Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2007

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung alle zwei Jahre einen Bericht über ihre Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz; § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 22. März 2006 vorgelegten Tätigkeitsbericht 2004/2005 an und deckt den Zeitraum vom 1. Januar 2006 bis zum 31. Dezember 2007 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abgerufen werden.

Impressum

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

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

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

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Druckerei Pietsch, Kloster Lehnin

Inhaltsverzeichnis

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

Anlagen

Verzeichnis der öffentlichen Stellen **Gliederungspunkt**

Einleitung

Wer in den beiden zurückliegenden Jahren morgens die Zeitung aufschlug, konnte so gut wie täglich etwas zu Datenschutzthemen lesen. Auch das Thema Akteneinsicht wurde verstärkt öffentlich diskutiert.

Zwei Entwicklungen haben die Diskussionen zum Datenschutz in der Öffentlichkeit beherrscht: Zum einen der vielstimmige Ruf nach präventiven Sicherheitsmaßnahmen, zum anderen der trotz des föderalen Systems verstärkte Aufbau von Zentraldateien mit einer zunehmenden Fülle von Daten aller Bürgerinnen und Bürger. Beide Entwicklungen sind stark geprägt durch die technischen Fortschritte sowie Fragen der Datensicherheit.

Allein die Auflistung der Gesetzgebung in den Bereichen Inneres und Justiz ist beeindruckend. Der Bundestag hat u. a. ein Gesetz zum Aufbau einer Antiterrordatei, zur Einführung der Vorratsdatenspeicherung und zur Aufnahme des Fingerabdrucks in den Reisepass verabschiedet. Noch diskutiert werden die gesetzliche Regelung einer Online-Durchsuchung zu präventiven Zwecken der Polizei sowie die Ausweitung der Videoüberwachung. Die Online-Durchsuchung hat bereits der Gesetzgeber in Nordrhein-Westfalen dem dortigen Verfassungsschutz eingeräumt. Der brandenburgische Landtag hat im Dezember 2006 das Polizeigesetz novelliert und darin ebenfalls neue Befugnisse wie die präventive Telefonüberwachung, eine Videoüberwachung, die Kennzeichenfahndung und den Einsatz von IMSI-Catchern zur Standortfeststellung vorgesehen. Alle diese neuen Regelungen enthalten einen präventiven Ansatz, d. h. sie werden im Vorfeld möglicher Straftaten wirksam. Das Verhindern von Straftaten wird damit in den Vordergrund gerückt; gleichzeitig wird zunehmend in die Datenschutzrechte Unbeteiligter eingegriffen.

Bei allen diesen Eingriffsbefugnissen stellt sich die Frage, wie viel Vorfeldüberwachung ein Staat vertragen kann. Das Bundesverfassungsgericht befasst sich folglich verstärkt mit den datenschutzrechtlichen Gesetzen hierfür. Beispielhaft seien hier die zurückliegenden Entscheidungen zum Großen Lauschangriff, zur präventiven Telefonüberwachung im Polizeigesetz des Landes Niedersachsen oder zum Einsatz von IMSI-Catchern bzw. zum Kontendatenabrufverfahren genannt. Aktuell liegen Verfassungsbeschwerden u. a. zur Antiterrordatei, zur Kennzeichenfahndung, zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen sowie zum Fingerabdruck als zusätzlichem biometrischen Merkmal im neuen Reisepass vor. Die meisten dieser Entscheidungen des Bundesverfassungsgerichts haben in der Vergangenheit zu deutlichen Korrekturen der Gesetze im Sinne der Bürgerrechte geführt. Es ist bedauerlich, dass die rechtzeitigen Hinweise von Sachverständigen während der Gesetzgebungsverfahren ignoriert werden und

dem höchsten Gericht beinahe schon automatisch die Aufgabe zukommt, diese Versäumnisse zu kompensieren.

Bei den im Jahr 2007 beschlossenen Eingriffsbefugnissen fällt auf, dass auch Journalisten zunehmend von Überwachungsmaßnahmen betroffen sind. Beispielhaft sind hier Telefonüberwachungen oder Briefdurchleuchtungen zu nennen. Kann die Presse weiterhin Sachverhalte aufdecken, wenn sie selbst in den Blickpunkt der Fahnder gerät?

Aufgabe der Datenschutzbeauftragten ist es, immer wieder die Frage nach der Erforderlichkeit und Verhältnismäßigkeit neuer Eingriffsbefugnisse zu stellen. Die Abwägung der betroffenen Rechtsgüter mit dem Recht auf informationelle Selbstbestimmung bleibt in jedem Einzelfall eine schwierige Aufgabe. Gerade bei der Gegenüberstellung von Sicherheit und Freiheit zeigt sich, dass es beides nicht absolut geben kann.

Die Zentraldateien sind das zweite große Thema. Fast unbemerkt hat der Gesetzgeber dem Bundeszentralamt für Steuern größere Kompetenzen eingeräumt. Künftig erhalten alle Bürgerinnen und Bürger eine einheitliche Identifikationsnummer für alle Steuerarten. Darüber hinaus entsteht ein Bundesmelderegister, das die bereits vorhandenen kommunalen Register ergänzen soll.

Das Projekt mit dem schönen Namen „ELENA“ (elektronische Einkommensnachweise) wurde zunächst nicht weiterverfolgt. Dahinter verbirgt sich das Vorhaben, die Einkommensdaten sämtlicher, in Deutschland abhängig Beschäftigter in einem bundesweiten Register zu speichern und für Verfahren zur Verfügung zu stellen, in denen der Nachweis des Einkommens erforderlich ist. Zwar ist der Trend zur Zentralisierung ungebrochen, aber ist diese überhaupt notwendig? Welche Risiken bergen zentrale Datenbanken und wie ist es um die Sicherheit der Daten bestellt?

Großbritannien hat im November 2007 den bisher größten bekannten Datenverlust seiner Geschichte erlebt. Zwei CDs mit unverschlüsselten, nur durch ein Passwort geschützten Daten von 25 Millionen Briten aus siebeneinhalb Millionen Haushalten, die Kindergeld empfangen, sind verloren gegangen: Namen, Anschriften, Kontonummern, Sozialversicherungsnummern. Dieser Datenverlust ist ein Beispiel dafür, dass es keine vollständige Sicherheit gibt und bei immer größer werdenden Zentraldateien die Risiken auch für jeden einzelnen zunehmen. Wie würde mit einem vergleichbaren Fall in der Bundesrepublik Deutschland umgegangen? Würden die Warnungen der Datenschutzbeauftragten auch dann noch ignoriert?

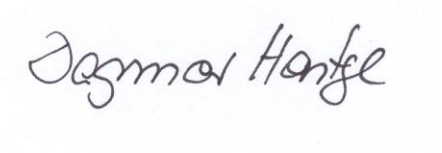
Die Zahl der gesetzlich erlaubten, automatisierten Kontrollverfahren durch staatliche Behörden hat stetig zugenommen. Das Kontendatenabrufverfahren wurde auf Empfänger von Arbeitslosengeld II ausgedehnt, die zunächst ausgenommen werden sollten.

In Brandenburg haben wir uns nochmals verstärkt mit dem Thema Datensicherheit befasst. Um das Vertrauen seiner Bürger zu gewinnen, muss der Staat alles unternehmen, um die Sicherheit ihrer Daten zu gewährleisten. Dieser Aufgabe können öffentliche Stellen aber nur gerecht werden, wenn sie sowohl finanziell als auch personell angemessen ausgestattet sind.

Neben der Wahrung von Datenschutzrechten hat meine Behörde den gesetzlichen Auftrag, die Umsetzung des Rechts auf Informationszugang im Land Brandenburg zu begleiten. Hier sind die Zahl der Fälle, die Bürger in den Jahren 2006 und 2007 an uns herangetragen haben, zwar etwa gleich hoch geblieben, die Sachverhalte aber insgesamt komplizierter geworden. Auf der anderen Seite steht dem ein großes Bemühen der öffentlichen Stellen gegenüber, das Akteneinsichts- und Informationszugangsgesetz in ihrer täglichen Arbeit zu berücksichtigen und so die Anträge der Bürger auf Akteneinsicht kompetent bearbeiten zu können. Trotz dieser positiven Entwicklung würde ich mir wünschen, dass noch mehr Bürger ihre Informationszugangsrechte in Anspruch nehmen. Letzten Endes scheitert dies aber oftmals daran, dass vielen das ihnen zustehende Recht noch immer unbekannt ist. Auch zehn Jahre nach Verabschiedung des Gesetzes bleibt es eine wichtige Aufgabe der Landesbeauftragten, sowohl Behörden beim Umgang mit diesem Recht zu beraten als auch den Bürgern ihre Teilhaberechte zu vermitteln.

Die vergangenen Jahre haben gezeigt, dass Datenschutz und Informationsfreiheit aktuelle Themen unserer Zeit sind. Der nachfolgende Bericht verdeutlicht, dass nahezu alle Lebensbereiche davon berührt werden. Ich wünsche daher allen Leserinnen und Lesern meines Tätigkeitsberichts eine interessante Lektüre und würde mich über Rückmeldungen durchaus freuen.

Kleinmachnow, den 11. März 2008



Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Novellierung des Brandenburgischen Datenschutzgesetzes

Im Berichtszeitraum wurden in Brandenburg zahlreiche Gesetze mit datenschutzrelevanten Regelungen geändert. Dass für die Arbeit der Aufsichtsbehörde wichtigste Gesetz war das Brandenburgische Datenschutzgesetz. Es wurde zum dritten Mal seit seinem In-Kraft-Treten novelliert. Erstmals stand die Novellierung unter dem Tenor der Entbürokratisierung. Ziel der Novellierung war die Rückführung des Niveaus des Brandenburgischen Datenschutzgesetzes auf die von der EG-Datenschutzrichtlinie geregelten so genannten Mindeststandards. Unter dieser Maßgabe legte das Ministerium des Innern einen Änderungsentwurf vor. Es wurden zahlreiche Genehmigungs- und Meldepflichten gestrichen, das Instrument der Auftragsdatenverarbeitung kürzer und verständlicher formuliert und die Vorschriften zur automatisierten Datenverarbeitung dem Stand der heutigen technischen Entwicklung angepasst. All dies sind sinnvolle Änderungen, die in der Praxis zu einer besseren Anwendbarkeit führen werden.

Allerdings enthielt der in den Landtag eingebrachte Gesetzesentwurf auch Änderungen, die zu einer starken Reduzierung des Datenschutzniveaus hätten führen können. Die ausdrückliche Forderung eines Sicherheitskonzeptes wurde erheblich abgeschwächt und die Regelung eines Datenschutzaudits im Brandenburgischen Datenschutzgesetz gänzlich gestrichen. Risikoanalyse und Sicherheitskonzepte sowie deren Fortschreibung stellen aber auch dann die Basis jeder IT-Sicherheit dar, wenn ausschließlich andere als personenbezogene Daten verarbeitet werden. Das Datenschutzgütesiegel/-audit hat sich beispielsweise seit dem Jahre 2001 in Schleswig-Holstein so gut bewährt, dass die Europäische Kommission darauf aufmerksam geworden ist. Unter Mitarbeit des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein lässt sie nunmehr in einem Projekt Maßstäbe für ein europäisches Gütesiegel und Audit erarbeiten.

Obwohl Brandenburg als erstes Bundesland eine Auditregelung geschaffen hatte, wurde diese jedoch nie in die Praxis umgesetzt − ganz im Gegensatz

zu anderen Bundesländern, die eine entsprechende Regelung als Wettbewerbsvorteil für sich zu nutzen wussten.

Da die Datensicherheit für die Umsetzung des Datenschutzes von zentraler Bedeutung ist, haben wir uns sehr darum bemüht, den Blick der Parlamentarier im Gesetzgebungsverfahren auf den Stellenwert eines Sicherheitskonzeptes sowie auf die Chancen, einer angewandten Auditierung, zu richten. Diese Bemühungen und die vom Ausschuss für Inneres durchgeführte Expertenanhörung haben Früchte getragen. Der Innenausschuss hat sich in seiner Beschlussempfehlung für die explizite Aufnahme eines verpflichtenden Sicherheitskonzepts in das Brandenburgische Datenschutzgesetz sowie dessen Fortschreibung wie auch für die Beibehaltung der Auditregelung ausgesprochen. Am Ende ist das Parlament dieser Empfehlung zum Brandenburgischen Datenschutzgesetz mehrheitlich gefolgt.

Somit ist vor Einführung eines datenschutzrelevanten IT-Verfahrens auf der Grundlage einer Risikoanalyse stets ein Sicherheitskonzept zu erstellen. Das Konzept ist fortzuschreiben, um es immer aktuell zu halten. Für die Auditregelung bedarf es allerdings noch eines Ausführungsgesetzes, ansonsten wäre der Beibehalt der Regelung nur ein inhaltloses Lippenbekenntnis. Es ist also noch einiges zu tun, bis auch in Brandenburg die ersten Auditierungen durchgeführt werden können.

Im Zuge der Novellierung des Brandenburgischen Datenschutzgesetzes wäre die Zusammenlegung der Aufsichtsbehörden für den nicht öffentlichen und den öffentlichen Bereich ein ganz wesentlicher tatsächlicher Schritt zur Entbürokratisierung gewesen. Der Sonderausschuss zur Überprüfung von Normen und Standards des Landtags Brandenburg hatte genau dies auch in seinem Abschlussbericht empfohlen. Trotzdem wurde die Zusammenlegung der Aufsichtsbehörden nicht in das novellierte Gesetzes aufgenommen. Gegen die Zusammenlegung zum jetzigen Zeitpunkt wird angeführt, dass es zuvor schwierige verfassungsrechtliche Fragen zu lösen gelte. Außerdem sollte die Entscheidung des Europäischen Gerichtshofs abgewartet werden. Dieser befasst sich mit einer Klage der Europäischen Kommission gegen die Bundesrepublik Deutschland wegen der fehlenden völligen Unabhängigkeit der Aufsichtsbehörden in Deutschland, die im Widerspruch zu der Regelung der EG-Datenschutzrichtlinie steht.

Die rechtlichen Rahmenbedingungen im Land Brandenburg sind seit langem bekannt. Trotzdem ist bisher nicht nach einer Lösung gesucht worden. Weder ist ersichtlich, dass eine Zusammenlegung aus rechtlichen Gründen nicht umgesetzt werden könnte, noch gibt es wegen des anhängigen Klageverfahrens einen Grund, weitere Jahre abzuwarten. Hier wurde der Bürokratieabbau nicht ernst genommen.

