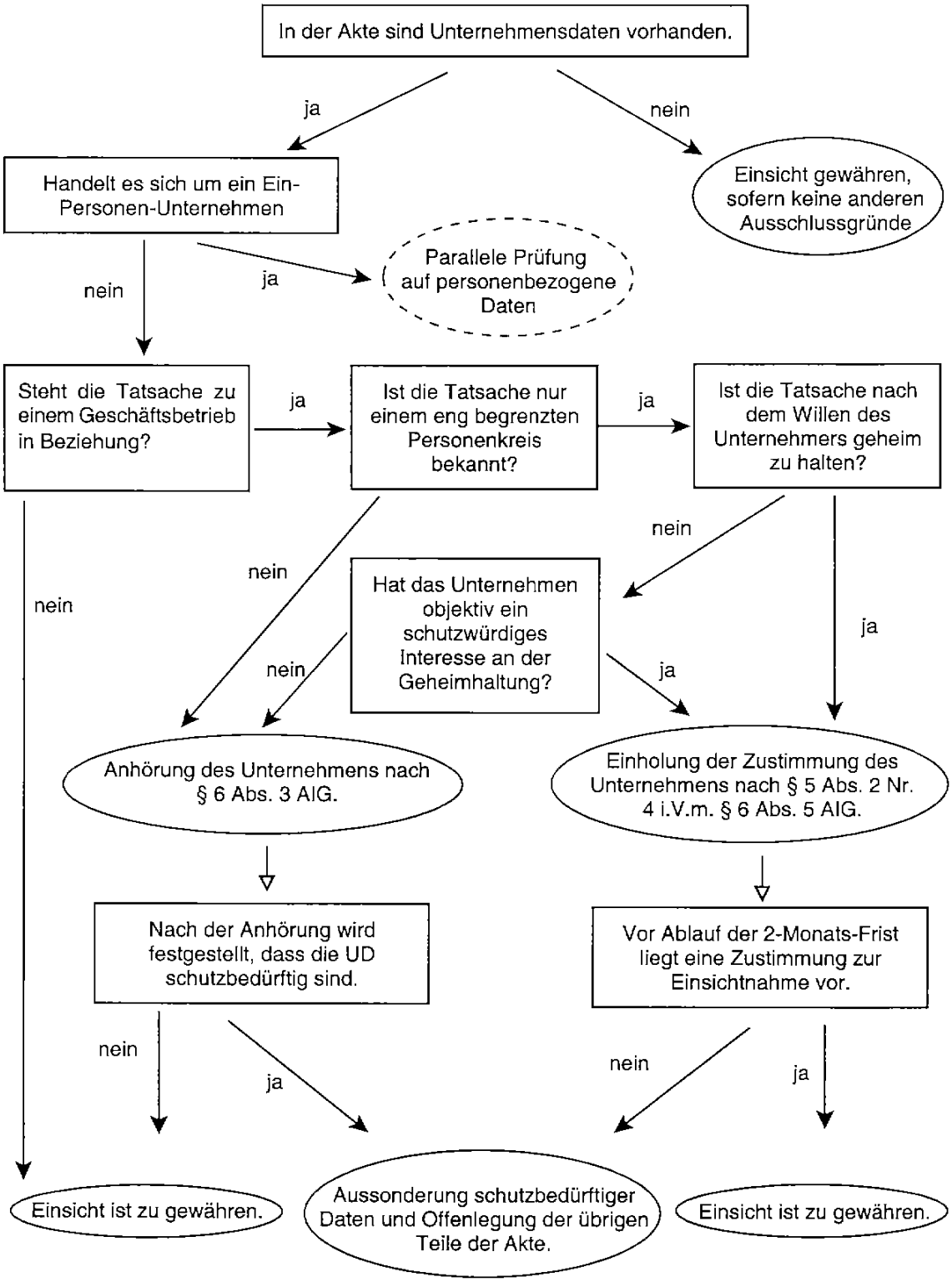
(2) Jeder hat das Recht, den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht anzurufen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat die Befugnisse nach §§ 23, 25 und 26 des Brandenburgischen Datenschutzgesetzes.

(3) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht legt dem Landtag jährlich einen Bericht über seine Tätigkeit vor.