Die Belastung meiner Behörde durch fälschlicherweise an uns gerichtete Anfragen zum Datenschutz im nicht öffentlichen Bereich hat ebenso erheblich zugenommen, wie die Doppelbefassungen beider Aufsichtsbehörden. Ein Beispiel hierfür ist das Projekt „Netzwerke für gesunde Kinder“ in Brandenburg.[1] Bürgern, aber auch Unternehmen, können wir die Aufsichtssituation in Brandenburg nur schwer verständlich machen. Dass es vor dem Hintergrund des bereits erwähnten Klageverfahrens vor dem Europäischen Gerichtshof auch anders geht, haben der Freistaat Sachsen und das Land Niedersachsen gezeigt. Beide Länder haben die Aufsichtsregelungen während des laufenden Vertragsverletzungsverfahrens dahingehend geändert, dass nunmehr der jeweilige Landesbeauftragte sowohl für die Datenschutzaufsicht über den öffentlichen als auch über den nicht öffentlichen Bereich zuständig ist. In Brandenburg ist dies nicht gelungen. Wieder einmal heißt es: „Wir prüfen“. Der Ausschuss des Innern des Landtages Brandenburg hatte dem Ministerium des Innern im Jahre 2006 einen Prüfauftrag für eine Zusammenlegung der Aufsichtsbehörden bis zum 30. Juni 2008 erteilt. Was wird sich aber bis dahin an der Ausgangssituation geändert haben?

1.2 E-Government und Datensicherheit – Wunsch und Wirklichkeit

1.2.1 Hohes Sicherheitsniveau mit IT-Sicherheitskonzept

Die stetig steigende Zahl von Angriffen, sowohl qualitativ als auch quantitativ, und die zunehmende Komplexität einer immer stärker vernetzten Gesellschaft erfordern einen erhöhten Aufwand, um die Sicherheit der Informationstechnologie zu gewährleisten. Durch die Erstellung eines IT-Sicherheitskonzeptes lassen sich die Gefahren identifizieren und bewerten sowie angemessene Sicherheitsmaßnahmen ableiten.

Bedingt durch den hohen Komplexitätsgrad der Software wird immer mehr Programmcode generiert, was wiederum zu einer höheren potenziellen Angreifbarkeit führt. Dies hat unmittelbare Auswirkungen auf die Gewährleistung eines angemessenen Sicherheitsniveaus für die Verarbeitung personenbezogener Daten. Die Erfahrungen der vergangenen Jahre haben gezeigt, dass pauschal umgesetzte Standard-Sicherheitsmaßnahmen zwar die IT-Sicherheit erhöhen können, jedoch nicht ausreichend sind, um Gefahren für die Rechte und Freiheiten der Betroffenen auszuschließen. Diesem Umstand hat der Gesetzgeber in Brandenburg Rechnung getragen und bei der Novellierung des Brandenburgischen Datenschutzgesetzes (BbgDSG) deutliche Vorgaben für den Bereich der Datensicherheit gesetzlich festgeschrieben. Nunmehr ist in § 7 Abs. 3 BbgDSG verankert, dass die Freigabe eines neuen

[1] vgl. A 8.6

automatisierten Verfahrens oder dessen wesentlichen Änderungen nur erteilt werden darf, wenn im Vorfeld eine Risikoanalyse und ein IT-Sicherheitskonzept erstellt wurde. Die getroffenen Entscheidungen sind kontinuierlich zu überprüfen und bei Bedarf an veränderte Bedingungen z. B. Veränderung der inneren Strukturen einer öffentlichen Stelle (Geschäftsprozesse, Fachaufgaben oder organisatorische Gliederungen), Veränderung der Bedrohungsszenarien, Weiterentwicklung der Sicherheitstechnik und Veränderung der äußeren Rahmenbedingungen anzupassen.

Vor Erstellung eines IT-Sicherheitskonzeptes ist es erforderlich, organisatorische Rahmenbedingungen zu schaffen, konzeptionelle Vorgaben zu erarbeiten und strategische Leitaussagen zu formulieren. Dies erfolgt in der Regel über eine IT-Sicherheitsleitlinie. Eine entsprechende IT-Sicherheitsleitlinie für die Landesverwaltung Brandenburg wurde Ende 2007 von der Landesregierung beschlossen und per Runderlass bekannt gegeben.[2] Da diese jedoch für Kommunen nicht verbindlich ist, müssen sie eigene Leitlinien schaffen. Wir empfehlen ihnen, sich dabei an der Leitlinie des Landes zu orientieren. Aufgabe der Leitlinie ist auch, das Bewusstsein der Behördenleitung für die Verantwortung in der IT-Sicherheit zu stärken.

Bei der Betrachtung aller technischen, organisatorischen, personellen und infrastrukturellen Komponenten bieten spezielle Instrumente Unterstützung. Das bekannteste und meist genutzte ist das Grundschutztool (GSTOOL)[3] des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Software richtet sich an Anwender der IT-Grundschutzkataloge und umfasst u. a. die Vorgehensweise zur Erstellung und Verwaltung von IT-Sicherheitskonzepten nach BSI-Standard 100-2 und 100-3. Dieses Tool ist für die unmittelbare Bundes-, Landes- und Kommunalverwaltung kostenlos. Das Bundesamt für Sicherheit in der Informationstechnik bietet zudem einen technischen Support an und entwickelt das Tool ständig weiter. Die Sicherheitskonzepte werden in Form einer Datenbank gespeichert. Dies erfolgt lokal auf einem mit dem Tool mitgelieferten Datenbank-Server oder auf einem zentral installierten SQL-Server.

Das schwächste Glied in der Kette einer funktionierenden IT-Sicherheit bestimmt das Sicherheitsniveau des gesamten Systems. Oftmals werden nicht unerhebliche Summen in die Errichtung von technischen Schutzmaßnahmen investiert, der Mensch jedoch nur unzureichend betrachtet. Personal und Organisation im Rahmen eines IT-Sicherheitskonzeptes müssen daher besondere Berücksichtigung finden.

---

2 vgl. A 5.3.3

3 siehe http://www.bsi.de/gstool/index.htm

Um Gefahren identifizieren, bewerten und angemessen reagieren zu können, bedarf es der Erstellung eines IT-Sicherheitskonzeptes. Zum Schutz der personenbezogenen Daten sind öffentliche Stellen in Brandenburg verpflichtet, ein IT-Sicherheitskonzept im Rahmen der Freigabe eines Verfahrens zu erstellen. Die Verantwortung für die IT-Sicherheit verbleibt bei der Behördenleitung und sollte in einer Sicherheitsleitlinie dokumentiert werden.

1.2.2 Verschlüsselung und elektronische Signaturen

Bereits in unserem letzten Tätigkeitsbericht[4] haben wir beschrieben, dass Verschlüsselung und elektronische Signaturen besonders geeignet sind, um die Vertraulichkeit, Verbindlichkeit und Integrität bei der Verarbeitung personenbezogener Daten zu gewährleisten. Vor der Einführung neuer IT-Verfahren sollte daher geprüft werden, ob Verschlüsselung und digitale Signaturen vom Verfahren überhaupt unterstützt werden.

Im Berichtszeitraum wurde vom Ministerium des Innern ein Personalinformationssystem ausgeschrieben.[5] Hierbei handelte es sich vorerst um ein Pilotprojekt, welches nach erfolgreichem Abschluss flächendeckend eingeführt werden sollte. Das derzeit im Einsatz befindliche Personalinformationssystem PERIS[6] ermöglicht eine Verschlüsselung der in der Datenbank gespeicherten personenbezogenen Daten. Als das Verfahren PERIS vor mehreren Jahren eingeführt wurde, waren sich alle an der Verfahrenseinführung beteiligten Stellen einig, dass eine Verschlüsselung der Datenbank eine wichtige Maßnahme zum Schutz der gespeicherten Personaldaten darstellt und damit beispielsweise auch ein Zugriff der Administratoren auf diese Daten wirksam verhindert werden kann.

Die Zeiten ändern sich. Im Fall des vom Ministerium des Innern neu ausgeschriebenen Personalinformationssystems wurden zwar Forderungen für eine Datenbankverschlüsselung im Pflichtenheft aufgenommen, dann aber der Zuschlag einer Firma erteilt, deren Produkt standardmäßig nur die Verschlüsselung eines einzigen Datenfeldes (Kreditkartennummer) zulässt.

Aus unserer Sicht ist schwer nachvollziehbar, warum Personalinformationssysteme, die bereits vor mehreren Jahren in den Wirkbetrieb überführt wurden, wesentlich sicherer waren, als angeblich „hochmoderne“ Personalinformationssysteme der Gegenwart. Ein Aspekt liegt unseres Erachtens auch darin begründet, dass die öffentlichen Auftraggeber aus Kostengründen und Unkenntnis der datenschutzrechtlichen Forderungen bevorzugt Softwarepro-

---

4 vgl. Tätigkeitsbericht 2004/2005, A 2.10

5 vgl. auch A 5.4.5

6 vgl. Tätigkeitsbericht 1997/1998, A 13.2.9

dukte „von der Stange“ kaufen, als notwendige Sicherheitsmaßnahmen von den Softwareherstellern einzufordern. Der Auftragnehmer wird natürlich nur das umsetzen, was der Auftraggeber fordert. IT-Verfahren, die beispielsweise primär für den wirtschaftlichen Sektor erstellt wurden, können nicht „eins zu eins“ in den öffentlichen Bereich übernommen werden.

Auch das Ministerium der Finanzen arbeitet derzeit mit Hochdruck an der Einführung eines neuen Verfahrens NFM (Neues Finanzmanagement)[7], welches das im landesweiten Einsatz befindliche Haushalts-, Kassen- und Rechnungswesen-Verfahren (HKR-Verfahren) ProFiskal P3 ablösen soll. Bereits im Jahr 1997 haben wir das Ministerium der Finanzen aufgefordert[8], technisch-organisatorische Maßnahmen zu realisieren, die den Schutz der übertragenen und in der Datenbank gespeicherten personenbezogenen Daten gewährleisten. Vom Ministerium der Finanzen wurde uns damals zugesichert, spätestens bei der Einführung eines neuen Verfahrens die Gesamtheit der erforderlichen Maßnahmen zu berücksichtigen. Doch wie sieht die Realität aus? Im neuen Verfahren NFM wird eine Datenbankverschlüsselung standardmäßig nur für ein einziges Datenfeld (Kreditkartennummer) analog dem oben beschriebenen Personalinformationssystem unterstützt. Da bei diesem Verfahren personenbezogene Daten mit hohem Schutzbedarf (Schutzstufe C unseres Schutzstufenkonzeptes) verarbeitet werden, ist eine Verschlüsselung der Datenbank zwingend erforderlich. Positiv ist dagegen hervorzuheben, dass das Ministerium der Finanzen im IT-Sicherheitskonzept des neuen Verfahrens den chipkartenbasierten Einsatz der elektronischen Signatur als notwendige technisch-organisatorische Maßnahme festgeschrieben hat.

In den nächsten Jahren wird es aufgrund der neuen EU-Dienstleistungsrichtlinie[9] voraussichtlich eine Vielzahl von neuen bzw. geänderten IT-Verfahren geben, um den Forderungen der Richtlinie gerecht zu werden. So muss beispielsweise Unternehmen, die planen, eine Dienstleistung anzubieten, zukünftig ermöglicht werden, sämtliche Verwaltungsangelegenheiten EU-weit elektronisch abzuwickeln. Auch in diesem Zusammenhang werden Verschlüsselungsverfahren und Verfahren zur Erzeugung einer elektronischen Signatur eine wichtige Rolle spielen. Nur unter Verwendung der qualifizierten elektronischen Signatur können Vorgänge rechtsverbindlich im Internet oder anderen Weitverkehrsnetzen elektronisch abgewickelt werden.

---

7 vgl. auch A 9.3

8 vgl. Tätigkeitsbericht 1997/1998 unter 1.4.1.6

9 Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt vom 12. Dezember 2006 (ABl. EG L 376, S. 36)

Es sollte bereits in einer frühen Projektphase geprüft werden, ob neu einzuführende IT-Verfahren den besonderen Anforderungen des Datenschutzes gerecht werden. So ist insbesondere sicherzustellen, dass bei der Verarbeitung von personenbezogenen Daten mit hohem Schutzbedarf Möglichkeiten zur Verschlüsselung und zur Erzeugung elektronischer Signaturen zur Verfügung stehen.

1.2.3 Gesundheitsamt der Zukunft − Bürokratieabbau um jeden Preis?

Im Landkreis Havelland werden kinderärztliche Reihenuntersuchungen für die Klassenstufen 5/6 und 10 seit dem Jahre 2004 durch ein privatrechtlich organisiertes Krankenhaus – die Havelland Kliniken GmbH – durchgeführt. Eigentlich handelt es sich bei diesen Untersuchungen jedoch um eine öffentliche Aufgabe. Zu prüfen war somit, ob die Verarbeitung der Gesundheitsdaten durch Private rechtmäßig ist bzw. in welchen Grenzen sie zu erfolgen hat.

§ 8 Abs. 2 und 3 Brandenburgisches Gesundheitsdienstgesetz legt fest, dass der öffentliche Gesundheitsdienst Schuluntersuchungen selbst durchzuführen hat. Allerdings räumt der brandenburgische Gesetzgeber den Kommunen durch das Brandenburgische Standarderprobungsgesetz[10] die Möglichkeit ein, von Standards und Normen des Landes abzuweichen. Das Ministerium für Arbeit, Soziales, Gesundheit und Familie hat den zunächst befristeten Modellversuch der privatrechtlich organisierten Reihenuntersuchungen auf der Grundlage dieses Gesetzes bis Ende des Jahre 2009 verlängert.

Nach wie vor besteht die Möglichkeit, die Reihenuntersuchungen durch staatliche Stellen vornehmen zu lassen. Dies ist jedoch für die Eltern mit einem erheblichen organisatorischen Aufwand verbunden. Somit haben sie die Wahl: Schicken sie ihre Kinder zu staatlich durchgeführten Untersuchungen, müssen sie Terminvereinbarungen und ggf. längere Wege in Kauf nehmen. Entscheiden sie sich für die Dienste der Havelland Kliniken GmbH entfallen diese Unannehmlichkeiten. Da die gesetzlichen Datenverarbeitungsbefugnisse aber nur für den öffentlichen Gesundheitsdienst vorgesehen sind, bedarf es dann allerdings einer Einwilligung der Eltern in die Verarbeitung der Gesundheitsdaten ihrer Kinder.

Fraglich ist bereits, ob die Genehmigung dieses Modellprojekts überhaupt rechtmäßig war. Der brandenburgische Gesetzgeber hat mit dem Standar-

[10] Gesetz zur Erprobung der Abweichung von landesrechtlichen Standards in Kommunen des Landes Brandenburg sowie von landesrechtlichen Zuständigkeitszuweisungen (Brandenburgisches Standarderprobungsgesetz – BbgStEG) vom 28. Juni 2006 (GVBl. I S. 74), geändert durch Artikel 1 des Gesetzes vom 12. Juli 2007 (GVBl. I S. 125)

derprobungsgesetz zwar eine Möglichkeit geschaffen, von den eigenen Normen abzuweichen, kann die Geltung von Bundes- oder Europarecht jedoch nicht außer Kraft setzen. Das Gesetz enthält eine entsprechende Einschränkung. Gemäß Art. 8 Abs. 3 der Datenschutzrichtlinie (Richtlinie 95/46/EG) dürfen Gesundheitsdaten nur von Personen verarbeitet werden, die besonderen Schweigepflichten unterliegen und deren Verletzung unter Strafe steht. Da die ärztliche Schweigepflicht sowohl für Ärzte in öffentlichen als auch in privatrechtlich organisierten Gesundheitsdiensten gilt, bestehen gegen eine Datenverarbeitung an sich durch sie keine Bedenken. In einem konkreten Fall beschwerten sich Eltern bei der Klinik über eine aus ihrer Sicht zu weit gehende Befragung ihrer Tochter im Rahmen der Untersuchung. Diese Beschwerde wurde – einschließlich der damit zusammenhängenden Gesundheitsdaten – vom Gesundheitsamt über die Personalstelle der Kliniken und den zuständigen Chefarzt weitergeleitet, bis sie schließlich die betroffene Ärztin erreichte. Datenschutzgerechter wäre es, eine Klärung der Beschwerde ausschließlich durch ärztliches Personal vorzusehen. Nicht unproblematisch ist es, die Krankenhausverwaltung bei der Ausübung von Aufsichtsbefugnissen als ärztliches Hilfspersonal zu werten, das der von der Richtlinie geforderten, besonderen Schweigepflicht unterliegt. Der hier beschriebene Beschwerdeweg ergibt sich aus der Wahl der Havelland Kliniken GmbH als Vertragspartner anstelle einer der Schweigepflicht unterliegenden Person. Die Rechtmäßigkeit der Genehmigung des Vertrags auf der Grundlage des Brandenburgischen Standarderprobungsgesetzes ist daher insoweit fraglich.

Da vergleichbare Standardabweichungen künftig auch durch das Brandenburgische Gesundheitsdienstgesetz ermöglicht werden sollen, legten wir den Schwerpunkt unserer Tätigkeit auf eine entsprechende Beratung des Gesetzgebers.

Die Verarbeitung von Gesundheitsdaten durch ein privatrechtlich organisiertes Krankenhaus im Rahmen von obligatorischen kinderärztlichen Reihenuntersuchungen kann nur mit Einwilligung der Eltern erfolgen.

1.2.4 Wie sicher ist das Zentrale Fahrerlaubnisregister?

Zukünftig werden die Daten von 50 Millionen Fahrerlaubnisinhabern im Zentralen Fahrerlaubnisregister beim Kraftfahrt-Bundesamt gespeichert. Doch wo bleibt die Sicherheit?

Mit dem Zentralen Fahrerlaubnisregister wird sowohl rechtlich als auch technisch ein neuer Weg bei der zentralen elektronischen Speicherung von personenbezogenen Daten beschritten. Die örtlichen Fahrerlaubnisregister werden abgeschafft und Daten nicht mehr längerfristig dezentral vorgehalten.

Sie werden sofort nach Einstellung in das zentrale Register gelöscht, sodass eine nachträgliche Plausibilitätskontrolle nicht mehr möglich ist.

Weder das Straßenverkehrsgesetz noch die Fahrerlaubnisverordnung tragen dem Umstand Rechnung, dass alle Fahrerlaubnisbehörden bundesweit Zugriff auf den Gesamtdatenbestand haben. Dies wirft verschiedene Probleme hinsichtlich der Anforderungen an den Online-Dialogbetrieb auf. Fragen zur Lesbarkeit oder Veränderbarkeit der Daten zur langfristigen Beweissicherheit einzelner Verfahrensschritte auch über lange Zeit und der datenschutzrechtlichen Verantwortlichkeiten sind noch ungeklärt. Es ist dringend erforderlich, die Rechtsverbindlichkeit und Beweiskraft der gespeicherten Informationen sowohl für die Betroffenen als auch für die Behörden dauerhaft sicherzustellen. Als technisches Verfahren steht die qualifizierte elektronische Signatur zur Verfügung. Ferner muss auch die Sicherheit der Daten vor Verlust und unbefugter Kenntnisnahme während der Übertragung − etwa mittels Verschlüsselung, gewährleistet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Bundesregierung aufgefordert, die dazu notwendigen Änderungen im Straßenverkehrsgesetz und der Fahrerlaubnisverordnung in die Wege zu leiten und rechtsverbindliche Festlegungen für die Datensicherheit zu treffen.

Nach dem derzeitigen Stand des Projekts zur Online-Anbindung der Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrtbundesamtes fehlen Vorkehrungen zur Datensicherheit, die gewährleisen, dass die Fahrerlaubnisdaten integer, authentisch, revisionsfähig und transparent verarbeitet werden.

1.2.5 Geoinformationen und Persönlichkeitsrechte

Geoinformationen – also Daten mit Bezug zu geografischen Standorten – sind aus unserem täglichen Leben nicht wegzudenken. Die Möglichkeiten der Informationstechnik, verbunden mit der präzisen Lokalisierung von Personen und Gegenständen durch Satelliten- oder Mobilfunksysteme, eröffnen eine vielfältige Verwendung: Detaillierte digitale Karten und Ortspläne unterlegt mit Satelliten- oder Luftbildern werden ebenso selbstverständlich genutzt wie Navigationssysteme oder standortbezogene Dienste im Mobilfunk. Auch Land und Kommunen erzeugen und nutzen Geoinformationen in vielfältiger Weise und stellen diese im Rahmen einer geplanten europaweiten Geodateninfrastruktur für Wirtschaft und Bürger zur Verfügung.

Beim Umgang mit Geoinformationen sind neben anderen rechtlichen Rahmenbedingungen auch datenschutzrechtliche Vorgaben einzuhalten: Geoin-

formationen enthalten nicht nur Angaben über bestimmte Eigenschaften eines bestimmten Teils der Erdoberfläche. Sie können – insbesondere durch die Verknüpfung mit anderen Datenbeständen – auch ganz konkret Auskunft über den Aufenthalt oder das Eigentum von Personen geben. Deshalb beschäftigen sich die Datenschutzbeauftragten von Bund und Ländern intensiv mit der Frage, unter welchen Bedingungen die öffentliche Verwaltung personenbezogene Geoinformationen erheben und weiterverarbeiten darf.

Dabei muss zunächst definiert werden, wann Geoinformationen überhaupt personenbezogen sind. Entscheidendes Kriterium ist, ob die Informationen einem konkreten Grundstück zugeordnet werden kann. Nur wenn dies der Fall ist, können Persönlichkeitsrechte eines Eigentümers betroffen sein. Dabei kommt es nicht darauf an, dass die Person des Eigentümers direkt bekannt ist. Diese kann regelmäßig ohne großen Aufwand ermittelt werden. Deshalb müssen z. B. Luftbilder oder Satellitenaufnahmen, auf denen konkrete Eigenschaften eines einzelnen Grundstücks erkennbar sind, als personenbezogene Daten betrachtet werden.

Sind Geoinformationen als personenbezogene Daten anzusehen, ist die nächste Frage, ob sie als allgemein zugänglich zu bewerten sind. Für solche Daten sieht das Brandenburgische Datenschutzgesetz ebenso wie andere Datenschutzgesetze nur geringe Einschränkungen für die Verarbeitung vor; insbesondere ist die Zweckbindung stark gelockert. So sind beispielsweise Daten über die topographische Beschaffenheit oder das Klima als öffentlich zugänglich anzusehen und damit nahezu unbeschränkt verwertbar. Anders verhält es sich beispielsweise mit Luftbildern von Grundstücken, die auch Auskunft über den Aufenthalt einer Person, vorhandene Fahrzeuge oder die konkrete Nutzung des Grundstücks geben.

Das Land Brandenburg hat zahlreiche eGovernment-Projekte auf den Weg gebracht, die die Erhebung oder Verwertung von Geoinformationen betreffen. Beispielhaft seien hier die Projekte Forcierte Automatisierte Liegenschaftskarte-Einrichtung (FALKE), Liegenschaftskataster-Online (LiKa-Online) sowie die Zusammenführung von Automatisierter Liegenschaftskarte, Automatisiertem Liegenschaftsbuch, Raumbezugsdaten und topographischen Informationen im AFIS-ALKIS-ATKIS-Projekt. Um hierfür rechtliche Rahmenbedingungen und einen Ausgleich zwischen den Interessen von Wirtschaft und Verwaltung einerseits und den Persönlichkeitsrechten der Eigentümer andererseits zu schaffen, hat das Ministerium des Innern den Entwurf eines Geobasisinformations- und Vermessungsgesetzes vorgelegt. Für den sich noch in der Abstimmung innerhalb der Landesregierung befindlichen Entwurf wurde die Landesbeauftragte in die Beratungen einbezogen und konnte datenschutzrechtliche Hinweise geben.

Künftig wird in Umsetzung einer europäischen Richtlinie[11] europaweit eine übergreifende Geodateninfrastruktur geschaffen, deren Umsetzung in deutsches Recht auch von den Datenschutzbeauftragten in Bund und Ländern zu begleiten sein wird.

Bei der Erhebung und Verwertung von raumbezogenen Informationen (Geodaten) sind die schutzwürdigen Belange der betroffenen Grundstückseigentümer zu beachten. Die Landesbeauftragte wird sich weiterhin für angemessene datenschutzrechtliche Rahmenbedingungen einsetzen.

1.2.6 Fingerabdrücke im elektronischen Reisepass – Wurden alle Sicherheitsmaßnahmen getroffen?

Schon seit dem Jahre 2005 werden in Deutschland Reisepässe mit einem Speicherchip ausgegeben, auf dem die Passdaten und das Foto in digitaler Form gespeichert sind. Auf der Grundlage internationaler und europäischer Vereinbarungen werden seit dem 1. November 2007 zusätzlich auf dem Chip zwei digitale Fingerabdrücke gespeichert. Da wegen der hohen Sensitivität dieser Daten technische und organisatorische Maßnahmen in einer ganz neuen Qualität zu treffen waren, wurde vom 1. März bis zum 30. Juni 2007 ein bundesweiter Feldtest durchgeführt.

Der Gesetzgeber hat eigens eine Rechtsgrundlage in das Passgesetz aufgenommen, die die notwendigen rechtlichen Voraussetzungen für die Durchführung des Feldtests geschaffen hat. An dem Test beteiligten sich neben verschiedenen Institutionen auf Bundesebene, den Ländern und der Bundesdruckerei GmbH auch zahlreiche Kommunen, darunter eine kreisfreie Stadt in Brandenburg. Während des Feldversuchs wurden in der Passbehörde von jedem Antragsteller zwei Fingerabdrücke (in der Regel rechter und linker Zeigefinger) mit einem Scanner aufgenommen, zwischengespeichert und elektronisch an die Bundesdruckerei übermittelt. Diese stellte aus den Daten einen gültigen Pass her, der allerdings nicht die Fingerabdrücke enthielt. Die Bundesdruckerei nutzte sie lediglich, um zu Versuchszwecken Testpässe herzustellen, bei denen auf dem Chip auch die Fingerabdrücke gespeichert wurden. Die bei den Passbehörden zwischengespeicherten Fingerabdrücke waren spätestens nach Aushändigung des Passes, die bei der Bundesdruckerei gespeicherten Daten bis 31. Juli 2007 zu löschen und die Testpässe zu vernichten.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht nutzte die Gelegenheit, sich bei Besuchen in der kreisfreien Stadt und in

[11] Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) (ABl. EG L 108, S. 1)

der Bundesdruckerei mit den grundsätzlichen Verfahrensabläufen bei der Beantragung und Ausstellung der elektronischen Reisepässe vertraut zu machen. Im Vordergrund stand dabei die Frage, wie bei der Passbehörde, der elektronischen Übertragung der Passdaten, der Weiterverarbeitung in der Bundesdruckerei und der Speicherung im Pass die Vertraulichkeit, Integrität und Authentizität der Daten gewährleistet werden. Insbesondere im Hinblick auf die Datenverarbeitung innerhalb der Passbehörde sowie die Übertragung an die Bundesdruckerei blieben zunächst einige Fragen offen, die während des Feldversuchs nicht abschließend geklärt werden konnten.

Nach der Aufnahme des Echtbetriebs am 1. November 2007 hat es eine Reihe von öffentlichen Diskussionen über die Datensicherheit im Zusammenhang mit dem elektronischen Reisepass gegeben. Die Datenschutzbeauftragten anderer Länder haben in ersten Prüfungen zum Teil erhebliche Mängel bei der Zwischenspeicherung biometrischer Daten in der Passbehörde, der sicheren Übertragung der biometrischen Daten über das Internet und bei der Prüfung der Authentizität der im Pass gespeicherten Fingerabdrücke festgestellt.[12] Zudem fehlte es an den notwendigen organisatorischen Grundlagen für eine sichere Datenverarbeitung: Fehlende Risikoanalysen und Sicherheitskonzepte sowie mangelndes Wissen über den Ablauf der Datenverarbeitung in den Passbehörden waren die Regel. Schließlich wurde mehrfach berichtet, dass sich die auf dem Chip gespeicherten Daten bereits aus größerer Entfernung auslesen ließen als vorgesehen.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird dies zum Anlass nehmen, die Beantragung und Ausstellung der elektronischen Reisepässe Anfang 2008 datenschutzrechtlich zu kontrollieren und zu überprüfen, ob die notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes getroffen worden sind.

Bei der Beantragung und Ausstellung elektronischer Reisepässe müssen die Passbehörden umfangreiche technische und organisatorische Maßnahmen treffen, um der hohen Sensitivität der im Pass elektronisch gespeicherten biometrischen Daten gerecht zu werden.