§ 12 In Kraft treten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Umgang mit Unternehmensdaten (UD) bei der Akteneinsicht auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes



Anlage 5

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

Stand: 1. Januar 2002

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix
Stellvertreter	Herr Urban
Mitarbeit bei: - Akteneinsicht und Informationszugang - Verwaltungsmodernisierung - Redaktion von Veröffentlichungen	Dipl. Verwaltungswissenschaftler Sven Müller App. 20
Sekretariat	Christine Objartel App. 10

Bereich Recht

Bereichsleiter	Dr. Frank Jendro App. 34
Arbeitsgebiete: - Rechtliche Grundsatzfragen - Landtag, Staatskanzlei - Landesrechnungshof - Wissenschaft, Forschung, Kultur - Beauftragter des Haushalts	
Arbeitsgebiete: - Arbeit, Soziales, Gesundheit, Frauen - Sozial- und Gesundheitsdaten allgemein	Frau Bultmann App. 44
Arbeitsgebiete: - Inneres (insbes. Polizei, Verfassungsschutz, Verkehrsordnungswidrigkeiten, Ausländer, Asylverfahren) - Staatsanwaltschaften - Presse- und Öffentlichkeitsarbeit	Lena Schraut App. 41

Arbeitsgebiete: App. 22
- Stadtentwicklung, Wohnen, Verkehr
- Justiz und Europaangelegenheiten (außer Staatsanwaltschaften)
- Wirtschaft

Arbeitsgebiete: App. 45
- Finanzen
- Bildung, Jugend, Sport
- Landwirtschaft, Umweltschutz, Raumordnung (einschließlich Abwasserzweckverbände)

Arbeitsgebiete: Herr Hermerschmidt
- Personaldaten allgemein App. 40
- Inneres
- Kommunalrecht (außer Abwasserzweckverbände)
- Rechtsfragen der elektronischen Verwaltung (eGovernment)
- Telekommunikation und Medien

Arbeitsgebiete: App. 42
- Personal- und Verwaltungsangelegen heiten des LDA
- Büroleitungsaufgaben
- Haushaltsangelegenheiten
- Beschaffungen allgemein

Arbeitsgebiete: App. 43
- Bibliothek
- Literaturbeschaffung
- Schreibdienst
- Informationsmaterialien

Bereich Technik

Bereichsleiter Herr Urban
App. 30

Arbeitsgebiete:
- Technisch/organisatorische Grundsatzfragen
- Landesverwaltungsnetz
- Videoüberwachung
- komplexe IT-Verfahren

Arbeitsgebiete: - Großrechner - Datenbanksysteme - kryptographische Verfahren - Wartung und Fernwartung - Statistik - Beratung der behördlichen Datenschutzbeauftragten und Personalräte	App. 31
Arbeitsgebiete: - UNIX-Systeme - Sicherheitsprodukte - Kartentechnologien - elektronische Signatur - Kommunikationsnetze - Telekommunikation und Medien	App. 32
Arbeitsgebiete: - Systemverwalter - Gebäudesicherung - Datenschutzaudit - Isolierte und vernetzte PC	App. 33
Arbeitsgebiete - Organisations- und Dienstanweisungen - Risikoanalysen und Sicherheitskonzepte - Bürgerbüro	N.N.
Arbeitsgebiete: - Lagerung und Entsorgung von Datenträgern - Mailboxkommunikation mit anderen Behörden - Schreibdienst - Informationsmaterialien	App. 12
Gleichstellungsbeauftragte	App. 43
Personalrat	App. 31
Behördlicher Datenschutzbeauftragter	Herr Hermerschmidt App. 40

Anlage 6

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
ABlEG	=	Amtsblatt der Europäischen Gemeinschaft
Abs.	=	Absatz
AGIB	=	Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland
AgrStatG-DVO	=	Agrarstatistikgesetz-Durchführungsverordnung
AIG	=	Akteneinsichts- und Informationszugangsgesetz
ALB	=	Automatisiertes Liegenschaftsbuch
ALK	=	Automatisierte Liegenschaftskarte
Anl.	=	Anlage
AO	=	Abgabenordnung
AUMO	=	Straftäter politisch motivierter Ausländerkriminalität
Bbg.	=	Brandenburgisch(es)
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPG	=	Landespressegesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgStatG	=	Brandenburgisches Statistikgesetz
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtsgesetz
BR-Drs.	=	Bundesrats-Drucksache
BSE	=	Bovine Spongiforme Enzephalopathie
BSI	=	Bundesamt für die Sicherheit in der Informationstechnik
BtMG	=	Betäubungsmittelgesetz
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BVerfSchG	=	Bundesverfassungsschutzgesetz
bzw.	=	beziehungsweise
CD-ROM	=	Compact-Disk-Read-Only-Memory
d. h.	=	das heißt
DES	=	Data Encryption Standard (112 Bit oder 168 Bit Schlüssellänge)
3DES	=	Data Encryption Standard (56 Bit Schlüssellänge
DNA	=	Deoxyribonucleic acid
Drs.	=	Drucksache
DSG	=	Datenschutzgesetz
DSV	=	Datenschutzverordnung Schulwesen
DVD	=	Digital Versatile Disk
EC	=	Electronic Cash