[12] siehe z. B. http://www.thueringen.de/imperia/md/content/datenschutz/die_epass_panne.pdf und http://www.lfd.m-v.de/dschutz/presse/pm-epass.pdf

1.3 Balance der Freiheit

1.3.1 Zwangsspeicherung des digitalen Lebens

Im letzten Tätigkeitsbericht haben wir über die auf europäischer Ebene geplante Einführung einer Vorratsdatenspeicherung in der elektronischen Kommunikation berichtet.[13] Nachdem die entsprechende europäische Richtlinie seit Mai 2006 in Kraft ist[14], hat der Deutsche Bundestag auf Vorschlag der Bundesregierung diese Vorgaben durch eine Änderung des Telekommunikationsgesetzes umgesetzt.[15]

Die neuen Vorschriften sehen vor, dass Anbieter, die öffentlich zugängliche Telefondienste, mobile Telefondienste und E-Mail-Dienste erbringen oder den Zugang zum Internet vermitteln (Access Provider), eine Reihe von Daten über die Inanspruchnahme dieser Dienste für einen Zeitraum von sechs Monaten speichern müssen. Damit wird nicht nur nachvollziehbar, wer mit wem zu welchem Zeitpunkt wie lange telefoniert hat. Zusätzlich werden beispielsweise bei der Nutzung eines Handys die Kennung von Gerät (IMEI) und SIM-Karte (IMSI) und der Standort bei Beginn des Telefonats, bei der E-Mail-Kommunikation die E-Mail- und die IP-Adressen von Absender und Empfänger sowie beim Internetzugang die dem Nutzer zugewiesene IP-Adresse und Beginn und Ende der Nutzung vorgehalten. Diese Verpflichtung gilt selbst dann, wenn der jeweilige Anbieter diese Daten nicht braucht und von sich aus gar nicht erst speichern würde.

Nach dem Gesetz werden die Daten grundsätzlich für die Verfolgung von Straftaten, zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit oder für Zwecke der Geheimdienste zur Verfügung stehen, soweit die für die Tätigkeit der jeweiligen Sicherheitsbehörden geltenden Gesetze (z. B. Strafprozessordnung, Polizeigesetze oder Verfassungsschutzgesetze) eine Nutzung dieser Daten konkret vorsehen.

Nach dem geltenden Verfassungsverständnis darf der Staat nur dann in Freiheitsrechte eingreifen, wenn es hierfür eine zwingende Rechtfertigung gibt, die in einem angemessenen Verhältnis zur Schwere des Eingriffs steht. Mit der angeordneten Vorratsdatenspeicherung wird nunmehr aber massiv in

---

13 vgl. Tätigkeitsbericht 2004/2005, A 3.2.1

14 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EG L 105, S. 54).

15 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198)

das grundrechtlich geschützte Fernmeldegeheimnis eingegriffen, obwohl auch die Befürworter dieser Eingriffe von vornherein davon ausgehen, dass die gespeicherten Kommunikations- und Bewegungsprofile fast nie benötigt werden. Die gesetzlich angeordnete anlassfreie Speicherung personenbezogener Daten widerspricht damit den vom Bundesverfassungsgericht aufgestellten Anforderungen an einen verfassungsgemäßen Eingriff in die Grundrechte der Betroffenen.

Die Datenschutzbeauftragten in Bund und Ländern haben daher in mehreren Entschließungen ihre Ablehnung der Vorratsdatenspeicherung bekräftigt.[16] Sie haben darauf verwiesen, dass die unbefangene Kommunikation eine der Grundvoraussetzungen einer freiheitlichen Gesellschaft ist, die durch die Vorratsdatenspeicherung erheblich beeinträchtigt wird. Zudem ist unverständlich, dass die Bundesrepublik Deutschland mit der Umsetzung der europäischen Vorgaben nicht abgewartet hat, bis der Europäische Gerichtshof über die Gültigkeit der europäischen Richtlinie entschieden hat.

Außerdem geht das Gesetz in einigen Punkten noch erheblich über die europäischen Vorgaben hinaus. Dies gilt insbesondere für die Tatsache, dass die unnötig vorgehaltenen Daten nicht nur für die Bekämpfung schwerer Straftaten, sondern auch für die Verfolgung bloßer Bagatellkriminalität zur Verfügung stehen sollen, sobald die Taten mittels Telekommunikation begangen sind.

Die von den Datenschutzbeauftragten geäußerten Befürchtungen, dass die einmal vorhandenen Daten weitere Begehrlichkeiten wecken, werden bereits Realität, bevor die Verpflichtung zur Vorratsdatenspeicherung umgesetzt ist: So hat der Bundesrat bereits wiederholt verlangt, dass die ursprünglich einmal zur Verfolgung schwerster Kriminalität, insbesondere terroristischer Straftaten gespeicherten Daten auch für rein zivilrechtliche Ansprüche von Rechteinhabern bei vermuteten Verletzungen von Urheberrechten zur Verfügung stehen sollten.

Inzwischen hat sich gezeigt, dass die Vorratsdatenspeicherung nicht nur das Vertrauen in eine unbeobachtete Kommunikation nachhaltig erschüttert, sondern auch die öffentlichen Stellen des Landes erheblich verunsichert. So haben wir bereits mehrere Anfragen erhalten, welche Daten eine öffentliche Stelle, die ihren Bediensteten die private Nutzung elektronischer Kommunikation anbietet, aufgrund der Verpflichtung zur Vorratsdatenspeicherung speichern muss. Die gesetzliche Verpflichtung zur Vorratsdatenspeicherung betrifft jedoch ausschließlich Anbieter von öffentlich zugänglichen Telekommunikationsdiensten. Hierzu gehören die Betreiber geschlossener Nutzer-

[16] siehe Anlagen 3.2 und 3.3.1

gruppen wie z. B. von Nebenstellenanlagen, Corporate Networks oder des Angebots der privaten Nutzung von E-Mail und Internet am Arbeitsplatz nicht, soweit diese Dienste nur den Beschäftigten zur Verfügung stehen. Eine Vorratsdatenspeicherung wäre in diesen Fällen rechtswidrig.

Die gesetzlich angeordnete Vorratsspeicherung von Daten über die Inanspruchnahme der elektronischen Kommunikation ist verfassungsrechtlich bedenklich. Auch fordern wir die Landesregierung auf, einer weiteren Aufweichung der Zweckbestimmung der gespeicherten Daten entschieden entgegenzutreten.

Öffentliche Stellen sind nicht befugt, Daten auf Vorrat zu speichern, wenn sie ihren Bediensteten die private Nutzung der dienstlichen Kommunikationseinrichtungen erlauben.

1.3.2 Heimliche Online-Durchsuchung von Computern

Am 31. Januar 2007 hat der Bundesgerichtshof einen Antrag des Bundeskriminalamts zur Online-Durchsuchung eines privaten Computers mit Verweis auf die fehlende Rechtsgrundlage abgelehnt.[17] Nach diesem höchstrichterlichen Beschluss hat das Bundesinnenministerium die Durchführung weiterer Online-Durchsuchungen sowie die Entwicklung der Durchsuchungssoftware (Remote Forensic Software, RFS) vorläufig gestoppt und strebt nunmehr zunächst die Schaffung einer ausreichenden Gesetzesgrundlage an. Gegen das nordrhein-westfälische Verfassungsschutzgesetz, welches eine entsprechende Befugnis enthält, wird unterdessen vor dem Bundesverfassungsgericht geklagt.

Nach Auffassung des Bundesgerichtshofs handelt es sich bei der Online-Durchsuchung nicht – wie ursprünglich vom Bundesinnenministerium vertreten – um eine Wohnraumdurchsuchung im Sinn von Art. 13 Grundgesetz (GG). Unabhängig von der Frage, ob das Recht auf Unverletzbarkeit der Wohnung auch vor einer Online-Durchsuchung schützt, steht aber fest, dass durch die Überwachung in das grundrechtlich garantierte Recht auf informationelle Selbstbestimmung eingegriffen wird.

Bei einer gesetzlichen Regelung wären deshalb besondere Verhältnismäßigkeits- und Verfahrensanforderungen zu beachten. Insbesondere wären Vorkehrungen zum Schutz des Kernbereichs der persönlichen Lebensgestaltung zu treffen, da Computer Informationen über eine Vielzahl an sozialen Interaktionen sowie an privaten und intimen Informationen enthalten können. Unab-

[17] Beschluss des Bundesgerichtshofs vom 31. Januar 2007 (StB 18/06)

dingbar wären schließlich ein Richtervorbehalt und die Verpflichtung, den Betroffenen im Nachhinein über den Eingriff zu benachrichtigen.

In dem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom August 2007 wird unter der Überschrift „Verdeckter Zugriff auf informationstechnische Systeme“ die Online-Durchsuchung geregelt. Danach soll die Datenerhebung zur Abwehr einer dringenden Gefahr oder zur Straftatenverhütung des internationalen Terrorismus zulässig sein, wenn dies andernfalls aussichtslos oder wesentlich erschwert wäre. Zielpersonen sind Störer und solche, die Informationen für den Störer entgegennehmen oder ihm ihren Computer überlassen. Weiterhin enthält die Vorschrift einen Richtervorbehalt und eine auf Behördenleiter bzw. deren Stellvertreter beschränkte Antragsbefugnis. Die Benachrichtigung der Betroffenen ist ebenfalls im Gesetzesentwurf geregelt. Eine Vorschrift zum Schutz des Kernbereichs privater Lebensgestaltung enthält darüber hinaus eine Einschränkung der bei Online-Durchsuchungen verwendeten Suchbegriffe, die das verfassungswidrige Eindringen in diesen Bereich von vornherein ausschließen soll. Ob dies überhaupt möglich ist, dürfte fraglich sein.

Unzulänglich sind die Anforderungen an die Bestimmtheit einer richterlichen Anordnung. Sie soll schon dann ergehen können, wenn die Zielperson zum Zeitpunkt der Aufnahme der Überwachung durch Name und Anschrift nicht genau sondern nur „soweit wie möglich“ bestimmt ist. Gerade bei eingriffsintensiven Ermittlungsmaßnahmen wie verdeckten Datenerhebungen muss aber bereits vor Beginn der Maßnahme sichergestellt werden, dass sie bei dem „Richtigen“, also dem polizeirechtlich Verantwortlichen für die Gefahr im Einzelfall erfolgt. Es ist davon auszugehen, dass bei den Vorermittlungen auch Name und Anschrift der Zielperson festgestellt würden. Entsprechendes gilt auch für das zu überwachende informationstechnische System. Es muss bekannt und damit genau zu bezeichnen sein, wenn die – wie beabsichtigt – speziell auf das Einsatzziel zugeschnittene RFS passen und wirksam sein soll. Das Erfordernis der Bestimmtheit ist auch bei der oben genannten Einschränkung der Suchbegriffe zu beachten. Nur so lässt sich ein effektiver Schutz des Kernbereichs der privaten Lebensgestaltung in einer laufenden Überwachung sicherstellen.

Neben den rechtlichen Bedenken gegen die Einführung von heimlichen Online-Durchsuchungen gibt es auch aus technischer Sicht eine Reihe von Aspekten, die bislang nicht hinreichend geklärt sind.

Kritisch zu beurteilen sind zunächst die Erfolgsaussichten bei der Einbringung der Durchsuchungssoftware RFS auf den Zielrechner bzw. in das Zielsystem. Zu den denkbaren Einbringungsmöglichkeiten gehören z. B. gezielt versandte

E-Mails mit der RFS als Anhang, verschenkte, „vergessene“ oder zugesandte CDs, USB-Speicher oder vergleichbare Datenträger, mit denen sich die RFS dem Adressaten unterschieben lässt, oder die Manipulation von Web-Seiten, von denen die RFS geladen wird. Diese Varianten erfordern die aktive Mitwirkung der Zielperson für ihren Erfolg. Es darf jedoch bezweifelt werden, ob es durch entsprechend sensibilisierte Personen zu einer solchen Mitwirkung kommt.

Weitere Möglichkeiten, die RFS auf dem Zielrechner zu platzieren, ergeben sich durch die Ausnutzung von Sicherheitslücken in der Standardsoftware mit Hilfe spezieller Programme (sog. Exploits), durch die Nutzung von Hintertüren, die von Herstellern auf Anforderung in Software eingebaut werden oder durch den physischen Zugriff auf den Rechner (z. B. nach Eindringen in die Wohnung des Betroffenen). Eine aktive Mitwirkung der Zielperson ist hierbei nicht erforderlich. Allerdings gibt es auch hier oft hinreichende Maßnahmen, die die Aussichten auf erfolgreiche Einbringung der RFS verringern (z. B. regelmäßige Systemupdates, Verwendung von Open Source Software, Verwendung und ständige Mitführung von tragbaren Rechnern, Komplettverschlüsselung der Festplatte). Zu beachten ist auch, dass es darüber hinaus eine Reihe von Gegenmaßnahmen gibt, mit denen Zielpersonen die Installation der Durchsuchungssoftware auf ihrem Rechner wirkungslos machen können. Hierzu gehören die Verwendung von getrennten PCs (Online- und Offline-System) mit kontrolliertem Datenaustausch, die Nutzung virtueller Zweitsysteme, die (Wieder-)Herstellung eines definierten, vertrauenswürdigen Ausgangszustandes des PCs vor Online-Aktivitäten (z. B. durch Live-CDs oder Systemabbilder) oder der Einsatz gängiger Sicherheitssoftware wie Firewalls, Einbruchserkennungssysteme oder heuristisch arbeitender Antivirensoftware.

Ungeachtet der Schwierigkeiten, die mit der Einbringung der RFS auf den Zielrechner verbunden sind, muss auch die Verlässlichkeit und Beweiskraft der im Zuge einer Online-Durchsuchung gewonnenen Erkenntnisse kritisch bewertet werden. Das Vorgehen bei der Online-Durchsuchung widerspricht dem der klassischen Computer-Forensik, bei der schreibgeschützte, bitweise identische Kopien von Datenträgern analysiert und nach relevanten Informationen durchsucht werden. Schon durch die RFS selbst wird der Untersuchungsgegenstand „Festplatte“ modifiziert. Ob weitere Änderungen auf dem Zielsystem durch Interaktionen zwischen den genutzten Software-Produkten sicher ausgeschlossen werden können und die RFS wirklich fehlerfrei und manipulationssicher funktioniert, kann – wenn überhaupt – nur durch Spezialisten mit sehr großem Aufwand verifiziert werden. Und letztlich stellt sich die Frage, welche Konsequenzen sich aus der möglichen Entdeckung der RFS durch die Zielperson oder Dritte ergeben. Wie soll dann verhindert werden, dass Spuren bewusst gelegt oder verfälscht werden?

Die Ermittlungsbehörden sollen zum Schutz des Kernbereichs der persönlichen Lebensgestaltung während der Online-Durchsuchung auch auf die Nutzung spezifischer Suchbegriffe, die nicht zur Erfassung von Inhalten aus diesem Bereich führen, vertrauen können. Allerdings sind weder die Suche nach bestimmten Datei- oder Verzeichnisnamen, nach Dateitypen oder -attributen noch die Volltextsuche nach Schlüsselworten geeignet, den Schutz des Kernbereichs allein mit technischen Mitteln zu garantieren. Ansonsten könnten sich Verdächtige anerkannter Begriffe der privaten Lebensführung für Dateinamen bedienen (z. B. geburtstagsliste.txt), um hinter diesen brisante Informationen zu verstecken.

Letztlich sind durch den Einsatz der Online-Durchsuchung auch negative Auswirkungen auf das Vertrauen in die IT-Infrastruktur und die IT-Sicherheit zu erwarten. Es dürfte in diesem Zusammenhang nicht verwundern, wenn staatliche E-Government-Angebote durch die Bürgerinnen und Bürger aus Angst vor einer heimlichen Online-Durchsuchung gar nicht oder nur sehr zögerlich genutzt würden.

Heimliche Online-Durchsuchungen von Computern sind mit erheblichen Eingriffen in die durch die Verfassung garantierten Grundrechte der Betroffenen verbunden. Sowohl aus rechtlicher als auch aus technischer Sicht bestehen begründete Bedenken gegen ihren Einsatz.

1.3.3 Novellierung des Brandenburgischen Polizeigesetzes

Im Jahre 2006 wurde das Brandenburgische Polizeigesetz novelliert und – neben der Änderung einiger bereits bestehender Vorschriften – die präventive Telekommunikationsüberwachung einschließlich Verwendung des so genannten IMSI-Catchers sowie die anlassbezogene Kennzeichenfahndung eingeführt.[18]

Das Brandenburgische Polizeigesetz enthält Vorschriften, bei denen starke Zweifel bestehen, ob sie den einschlägigen Entscheidungen des Bundes- und des Brandenburgischen Verfassungsgerichts Rechnung tragen. Hier sei daran erinnert, dass das Brandenburgische Verfassungsgericht schon bei dem Polizeigesetz von 1996 „die Grenzen des noch Angemessenen unter Wahrung des Wesensgehalts des Grundrechts“ nur gerade noch gewahrt sah.[19] Insgesamt ist aber nicht nur die Verfassungskonformität in Frage gestellt, sondern darüber hinaus auch die Normenklarheit und Verständlichkeit

[18] Viertes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 18. Dezember 2006 (GVBl. I S. 188)

[19] Urteil des Verfassungsgerichts des Landes Brandenburg vom 30. Juni 1999 (VfGBbg 3/98, Textziffer V c)

der geänderten Regelungen im Vergleich zum Kabinettsentwurf verschlechtert worden.

Eine der datenschutzrechtlich besonders bedenklichen Regelungen betrifft die Anordnung des Großen Lausch- und Spähangriffs (§ 33a, Abs. 4) und der Telekommunikationsüberwachung (§ 33b, Abs. 5). Eine Anordnung zur Telekommunikationsüberwachung kann schon ergehen, wenn die Zielperson des Eingriffs noch gar nicht konkret bekannt ist. Dies wäre aber allenfalls bei einer Anordnung zum Einsatz des IMSI-Catchers (§ 33b Abs. 5) – einem Gerät, das ein Handy überhaupt erst einmal identifiziert und seinen Standort feststellt – hinnehmbar. In einem solchen Fall liegt es in der Natur der Maßnahme, dass der Adressat noch nicht mit Name, Anschrift, Anschlussnummer u. Ä. eindeutig bestimmt ist. Alle anderen Anordnungen zur Überwachung von Kommunikationsinhalten verletzen jedoch das Bestimmtheitsgebot, wenn sie sich gegen Adressaten richten, zu denen nur unvollständige Angaben vorliegen. Immerhin muss der anordnende Richter prüfen, ob die Maßnahme nicht doch in den absolut geschützten Kernbereich persönlicher Lebensgestaltung des Betroffenen eindringt.

Weiterhin steht die unklare Bestimmung des „Adressaten“ im Widerspruch zu den beim Großen Lausch- und Spähangriff in § 33a Abs. 3 geforderten Voraussetzungen. Danach darf die Wohnungsüberwachung nur erfolgen, wenn die „Art der zu überwachenden Räumlichkeiten“ und das „Verhältnis der zu überwachenden Personen zueinander“ schon soweit abgeklärt worden sind, dass darüber Aussagen über den Kernbereich ihrer privaten Lebensgestaltung getroffen werden können.

Sehr bedenklich ist auch die Erweiterung des Kreises der Betroffenen auf die sog. Notstandpflichtigen. Bisher war eine Datenerhebung durch den verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes und zur Anfertigung von Bildaufzeichnungen außerhalb (§ 33 Abs. 1 und 2) wie innerhalb von Wohnungen (Abs. 3 bis 9) grundsätzlich auf den Kreis der Störer beschränkt. Nur wenn es um die Abwehr einer gegenwärtigen Gefahr für höchstrangige Individualgüter wie die körperliche Unversehrtheit und das Leben oder die Freiheit einer Person ging, durften auch nicht verantwortliche Personen in die polizeilichen Maßnahmen einbezogen werden und zwar unabhängig von ihrem Aufenthaltsort, also auch innerhalb ihrer Wohnung. Eine normenklare Vorschrift enthält das geänderte Polizeigesetz jedoch nicht. Vielmehr bleibt offen, wann genau Notstandspflichtige in den Kreis der Personen einzubeziehen sind, gegen die Überwachungsmaßnahmen durchgeführt werden dürfen. Durch die Verweisung ist § 33b aus sich selbst heraus nicht mehr verständlich. Die Vorschrift ist dadurch nicht mehr normenklar.

Mit § 33b Abs. 3 wurde zudem die Möglichkeit geschaffen, Telekommunikationsverbindungen nicht nur zu überwachen, sondern auch zu unterbrechen oder zu verhindern. Anders als bei der Unterbrechung eines einzelnen Telefonanschlusses sind bei der Unterbrechung des Fernsprechverkehrs von Handys nicht nur einzelne, sondern sämtliche in einer Funkzelle befindlichen Geräte betroffen. Das kann in Abhängigkeit von der konkreten Funkzelle mehrere hundert oder gar tausend Nutzer betreffen. Durch eine Unterbrechung der Kommunikation wird auf unbestimmte Dauer einer unbestimmten Anzahl von Teilnehmern die Ausübung eines Grundrechts verwehrt. Besonders problematisch ist, dass es im Unterbrechungszeitraum nicht möglich ist, Notrufe abzusetzen, was zu weiteren schweren Beeinträchtigungen führen kann. Im Gegensatz hierzu kann die Überwachungsbefugnis zu Ortungszwecken mittels IMSI-Catchergeräte noch hingenommen werden, da hier die tatsächliche Telekommunikation des Einzelnen nicht wahrnehmbar beeinträchtigt wird.

Neu aufgenommen wurde schließlich die Befugnis zur anlassbezogenen automatischen Kennzeichenfahndung. Selbst wenn sie nur anlassbezogen sein soll, stößt sie auf datenschutzrechtliche Bedenken, weil über eine Vielzahl von Personen Daten erhoben werden, die dazu durch ihr eigenes Verhalten keinen Anlass gegeben haben. Sie ist wie die Rasterfahndung ein Verdachtsgewinnungsinstrument, gerichtet gegen einen unbestimmten Personenkreis, von dem zum Zeitpunkt der Datenerfassung keine Gefahr im Sinne des Polizeirechts ausgeht. Ob bei der brandenburgischen Regelung der automatischen Kennzeichenfahndung das Verhältnismäßigkeitsprinzip ausreichend gewahrt wird, bleibt bis zu einer bevorstehenden Entscheidung des Bundesverfassungsgerichts über vergleichbare Vorschriften in den Polizeigesetzen von Bayern, Hessen und Schleswig-Holstein offen. Fest steht jedoch schon jetzt, dass durch den Einsatz automatischer Überwachungssysteme die Anzahl solcher Maßnahmen zunimmt, bei denen zunehmend gesetzestreue Bürger in polizeiliche Überwachungen einbezogen werden.

Die neuen Regelungen des Polizeigesetzes sind an vielen Stellen nicht ausreichend normenklar. Insbesondere bestehen Zweifel an der Verfassungsmäßigkeit der Vorschriften zum Großen Lausch- und Spähangriff sowie zur Telekommunikationsüberwachung. Ob und inwieweit die Vorschrift zur automatischen Kennzeichenfahndung Bestand haben wird, klärt das Bundesverfassungsgericht.

1.3.4 Verfassungsbeschwerde gegen das Antiterrordateigesetz

Im Dezember 2006 ist das Artikelgesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) in Kraft getreten. Art. 1 enthält das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Antiterrordateigesetz – ATDG).[20] Durch die Antiterrordatei wird ein Datenpool für die Erkenntnisse von Polizei und Nachrichtendiensten im Bereich der Terrorismusbekämpfung geschaffen, den es so bisher nicht gegeben hat. Im Juli 2007 ist Verfassungsbeschwerde gegen das Gesetz eingereicht worden. Der Aufforderung des Bundesverfassungsgerichts zur Stellungnahme sind die Datenschutzbeauftragten nachgekommen.

Mit Bundeskriminalamt, Bundespolizeidirektion, Landeskriminalämtern, Verfassungsschutzbehörden des Bundes und der Länder, Militärischem Abschirmdienst, Bundesnachrichtendienst und Zollkriminalamt sind durch § 1 Abs. 1 ATDG bereits 37 beteiligte Behörden zum Führen der Datei berechtigt. Dieser Kreis kann noch um weitere Polizeivollzugsbehörden − z. Zt. etwa 20 Stellen − erweitert werden. Insgesamt 57 Behörden greifen damit in Persönlichkeitsrechte ein. Dieser Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen wird dadurch noch verstärkt, dass personenbezogene Daten zusammengeführt werden, die von verschiedenen Bundes- und Landesbehörden mit unterschiedlichen Befugnissen auf unterschiedlichen Rechtsgrundlagen zu unterschiedlichen Zwecken gesammelt worden sind und von den beteiligten Stellen im Online-Verbund zu ihren unterschiedlichen Aufgaben mit unterschiedlichen Befugnissen genutzt werden können.

Die offene, den Kreis der beteiligten Behörden nicht eingrenzende Vorschrift, verletzt den Grundsatz der Normenklarheit und -bestimmtheit. Anlass, Zweck und Eingriffsgrenzen sind in der Ermächtigung aber möglichst genau festzulegen. Der Betroffene kann nicht ersehen, welche Polizeivollzugsbehörden die zu ihm gespeicherten Daten nutzen dürfen.

Verfassungsrechtliche Bedenken bestehen gegen die Regelung auch hinsichtlich der Wahrung des Verhältnismäßigkeitsgebots. Danach muss jede staatliche Maßnahme einen verfassungsrechtlich zulässigen Zweck verfolgen und geeignet, erforderlich und im Verhältnis zu dem beabsichtigten Zweck angemessen sein. Bei dieser Abwägung ist im Zusammenhang mit der Antiterrordatei zu berücksichtigen, dass dort auch „weiche“, d. h. auf ungesicherten, noch nicht abgeklärten Erkenntnissen beruhende, personenbezogene

[20] Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409)

Grunddaten und Wertungen der Nachrichtendienste gespeichert werden, die häufig weit im Vorfeldbereich tatsächlicher Gefahren erhoben wurden. Zu beachten ist weiterhin, dass die Nachrichtendienste zulässigerweise auch Erkenntnisse über Personen sammeln dürfen, deren Verhalten nicht nur zum Zeitpunkt der Erfassung sondern auch bei weiterer Beobachtung legal ist. Ausschlaggebend für die Verarbeitung personenbezogener Daten ist die nachrichtendienstliche Relevanz der Erkenntnis. Daher können auch Daten unbescholtener Personen Eingang in die Antiterrordatei finden. Zu den in der Datei zu speichernden Grunddaten gehören auch „besondere körperliche Merkmale“. Die Verarbeitung solcher sensitiven und höchst persönlichen Daten ist besonders dann ein schwerwiegender Grundrechtseingriff, wenn sie über einen Betroffenen gespeichert werden, der sich nichts hat zu Schulden kommen lassen.

Auch die Regelung des Inhalts der Antiterrordatei in § 2 ATDG ist aus Sicht der Datenschutzbeauftragten aus mehreren Gründen verfassungsrechtlich bedenklich. Bereits die Speicherung von Grunddaten in der Antiterrorismusdatei ist ein tiefer Eingriff in das Recht auf informationelle Selbstbestimmung mit ggf. weit reichenden Folgen für die Betroffenen. Allein die Tatsache der Speicherung im Zusammenhang mit Terrorismus kann für einen Betroffenen im Falle des Bekanntwerdens das Risiko erhöhen, im Alltag oder im Berufsleben gravierenden Nachteilen ausgesetzt zu werden.

Gem. § 2 ATDG ist bereits die „Befürwortung“ – im Gegensatz zur wesentlich weiter gehenden „Unterstützung“ – ein Tatbestandsmerkmal. Damit soll die Beobachtung möglichst weit ins Vorfeld verlagert werden, um mögliche Gefahrenquellen zu erkennen, von denen noch keine konkreten Handlungen ausgehen. So könnten auch Personen als bloße Befürworter in der Antiterrordatei gespeichert werden, die in internationalen Konflikten lediglich Partei ergreifen, aber über diese Meinungsäußerung hinausgehend keine weitere Aktivität entfalten oder beabsichtigen.

Nach dieser Vorschrift sind auch die Kontaktpersonen der in der Antiterrordatei geführten Personen zu speichern. Dabei handelt es sich nach der Legaldefinition um Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den als Primärpersonen zu Erfassenden nicht nur flüchtig oder zufällig in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind. Nach der Gesetzesbegründung können beispielsweise eine nähere persönliche oder geschäftliche Beziehung, die Dauer der Beziehung oder ein konspiratives Verhalten im Umgang untereinander als Kriterien für eine Einstufung als Kontaktperson ausreichen. Lediglich flüchtige oder rein zufällige Alltagskontakte reichen nicht aus. Es ist daher nicht unwahrscheinlich, dass insbesondere bei nicht eindeutigen Sachverhalten auch Daten Unbescholte-

ner als Kontaktpersonen in der Antiterrordatei eingestellt werden. Beispielsweise sehen die Verfassungsschutzgesetze eine Erfassung personenbezogener Daten auch unter der Voraussetzung vor, dass diese für die Erforschung und Bewertung einer verfassungsschutzrelevanten Bestrebung erforderlich sind. Diese Daten stehen dann auch den Polizeivollzugsdienststellen zur Verfügung, die sie ihrerseits wegen der für die Polizei geltenden engeren gesetzlichen Regelungen für Kontaktpersonen nicht selbst hätten erheben dürfen.

Schwerwiegende Grundrechtseingriffe bedürfen flankierender Vorkehrungen, die es ermöglichen, die Grundrechte der Betroffenen angemessen zu wahren. Eine Grundvoraussetzung dazu ist das Auskunftsrecht. Diese Voraussetzung erfüllt der einschlägige § 10 ATDG nur, soweit Daten offen, d. h. offen zugänglich für die beteiligten Behörden der Antiterrordatei, gespeichert sind. In diesen Fällen erteilt das Bundeskriminalamt im Einvernehmen mit der Stelle, die den Datensatz gespeichert hat, Auskunft. Für die verdeckt gespeicherten Daten, also die Datensätze, in die nur die einstellende, nicht aber die anderen beteiligten Behörden einsehen können, gelten für die Auskunftserteilung die Vorschriften der einstellenden Behörde.