EG	=	Europäische Gemeinschaft
EGG	=	Elektronischer-Geschäftsverkehr-Gesetz
EGMR	=	Europäischer Gerichtshof für Menschenrechte
ELREV	=	Elektronischer Rechtsverkehr
ELSTER	=	Elektronische Steuererklärung
EU	=	Europäische Union
evtl.	=	eventuell
ff.	=	folgende
G 10	=	Gesetz zu Artikel 10 Grundgesetz
geänd.	=	geändert
gem.	=	gemäß
GewO	=	Gewerbeordnung
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GHz	=	Giga Hertz
GmbH	=	Gesellschaft mit beschränkter Haftung
GO	=	Gemeindeordnung
GWS	=	Gewalttäter Sport
HGB	=	Handelsgesetzbuch
HTML	=	HyperText Markup Language
HTTP	=	HyperText Transfer Protocol
i. d. Fass.	=	in der Fassung
i. d. R.	=	In der Regel
i. S. v.	=	im Sinne von
IEEE	=	Institute of Electrical and Electronic Engineers
IMA-IT	=	Interministerieller Ausschuss für Informationstechnik
INPOL	=	Informationssystem der Polizei
ISDN	=	Integrated Services Digital Network
ISIS-MTT	=	Industrial Signature Interoperability Specification/Mail-TrusT
ISM	=	Industrial, Science, Medical
IT	=	Informationstechnik
KAN	=	Kriminalaktennachweis
Kap.	=	Kapitel
Kfz	=	Kraftfahrzeug
KitaG	=	Kindertagesstättengesetz
KPM	=	Koordinierungsstelle für Personalmanagement der Landesregierung
LAN	=	Local Area Network
LBG	=	Landesbeamtengesetz
LDA	=	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDS	=	Landesbetrieb für Datenverarbeitung und Statistik

LIMO	=	Linksorientierte politisch motivierte Gewalttäter
LRH	=	Landesrechnungshof
LT-Drs.	=	Landtags-Drucksache
LVN	=	Landesverwaltungsnetz
MAC	=	Media Access Control
m.a.u.s.	=	Medien an unsere Schulen
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
Nr.	=	Nummer
o. g.	=	oben genannte
OLG	=	Oberlandesgericht
ORB	=	Ostdeutscher Rundfunk Brandenburg
PASS	=	Polizeiliches Auskunftssystem Straftaten
PC	=	Personalcomputer
PERIS	=	Personalinformationssystem
PersVG	=	Personalvertretungsgesetz
PHW	=	Personengebundener Hinweis
PIN	=	Personal Identification Number
Pkt.	=	Punkt
PROREDDI	=	Programm zur Realisierung des DNA-Identitätsfeststellungsgesetzes
REMO	=	Rechtsorientierte politisch motivierte Gewalttäter
s.	=	siehe
S.	=	Seite; Satz
s. o.	=	siehe oben
SDÜ	=	Schengener Durchführungsabkommen
SFB	=	Sender Freies Berlin
SGB	=	Sozialgesetzbuch
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB V	=	Fünftes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
sog.	=	so genannt, so genannte
SSID	=	Service Set Identifier
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
TDDSG	=	Teledienstedatenschutzgesetz
TDG	=	Teledienstegesetz
TDSV	=	Telekommunikations-Datenschutzverordnung
TK	=	Telekommunikation
TKG	=	Telekommunikationsgesetz
u. a.	=	unter anderem
UIG	=	Umweltinformationsgesetz
UMTS	=	Universal Mobile Telecommunications System
Urt.	=	Urteil
usw.	=	und so weiter

v.	=	von, vom
VermLiegG	=	Vermessungs- und Liegenschaftsgesetz
vgl.	=	vergleiche
VO	=	Verordnung
VPN	=	Virtual Private Network
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless Local Area Network
WWW	=	World Wide Web
z. B.	=	zum Beispiel
z. T.	=	zum Teil
ZBB	=	Zentrale Bezügestelle
ZStV	=	Zentrales Staatsanwaltschaftliches Verfahrensregister

Stichwortverzeichnis