Zum Verfahren bedeutet dies, dass das Bundeskriminalamt seine Auskunft auf die offen gespeicherten Daten beschränkt und wegen ggf. verdeckt gespeicherter Daten, dem Anfragenden lediglich die an der Antiterrorismus beteiligten Behörden nennt. Das hat zur Folge, dass ein Betroffener nur dann sicher sein kann, Auskunft über zu ihm in der Antiterrorismusdatei gespeicherten Daten zu erhalten, wenn er sein Ersuchen nicht nur an das Bundeskriminalamt richtet, sondern in einem zweiten Schritt auch an alle genannten Behörden. Doch selbst dann erlangt der Antragsteller wegen der Auskunftsverweigerungsvorschriften in allen einschlägigen Gesetzen keine Gewissheit.

Dieses Verfahren wird den Vorgaben, die sich aus der Rechtsschutzgarantie in Art. 19 Abs. 4 GG auch für das behördliche Verfahren ergeben, nicht gerecht. Die Garantie des effektiven Rechtsschutzes umfasst nicht nur die gerichtliche Kontrolle und das gerichtliche Verfahren, sondern sie muss schon beim behördlichen Verfahren einsetzen, wenn das für die Inanspruchnahme des gerichtlichen Rechtsschutzes erforderlich ist. Wirksamer Rechtsschutz gegen Eingriffe in das Recht auf informationelle Selbstbestimmung ist aber nur gegeben, wenn der Betroffene überhaupt Kenntnis von diesen Eingriffen erhält.

Angesichts verfassungsrechtlicher Bedenken gegen zentrale Regelungen des Antiterrordateigesetzes richtet sich die Hoffnung – wie seit einigen Jahren bei vielen Sicherheitsgesetzen – auf das Bundesverfassungsgericht als die Bürgerrechte wahrendes Korrektiv.

1.3.5 Novellierung des Urheberrechts – Aushöhlung des Fernmeldegeheimnisses für wirtschaftliche Zwecke

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung, Gefahrenabwehr und der nachrichtendienstlichen Tätigkeit beschnitten wurde, soll es durch eine anstehende Novellierung des Urheberrechts auch erstmals zugunsten privater wirtschaftlicher Interessen erheblich eingeschränkt werden.

Die Bundesregierung hat zur Umsetzung einer europäischen Richtlinie[21] einen Gesetzentwurf vorgelegt, der es den Inhabern von Rechten des geistigen Eigentums erleichtern soll, ihre Rechte durchzusetzen. Der Entwurf dient vor allem dem Ziel, die illegale Nutzung urheberrechtlich geschützter Werke durch Internet-Tauschbörsen oder das Herunterladen von Musik, Filmen oder Software aus dem Internet stärker zu unterbinden und Rechteinhaber vor der zunehmenden Produktpiraterie zu schützen.

Zentraler Baustein dieser Pläne ist ein Auskunftsanspruch, der den Rechteinhabern auch gegenüber solchen unbeteiligten Dritten zugestanden werden soll, die selbst keine Urheberrechtsverletzungen begangen haben. Insbesondere sollen Internet-Provider verpflichtet werden, Auskünfte über die vom Fernmeldegeheimnis geschützten Daten ihrer Nutzer zu erteilen. Damit sollen z. B. Anbieter und Nutzer illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können. Bisher ist dies nur auf der Grundlage eines Strafverfahrens möglich, da in das Fernmeldegeheimnis zugunsten privater wirtschaftlicher Interessen nicht eingegriffen werden kann.

Während die europarechtlichen Vorgaben den Mitgliedstaaten so viel Spielraum lassen, dass auf Eingriffe in das Fernmeldegeheimnis ganz verzichtet werden könnte, sieht der Gesetzentwurf solche Eingriffe sehr wohl vor, allerdings erst nach einer gerichtlichen Entscheidung. Die Länder haben im Bundesrat nun sogar gefordert, diesen richterlichen Vorbehalt zu streichen, sodass eine effektive vorherige Kontrolle von Eingriffen in das Fernmeldegeheimnis nicht mehr stattfinden würde.

Völlig unakzeptabel ist die darüber hinaus von den Ländern erhobene Forderung, die aufgrund der Verpflichtung zur Vorratsdatenspeicherung zwangsweise vorgehaltenen Daten über das Kommunikationsverhalten auch für die zivilrechtlichen Auskunftsansprüche der Rechteinhaber zu öffnen, obwohl

[21] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. EU L 157, S. 45)

diese Speicherung zunächst nur mit der Abwehr terroristischer Bedrohungen begründet wurde.[22]

Wir fordern die Landesregierung auf, einer weiteren Aushöhlung des Fernmeldegeheimnisses zugunsten privater Interessen im Bundesrat entschieden entgegenzutreten. Sie sollte sich zumindest dafür einsetzen, dass Eingriffe in das Fernmeldegeheimnis auch künftig nur mit richterlicher Erlaubnis stattfinden und Zugriffe auf Daten, die zum Zwecke der Ahndung schwerer Straftaten erhoben wurden, zur Verfolgung privater wirtschaftlicher Belange nicht zugelassen werden.

1.3.6 Zentrale Datenbanken – was von der Privatsphäre übrig bleibt

Aus allen Lebensbereichen gewonnene Daten können mittels großer Datenbanken zu umfassenden persönlichen Profilen zusammengeführt werden. Zunehmend werden solche Informationen an zentralen Stellen gesammelt. Die Auswertung scheinbar unbedeutender personenbezogener Daten und ihre Zusammenführung zu einem aussagekräftigen Persönlichkeitsprofil ist dann ein Kinderspiel.

Die Tendenz zur Einführung zentraler Datenbanken wird ergänzt durch eine immer engmaschigere Vernetzung bereits bestehender, dezentraler Datenbanken. Nicht nur öffentliche Stellen, sondern auch Wirtschaftsunternehmen erhalten so die Möglichkeit, aus einem nie da gewesenen Bestand personenbezogener Daten zu schöpfen. Während die erstmalige Einrichtung einer Datenbank zumeist an eine strenge Zweckbindung gekoppelt ist, wird diese später, wenn die entsprechenden Verfahren längst Routine sind, wieder teilweise oder vollständig zurückgenommen.

Dieser Tätigkeitsbericht beschäftigt sich unter anderem mit dem Aufbau einer zentralen Steuerdatei und der Vergabe einer einheitlichen und lebenslangen Steueridentifikationsnummer, die einem – verfassungswidrigen – zentralen Personenkennzeichen gleichzukommen droht (Gliederungspunkt A 9.2). Außerdem machen wir auf die geplante Antiterrordatei aufmerksam, die einer Vielzahl von Behörden einen Zugriff auf Erkenntnisse von Polizei und Nachrichtendiensten in ungekanntem Ausmaß ermöglicht (A 1.3.4). Auch werden künftig die Daten der Fahrerlaubnisinhaber in einem zentralen Register gespeichert, ohne dass derzeit die Sicherheit der Daten gewährleistet wäre (A 1.2.4). Der neue Elektronische Reisepass mit biometrischen Daten (e-Pass) enthält nunmehr zusätzliche Daten, die auf einem RFID-Chip gespeichert sind. Obwohl der Pass bereits eingeführt wurde, besteht nach wie vor ein Risiko, dass die Daten auch von Unbefugten ausgelesen werden können

[22] vgl. A 1.3.1

(A 1.2.6). Während niemand einen Reisepass besitzen muss, stellen entsprechende Planungen für den obligatorischen biometrischen Personalausweis eine noch gravierendere Gefahr für den Missbrauch personenbezogener Daten dar. Auch wenn diese dezentral gespeichert bleiben, können sie technisch betrachtet aber aufgrund der Vernetzung der Datenverarbeitung ohne weiteres zusammengeführt werden.

Die Erfassung des Verkehrs durch Kontrollstellen für die Autobahnmaut, das geplante nationale Bildungsregister mit einer bundesweit lesbaren Identifikationsnummer für Schüler, zentralisierte Scoringverfahren der Kreditwirtschaft zwecks Bonitätsprüfung der Kreditnehmer oder auch die Planungen für ein Bundesmeldegesetz, das möglicherweise ein einheitliches Melderegister schafft oder die vorhandenen, dezentralen Register vernetzt oder auch das Vorhaben, die Einkommensnachweise abhängig Beschäftigter bundesweit zu erfassen (Projekt ELENA – elektronische Einkommensnachweise) sind weitere Beispiele für mögliche Eingriffe in die Persönlichkeitsrechte der Bürgerinnen und Bürger.

Die Erfahrungen mit bereits bestehenden zentralen Datenbanken haben gezeigt, dass gerade die leichte Verfügbarkeit und Verknüpfbarkeit der Informationen stets neue Begehrlichkeiten weckt. Diese bewirken, dass über kurz oder lang die Zweckbindung aufgeweicht, die Zugriffsmöglichkeiten erweitert und die Datenerhebung ausgedehnt und somit die Eingriffe in das Recht auf informationelle Selbstbestimmung erweitert werden.

Zentrale Datenbanken gefährden in vielen Fällen die Datenschutzrechte der darin erfassten Bürgerinnen und Bürger. Sie stellen ein Instrument dar, das so sparsam wie möglich eingesetzt werden sollte. Die Landesbeauftragte stellt in diesem Tätigkeitsbericht anhand verschiedener Beispiele dar, welche Risiken zentrale Datenbanken bergen und wie diesen vorzubeugen ist.

1.4 Zehn Jahre Akteneinsichts- und Informationszugangsgesetz

„Die Bürokratie verbirgt ihr Wissen und Tun vor der Kritik, soweit sie es irgend kann ... Der Begriff des „Amtsgeheimnisses“ ist ihre spezifische Erfindung“.[23] Was der Soziologe Max Weber eher abstrakt beschrieb, beherzigte die Praxis lange Zeit durch das Befolgen der bekannten drei ehernen Grundsätze der öffentlichen Verwaltung: „Das haben wir noch nie so gemacht, das haben wir schon immer so gemacht, da könnte ja jeder kommen!“ Wer von der Verwaltung Informationen haben wollte, musste genau darlegen, wofür er sie benö-

[23] siehe Weber, Max, Wirtschaft und Gesellschaft, J. B. Mohr, Tübingen 1972, 5. Auflage, Nachdruck 1990: 572; 573

tigte; einen Anspruch hatte er außerhalb eines konkreten Verwaltungs- oder Gerichtsverfahrens nicht.

Das hat sich mit dem In-Kraft-Treten des Akteneinsichts- und Informationszugangsgesetzes am 20. März 1998 in Brandenburg geändert – das allgemeine Amtsgeheimnis gilt seither nicht mehr. Jetzt „kann jeder kommen“; das Gesetz gibt allen Interessierten einen grundsätzlichen Anspruch auf Informationszugang. Nicht mehr der Antragsteller muss sein Einsichtsinteresse darlegen, sondern die Verwaltung hat zu begründen, weshalb überwiegende schutzwürdige Geheimhaltungsinteressen diesem Wunsch gegebenenfalls entgegenstehen. Ein Zufall war es wohl nicht, dass gerade ein neues Bundesland diesen Weg als Erstes beschritt, hat die noch frische Erfahrung mit der DDR doch gezeigt, welche Bedeutung einem exklusiven Herrschaftswissen zukommen kann. Innerhalb der Bundesrepublik betrat Brandenburg mit der Regelung Neuland: Von den einen um die bürgerfreundliche Reform beneidet, erntete das Land skeptische Blicke von den anderen, die um den Bestand einer funktionsfähigen Verwaltung bangten.

Auch innerhalb Brandenburgs war die Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes umstritten. Dabei ergibt sich schon aus Art. 21 Abs. 4 der Landesverfassung die Notwendigkeit der Schaffung einer gesetzlichen Grundlage: Jeder hat „nach Maßgabe des Gesetzes das Recht auf Einsicht in Akten und sonstige Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen“. Das gilt auch für die – maßgeblich auf den Verfassungsentwurf des Runden Tisches zurückzuführenden – Informationsrechte der Bürgerinitiativen nach Art. 21 Abs. 3 der Landesverfassung. Diskutiert wurde vor allem die Frage, welchen Einschränkungen das Verfassungsrecht auf Informationsfreiheit in der Praxis unterworfen sein soll.

Erwartungen und Befürchtungen standen einander gegenüber. Die Befürworter blickten auf Länder wie Schweden oder die Vereinigten Staaten von Amerika. Dort gibt es eine lange Tradition der Transparenz sowie eine Verwaltungskultur, in der die Behörden sich selbst als Dienstleister für die Bürger verstehen. Der auch der Landesverfassung zu Grunde liegende Gedanke, dass eine politische Mitgestaltung nur gelingen kann, wenn die hierfür erforderlichen Informationen zur Verfügung stehen, stand im Mittelpunkt der Argumentation. Das Gesetz sollte die Möglichkeiten zur Teilhabe am politischen Geschehen in der noch neuen Demokratie fördern und es sowohl Bürgern als auch Bürgerinitiativen erleichtern, sich einzumischen. Je transparenter eine Verwaltung ist, desto leichter lassen sich, so die Hoffnungen der Befürworter, Amtsmissbrauch und Korruption wenn schon nicht völlig verhindern, so doch zumindest aufdecken.

Skeptiker wandten ein, dass ein allgemeines Recht auf Akteneinsicht einen zusätzlichen Verwaltungsaufwand nach sich ziehen könnte, der den täglichen Verwaltungsablauf zu sehr behindern würde. Die Beziehungen zu anderen Bundesländern sowie zum Bund – die damals noch keine Informationsfreiheitsgesetze kannten – seien gefährdet, weil den Verwaltungen des Landes Brandenburg aus Angst vor einer möglichen Herausgabe keine Informationen mehr übermittelt werden würden. Befürchtungen, das Gesetz könnte gar einen Standortnachteil bewirken, wurden damit begründet, Unternehmen müssten nunmehr befürchten, von Konkurrenten ausspioniert zu werden und daher abwandern oder sich gar nicht erst ansiedeln. Aber auch unter Datenschützern, die daran gewohnt waren, im Zweifelsfall eine restriktive Herausgabe von Informationen zu fordern, waren zumindest die Grenzen der Informationsfreiheit umstritten, obwohl gerade das Grundrecht auf „informationelle Selbstbestimmung“ dem Einzelnen auch ein Recht auf Teilhabe am Herrschaftswissen einräumt.

Während ein erster Fraktionsentwurf für ein Akteneinsichtsgesetz im Jahre 1994 auf Grund der Beendigung der Wahlperiode scheiterte, errang der drei Jahre später entstandene Regierungsentwurf für ein Akteneinsichtsrechtsgesetz schließlich Gesetzeskraft. Im Verlauf der Beratungen wurde er jedoch an wesentlichen Stellen modifiziert. Verzichtet wurde beispielsweise auf die ursprünglich geforderte Darlegung eines berechtigten Interesses als Voraussetzung für den Informationszugang. Im Gesetz wurde die Bestellung eines Landesbeauftragten für das Recht auf Akteneinsicht verankert, der Anwendungsbereich auf beliehene Unternehmer erweitert und die Behörden verpflichtet, die Antragsteller zu beraten sowie die Ablehnungen von Anträgen schriftlich zu begründen. Auch die zunächst vorgesehene Berücksichtigung des wirtschaftlichen Nutzens der Informationen bei der Berechnung der Gebühren wurde gestrichen. Schließlich trat das vom Landtag verabschiedete Akteneinsichts- und Informationszugangsgesetz am 20. März 1998 in Kraft. Sowohl der enge Anwendungsbereich des Gesetzes als auch die im Vergleich zu anderen Informationsfreiheitsregelungen zahlreichen und strikten Ausnahmetatbestände machen deutlich, dass es ein aus langem Ringen unterschiedlicher Standpunkte geborener Kompromiss ist. Unabhängig von der Expertendiskussion um die Frage, ob das Gesetz den Anforderungen der Landesverfassung im Einzelnen gerecht wird, begann mit ihm im Frühjahr vor zehn Jahren der Alltag der Informationsfreiheit in Brandenburg.

Die Praxis zeigte schnell, dass sich weder die hoffnungsvollen Erwartungen der Gesetzesbefürworter erfüllten, noch die apokalyptischen Befürchtungen der Gegner bewahrheiteten. Die anfängliche Schwierigkeit lag vielmehr in der mangelnden Bekanntheit der neuen Regelung. Während die Behörden unsicher in der Anwendung des Akteneinsichts- und Informationszugangsgesetzes waren oder von dessen Existenz vielfach noch gar nichts wussten, dach-

ten viele Bürger bei diesem Gesetz zunächst eher an den Anspruch auf Einsicht in Akten des Staatssicherheitsdienstes der DDR nach dem Stasiunterlagengesetz als an ein allgemeines Informationszugangsrecht.

In der Folgezeit ist es weder zu einem nicht zu bewältigenden Ansturm auf die Verwaltung gekommen, noch flüchteten Unternehmen vor der Informationsfreiheit in andere Bundesländer. Ebenso konnte weder ein sprunghafter Anstieg des politischen Engagements der Brandenburger verzeichnet, noch die Aufdeckung eines Korruptionsskandals mit Hilfe der Akteneinsicht vermeldet werden. Im Mittelpunkt des Interesses der Antragsteller standen die „kleinen“ Dinge des Alltags: Das Bauvorhaben in der eigenen Straße, die Konzeption einer Schulsportanlage, die geplante Ortsumfahrung, die Verkehrsüberwachung, die Kosten für Wasser und Abwasser, die Nutzung der Schwimmhalle, die Errichtung eines Kinderspielplatzes oder einer verkehrsberuhigten Zone. Nach den Unsicherheiten der ersten Jahre kam es zu einer gewissen Routine im Umgang mit dem neuen Recht.

In Zweifelsfällen hat jeder das Recht, die Landesbeauftragte für das Recht auf Akteneinsicht anzurufen, wenn er der Auffassung ist, in seinem Recht auf Informationszugang verletzt zu sein. Gleichwohl ist die Landesbeauftragte bemüht, dass es gar nicht erst zu einer Beschwerde kommt. Der Schwerpunkt ihrer Arbeit liegt dementsprechend im Vorfeld der formalen Petitionsverfahren – auf der Beratung von Bürgern und Akten führenden Stellen. Sie begleitet seit 1998 die Anwendung des Gesetzes auch durch Fortbildungen, rechtliche Gutachten und Stellungnahmen gegenüber dem Landtag und der Landesregierung, Bürgersprechstunden und die Herausgabe von Arbeitshilfen und Broschüren sowie durch ihr Internetangebot. Kommt es dennoch in einem Konfliktfall zu einer Eingabe an die Landesbeauftragte, bemüht sie sich in erster Linie um eine Vermittlung zwischen den beteiligten Parteien, sie kann aber auch Verstöße gegen das Akteneinsichts- und Informationszugangsgesetz feststellen und schließlich förmlich beanstanden. Zu diesem letzten Mittel ist es in den zurückliegenden zehn Jahren jedoch nur selten gekommen. Mit ihrer auf Vermittlung in Beschwerdefällen und Beratung öffentlicher Stellen ausgerichteten Tätigkeit trägt die Landesbeauftragte damit regelmäßig auch dazu bei, aufwändige und kostenintensive Widerspruchs- und Klageverfahren zu vermeiden.

Es hat sich gezeigt, dass der Löwenanteil der Anfragen von Bürgern an die Kommunen gerichtet ist. Entscheidungen, die hier gefällt werden, betreffen das eigene Lebensumfeld häufig viel unmittelbarer, als Entscheidungen oberster Landesbehörden. Inhaltlich waren vor allem Informationen aus der Bau- und Planungsverwaltung gefragt, aber auch beispielsweise Niederschriften von Gemeindevertretersitzungen oder solche aus den Bereichen Landwirtschaft, Umwelt- und Verbraucherschutz.

Immer wiederkehrende Schwierigkeiten weisen auf die Schwachstellen des Akteneinsichts- und Informationszugangsgesetzes hin. Einige wurden im Verlauf der letzten zehn Jahre – nicht zuletzt auch auf Vorschlag der Landesbeauftragten – ausgeräumt: Die zunächst fehlende Bearbeitungsfrist wurde ebenso ergänzt wie der verpflichtende Hinweis an den Antragsteller auf das Recht, die Landesbeauftragte im Ablehnungsfall anzurufen. Die Formulierung des Satzungserfordernisses zur Kostenerhebung durch die Kommunen wurde klarer gefasst und im Zuge der Anpassung verwaltungsrechtlicher Vorschriften an den elektronischen Rechtsverkehr neben der schriftlichen auch die elektronische Antragstellung ermöglicht.

Aber auch nach diesen Änderungen sieht das Gesetz in vielen Fällen die Ablehnung des Informationszugangs vor, obwohl ein berechtigtes Schutzinteresse überwiegender öffentlicher oder privater Belange nicht zu erkennen ist. So erstreckt sich bereits der Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes neben den öffentlichen Stellen nur auf beliehene Unternehmer. Auf andere privatrechtlich organisierte Unternehmen, die gleichfalls öffentliche Aufgaben wahrnehmen, findet das Gesetz keine Anwendung, selbst wenn sie sich zu hundert Prozent in staatlicher Hand befinden. Vor dem Hintergrund einer verstärkten Privatisierung öffentlicher Aufgaben werden die Informationsrechte dadurch nicht unwesentlich eingeschränkt.

Entsprechendes gilt hinsichtlich der Nichtanwendbarkeit des Akteneinsichtsrechts für laufende Verfahren.

Ein sehr restriktiver Schutz von Unternehmensdaten, aber auch von Angaben mit Personenbezug verringert die Chancen des Antragstellers auf Informationszugang. Daneben müssen Verwaltungen, bevor sie Informationen preisgeben dürfen, häufig erst Dritte um ihr Einverständnis bitten oder sie zumindest anhören, was zu einem hohen Bearbeitungsaufwand für die Verwaltung und einer langen Verfahrensdauer führt. Das gilt auch für solche Fälle, in denen durch die Gewährung der Akteneinsicht nicht oder nur sehr geringfügig in deren Rechte eingegriffen wird. Gestaltungsspielräume durch das Einräumen der Möglichkeit von Ermessensentscheidungen, die hier ausgleichend wirken könnten, fehlen.

Aufsichtsakten, also gerade solche Unterlagen, an deren Bekanntwerden ein verstärktes öffentliches Interesse besteht, sind nach dem Gesetz generell unzugänglich.

Ebenso enthält das Akteneinsichts- und Informationszugangsgesetz kein ausdrückliches Recht auf die Herausgabe von Fotokopien, was in der Praxis immer wieder zu unnötigen Komplikationen führt. Enttäuschungen auf Seiten

der Antragsteller, die sich einen weiter gehenden Informationszugang erhoffen, sind dadurch vorprogrammiert.

Andererseits spricht die in aller Regel routinierte und geräuschlose Anwendung des Akteneinsichts- und Informationszugangsgesetzes für die Fähigkeit der brandenburgischen Landes- und Kommunalverwaltung, in der Praxis das Beste daraus zu machen. Gemessen am gesamten Aufkommen landen nur relativ wenige Beschwerden auf dem Schreibtisch der Landesbeauftragten oder gar bei Gericht. Gründe für Beschwerden waren in den ersten Jahren häufig noch die Unkenntnis der neuen Rechtslage oder die Unsicherheit im Umgang mit dem Gesetz, später kamen immer kompliziertere rechtliche Fragen hinzu.

Die Anwendung des Akteneinsichts- und Informationszugangsgesetzes wird durch die Komplexität des gesamten Informationszugangsrechts erschwert. So können unterschiedliche Rechtsgrundlagen für den Informationszugang in Frage kommen. Neben den individuellen Einsichtsansprüchen der von einer Datenverarbeitung Betroffenen aus dem Datenschutzrecht sowie dem Zugangsrecht von Beteiligten in einem Verwaltungsverfahren ist häufig das dem allgemeinen Akteneinsichtrecht vorgehende Umweltinformationsgesetz zu beachten. Da viele Fragen – vor allem auf kommunaler Ebene – in unmittelbarem Zusammenhang mit Umweltinformationen stehen, soll an dieser Stelle vertieft darauf eingegangen werden:

Das Umweltinformationsgesetz regelt den Zugang zu Umweltinformationen und basiert auf der inzwischen weit gehend novellierten europäischen Umweltinformationsrichtlinie von 1990. Vier Jahre später wurde in der Bundesrepublik Deutschland das erste Umweltinformationsgesetz verabschiedet, das zunächst für Bund und Länder galt und erstmals einen – wenn auch auf den Umweltbereich beschränkten – Anspruch auf Informationszugang konstituierte. Auch in die brandenburgische Landesverfassung fand dieses Recht Eingang: Nach deren Art. 39 Abs. 7 hat jeder ein Recht auf derartige Informationen, soweit dem nicht überwiegende öffentliche oder private Interessen entgegenstehen. Seit März 2007 verfügt Brandenburg über ein eigenes Umweltinformationsgesetz, das inhaltlich in weiten Teilen auf das Bundesumweltinformationsgesetz verweist. Häufig ist nicht eindeutig zu klären, welchem Bereich die in der Akte enthaltenen Informationen zuzurechnen sind. Nur wenn es sich um solche über die Umwelt handelt, kommt das Umweltinformationsrecht zum Tragen. Überschneidungen zwischen diesem und dem Akteneinsichts- und Informationszugangsgesetz sind dabei eher die Regel als die Ausnahme. Dies gilt insbesondere auf dem Gebiet des Bauens und der Planung, da hier die meisten Maßnahmen oder Tätigkeiten naturgemäß auch Umweltauswirkungen zeitigen und das Interesse an einem Informationszugang höher ist als in anderen Bereichen. Problematisch ist dies

nicht nur im Hinblick auf die komplizierte Anwendung, sondern auch auf den dadurch deutlich werdenden Unterschied: Nach dem Umweltinformationsgesetz erhält der Antragsteller weiter gehende Informationen als nach dem recht restriktiven Akteneinsichts- und Informationszugangsgesetz. Letztlich hängt der Erfolg eines Einsichtsbegehrens in diesen Fällen nicht nur vom Sachverhalt, sondern vielmehr auch von der geschickten Auswahl und Darlegung der in Frage kommenden Rechtsgrundlage ab. Was auf der einen Rechtsgrundlage offen gelegt wird, muss auf der anderen geheim gehalten werden – diese unterschiedlichen Rechtsfolgen für eigentlich identische Informationsbegehren sind weder den Verwaltungen noch den Antragstellern zu vermitteln.

Der Gesetzgeber hat das Problem erkannt und die Geltung des Umweltinformationsgesetzes des Landes Brandenburg bis zum 31. Dezember 2008 befristet. Bis zu diesem Zeitpunkt soll es mit dem Akteneinsichts- und Informationszugangsgesetz zu einer einheitlichen Regelung zusammengeführt werden. Dabei wird es darauf ankommen, anwendbare und allgemein verständliche Formulierungen zu finden und die Regelungen soweit wie möglich zu vereinheitlichen. Ein und derselbe Sachverhalt darf keine unterschiedlichen Rechtsfolgen mehr nach sich ziehen.

Während Brandenburg vor zehn Jahren noch als Vorreiter der Informationsfreiheit galt, haben mittlerweile acht Bundesländer Informationsfreiheitsgesetze verabschiedet, andere diskutieren derzeit entsprechende Gesetzentwürfe. Einige dieser Länder haben von Brandenburg – dem vorsichtigen Pionier – gelernt und sind mutiger vorgegangen. Ausnahmetatbestände sind dort oft mit Ermessensspielräumen versehen und der Anwendungsbereich weiter gefasst. Für das Informationsfreiheitsgesetz des Bundes, das gegenüber Bundesbehörden gilt, trifft dies allerdings nur bedingt zu. Zu groß scheinen die Widerstände und Bedenken gewesen zu sein, als dass der Gesetzgeber sich hier zu einer weiter gehenden Regelung hätte durchringen können.

Vorangebracht wird die Transparenz der öffentlichen Verwaltung hingegen verstärkt durch die Europäischen Gemeinschaften, deren Transparenzverordnung (Verordnung EG Nr. 1049/2001) aus dem Jahre 2001 gerade überarbeitet wird. Der Zugang zu wichtigen Dokumenten sowohl aus der Rechtssetzung als auch Rechtsprechung über die Webseiten der Gemeinschaft hat sich seither entscheidend verbessert; Parlament, Kommission und Rat bieten im Internet Dokumentenregister und Hilfestellungen an, um das Auffinden von Informationen zu erleichtern.

Aber nicht nur in Bezug auf die eigenen Informationen sowie im Umweltbereich wirkt das europäische Gemeinschaftsrecht als Motor für die Entwicklung in Brandenburg. Vielmehr hat sich die Europäische Gemeinschaft auch inten-

siv mit der Frage der Weiterverwendung öffentlicher Informationen befasst. Sie stellte fest, dass die komplexen und unterschiedlichen Nutzungsregelungen in den einzelnen Mitgliedsstaaten eine Hemmschwelle für solche Unternehmen darstellen, die aus Informationen des öffentlichen Sektors Informationsprodukte weiterentwickeln und auf dem Markt anbieten. Eine entsprechende Richtlinie aus dem Jahr 2003 wurde durch das Informationsweiterverwendungsgesetz vom 13. Dezember 2006 umgesetzt. Dieses Gesetz gilt auch für öffentliche Stellen in Brandenburg. Es soll einheitliche Konditionen für die Vermarktung von Informationen des öffentlichen Sektors durch private Unternehmen herstellen, enthält aber kein eigenes Zugangsrecht. Vielmehr basiert es auf den vorhandenen Informationszugangsregelungen, also auch auf dem brandenburgischen Akteneinsichts- und Informationszugangsgesetz. Nur was auf dessen Grundlage herausgegeben wird, kann auch von der Wirtschaft genutzt werden. Der Markt kann sich folglich nur so gut oder schlecht entwickeln, wie die Rechtslage die Offenlegung von Informationen vorsieht. Dem Informationsrecht kommt somit eine wirtschaftliche Dimension zu, deren Bedeutung in einer Dienstleistungsgesellschaft stetig wächst und bereits heute einen Wert von mehreren Milliarden Euro umfasst. Auch dies wird bei einer Neugestaltung des Informationszugangsrechts in Brandenburg zu beachten sein.

Durch eine Konsultation über die „Europäische Transparenzinitiative“ löste die Kommission ein lebhaftes öffentliches Interesse aus. Hintergrund der Initiative war unter anderem das Ziel, die Transparenz auf dem Gebiet der Fördermittelvergabe zu verbessern. Im Ergebnis der Konsultation hat sich die Europäische Union nunmehr zu vollständiger Transparenz in Bezug auf die Empfänger von Geldern aus dem Gemeinschaftshaushalt verpflichtet. Ab 2008 werden die Daten der Empfänger von Zuschüssen aus den Strukturfonds, ab 2009 die Daten der Empfänger von Geldern im Rahmen der Gemeinsamen Agrarpolitik veröffentlicht. Da die Fördermittel vor allem von den Mitgliedsstaaten ausgereicht werden, hat dieser Beschluss unmittelbare Bedeutung auch für das Land Brandenburg. Das Wissen um den Verbleib von Steuergeldern wird damit einen entscheidenden Schritt vorangebracht. Im Zuge der Weiterentwicklung der brandenburgischen Informationsrechte kann dies nicht länger durch starre Ausnahmetatbestände ignoriert werden.

Weit über den tagespolitischen Horizont hinaus reicht auch das Anliegen von Verbrauchern, Verbänden und Bürgerinitiativen, die sich mit den kargen Informationen über die von ihnen konsumierten Produkte nicht mehr zufrieden geben wollen. Als Reaktion auf die zahlreichen Lebensmittelskandale der letzten Jahre hat der Bundesgesetzgeber im Jahre 2007 das auch von Landesbehörden anzuwendende Verbraucherinformationsgesetz verabschiedet. Dadurch erhalten die Verbraucher einen Anspruch auf Informationen, die den Behörden vorliegen, also beispielsweise über die Beschaffenheit und die

Herstellungsbedingungen von Lebensmitteln oder über ihre Eignung, Allergien auszulösen. Die Behörden haben ihrerseits das Recht, über bestimmte Sachverhalte aktiv zu informieren und unter Umständen die Namen von Firmen bekannt zu geben, von deren Produkten ein Risiko ausgehen könnte. Wegen weit gehender inhaltlicher Ausnahmen und zeitintensiver Verfahrensvorschriften sieht sich das Gesetz massiver Kritik ausgesetzt. Sein wesentlicher Verdienst besteht darin, dem Thema der Verbraucherinformationen überhaupt eine gewisse Aufmerksamkeit zuteil werden zu lassen.

Nicht nur durch die Rechts-, sondern auch durch die technologische Entwicklung wird die Transparenz öffentlicher Stellen permanent fortentwickelt. Insbesondere die verstärkte Nutzung des Internet sowohl durch Verwaltungen als auch durch Antragsteller weist auf den wachsenden Bedarf an Informationen hin. Es reicht heute nicht mehr, nur noch Pressemitteilungen und offizielle Verlautbarungen auf die behördliche Website zu stellen. Weiter gehende Informationen sind gefragt. Aktive Veröffentlichungspflichten werden durch Informationsfreiheitsgesetze anderer Länder sowie durch das Umweltinformationsgesetz bereits festgeschrieben. Das routinemäßige Einstellen häufig eingesehener Dokumente ins Internet gehört zur alltäglichen Arbeit beispielsweise amerikanischer Behörden. Diese sind zugleich verpflichtet, eigene Internet-Seiten zur Informationsfreiheit zu führen, die meist hohe Besucherzahlen aufweisen.

Der Wandel in den Beziehungen zwischen Bürger und Staat ist keineswegs abgeschlossen. Auf dem Gebiet der Informationsfreiheit zeigt sich vielmehr, dass nicht nur das Bewusstsein über die Bedeutung von Informationen, sondern auch die Kommunikationsbeziehungen zwischen beiden Seiten einer ständigen Weiterentwicklung unterliegen. Die Verwaltungskultur passt sich allmählich den Anforderungen nach größerer Transparenz an. Diese Praxis steht in einer Wechselwirkung mit den Gesetzen, die solche Änderungen einerseits forcieren, zumindest aber nachholend beschreiben, andererseits jedoch begrenzen. Die in Brandenburg geplante Zusammenführung des Akteneinsichts- und Informationszugangsgesetzes mit dem Umweltinformationsgesetz bietet dem Land die Möglichkeit, sich in Deutschland nach zehn Jahren wieder an die Spitze der Informationsfreiheit zu setzen.

2 Technisch-organisatorische Entwicklungen

2.1 Vorabkontrolle – neu im Brandenburgischen Datenschutzgesetz

Beim erstmaligen Einsatz oder bei wesentlichen Änderungen automatisierter Verfahren, von denen besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können, ist vor der Verfahrensfreigabe eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten durchzuführen.

Nach § 10a Brandenburgisches Datenschutzgesetz (BbgDSG) ist die Vorabkontrolle vor dem erstmaligen Einsatz der automatisierten Verfahren oder bei wesentlichen Änderungen durchzuführen. Wesentliche Änderungen sind beispielsweise das Hinzufügen neuer sensitiver Datenarten, die Einführung zusätzlicher Datenübermittlungen, die Erweiterung automatisierter Datenabrufe oder − bei einer Datenverarbeitung im Auftrag − die Wahl eines anderen IT-Dienstleisters. Sofern lediglich die eingesetzte Hardware oder das Betriebssystem geändert werden, stellt dies keine wesentliche Verfahrensänderung dar.

Besondere Risiken für die Rechte und Freiheiten der Betroffenen bestehen regelmäßig bei der Verarbeitung personenbezogener Daten gem. § 4a BbgDSG. Dazu zählen Angaben:

- über die rassistische oder ethnische Herkunft,
- zu politischen Meinungen,
- zu religiösen oder weltanschaulichen Überzeugungen,
- über die Zugehörigkeit zu Gewerkschaften oder Parteien,
- über die Gesundheit oder das Sexualleben.

Eine Vorabkontrolle ist aber regelmäßig auch dann durchzuführen, wenn in dem Verfahren Daten verarbeitet werden, die Strafverfahren, Ordnungswidrigkeiten, sensitive Bereiche der öffentlichen Sicherheit und Ordnung oder Personaldaten betreffen.

Das Datenschutzrecht sieht für diese Art personenbezogener Daten ein besonders hohes Schutzniveau vor, das bei der Zulässigkeitsprüfung für eine automatisierte Datenverarbeitung zu beachten ist. Diese darf nur eingeführt werden, wenn den damit verbundenen Gefahren für die Persönlichkeitsrechte

der Betroffenen mit ausreichend starken Schutzmaßnahmen entgegengewirkt werden kann und die verbleibenden Restrisiken unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar sind.

Die Daten verarbeitende Stelle hat zur Prüfung der Zulässigkeit der Datenverarbeitung und der erforderlichen Sicherheitsmaßnahmen dem behördlichen Datenschutzbeauftragten unter anderem die Ergebnisse einer Risikoanalyse und das daraus abgeleitete Sicherheitskonzept[24] vorzulegen. Zur Beurteilung des Verfahrens sind darin vor allem konkrete Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz für das automatisierte Verfahren zu treffen. Stellt das Sicherheitskonzept ein zu hohes verbleibendes Restrisiko fest, muss geprüft werden, ob durch eine Nachbesserung technischer oder organisatorischer Maßnahmen noch eine datenschutzgerechte Verarbeitung ermöglicht werden könnte. Ist das nicht der Fall, darf das Verfahren nicht freigegeben werden.

Wir begrüßen die Aufnahme der Vorabkontrolle in das BbgDSG. Sie ersetzt allerdings nicht die Notwendigkeit, bereits im Vorfeld bei der Planung von IT-Verfahren datenschutzrechtliche Belange ausreichend zu berücksichtigen. Mit der Vorabkontrolle werden die Befugnisse der behördlichen Datenschutzbeauftragten wesentlich erweitert, sie haben im Zweifelsfall unsere Behörde zu konsultieren.

2.2 Biometrische Verfahren – Welcher Finger darf's denn heute sein?

Biometrische Verfahren sind in aller Munde. Politik und Wirtschaft sehen in ihrem Einsatz ungeahnte neue Möglichkeiten der zuverlässigen und sicheren Erkennung von Personen. Zu den aktuellen Anwendungen gehören z. B. die Nutzung des Fingerabdrucks als Ersatz für den Zündschlüssel im Auto oder zur Freigabe von Zahlungen per Mobiltelefon. Und aus der Politik werden immer wieder Forderungen nach einer zentralen Speicherung biometrischer Merkmale aller Bürgerinnen und Bürger für Zwecke der Aufklärung von Straftaten laut.

Prominentestes Beispiel des praktischen Einsatzes biometrischer Verfahren ist in Deutschland zurzeit die Ausstattung von Reisepässen (und demnächst auch von Personalausweisen) mit einem per Funk auslesbaren Chip, auf dem das Gesichtsbild sowie die Bilder von zwei Fingerab-

[24] vgl. A 2.11

drücken des Inhabers gespeichert sind. Über den aktuellen Stand dieser Projekte informieren wir an anderer Stelle in diesem Bericht.[25]

Allgemein befasst sich die Biometrie mit der Messung und Auswertung bestimmter Merkmale von Lebewesen. Im hier betrachteten Kontext geht es um die automatisierte (Wieder-)Erkennung von Personen anhand ihrer Merkmale. Durch die Nutzung moderner Rechentechnik soll dieser Prozess vereinfacht, beschleunigt und verlässlicher gestaltet werden.

Bei den individuell charakteristischen Eigenschaften, die in biometrischen Verfahren genutzt werden, ist zwischen physiologischen Merkmalen und verhaltensbasierten Merkmalen zu differenzieren. Zur ersten Gruppe gehören z. B. das Gesichtsbild, Finger- oder Handabdruck, Irismuster und DNA. Der zweiten Kategorie sind z. B. Schreib- und Sprechverhalten, Tippgewohnheiten an der Tastatur, Mimik, Gestik oder Gang zuzuordnen. Es gibt mittlerweile biometrische Systeme, die mehrere Merkmale zur Erkennung einer Person heranziehen oder bei denen Merkmale mehrfach gemessen werden. Beides soll die Genauigkeit des Ergebnisses erhöhen.

Bei jedem biometrischen Verfahren ist eine Phase des sog. Einlernens (Enrolment) erforderlich. Diese dient dazu, die biometrischen Merkmale erstmalig zu erfassen, zu bearbeiten und mit der Zuordnung zur betreffenden Person digital zu speichern. Die Speicherung kann in Form von Rohdaten (z. B. als Bild- oder Tondatei) oder Referenzmustern (Templates) erfolgen. Bei letzteren werden aus den Rohdaten nur die jeweils wesentlichen, charakteristischen Elemente extrahiert und abgespeichert (z. B. wichtige Punkte im Gesicht und ihre Lage zueinander). Aus Sicht des Datenschutzes ist die Speicherung von datensparsameren Referenzmustern der Speicherung von Rohdaten vorzuziehen.

Soll die betreffende Person nach dem Einlernen (wieder-)erkannt werden, so werden die biometrischen Merkmale erneut erfasst und digitalisiert. Für den Abgleich mit den gespeicherten Daten gibt es zwei Varianten: Bei der Verifikation gibt die Person an, eine bestimmte Identität zu besitzen. Das System vergleicht die aktuellen mit den gespeicherten biometrischen Daten und bestätigt die Identität oder nicht (1:1-Abgleich). Bei der Identifikation vergleicht das System die aktuellen biometrischen Daten mit allen gespeicherten Datensätzen und bestimmt die Person aus dieser Menge (1:n-Abgleich). Während bei der Identifikation die biometrischen Daten aller Betroffenen, die bestimmt werden sollen, zentral in einer Datenbank gespeichert werden müssen, ist dies bei der Verifikation nicht erforderlich. Hier reicht eine dezent-

[25] vgl. A 1.2.6

rale Speicherung beim Betroffenen selbst (wie z. B. im Funkchip des Reisepasses).

Alle biometrischen Verfahren liefern prinzipiell nur Aussagen zum Grad der Übereinstimung von aktuell gemessenen und gespeicherten biometrischen Daten: Überschreitet die Übereinstimmung einen einstellbaren Schwellwert, wird die Person als erkannt angesehen. Insofern gibt es bei jedem biometrischen Verfahren Fehler. Betrachtet man z. B. ein System zur Zugangskontrolle, so können einerseits Personen vom System akzeptiert werden, obwohl sie zwar selbst keine Berechtigung, aber sehr ähnliche biometrische Merkmale eines Berechtigten haben. Andererseits können Personen zurückgewiesen werden, die eigentlich berechtigt wären, deren biometrische Merkmale aber wegen ungünstiger Bedingungen nur unzureichend erkannt werden. Die Häufigkeit von Fehlern beider Arten kann durch die Konfiguration des biometrischen Systems beeinflusst werden. Fehlerraten bei gängigen Systemen zur Gesichts- oder Fingerabdruckerkennung liegen zwischen 0,01 % und 10 %. Die Fehlerraten bei der DNA-Analyse sind um Größenordnungen kleiner.

Aktuelle Forschungen zu biometrischen Verfahren betreffen neben der Verbesserung der Leistungsfähigkeit bekannter Verfahren und der Senkung ihrer Fehlerraten auch neue Aspekte, wie z. B. die Erkennung und Verfolgung von Einzelnen in einer großen Personenmenge oder die Identifizierung verdächtigen Verhaltens von Personen. Weiterhin wird intensiv an der Erhöhung der Überwindungssicherheit und der Lebenderkennung bei der Messung biometrischer Merkmale gearbeitet. In der Vergangenheit wurde immer wieder öffentlichkeitswirksam demonstriert, dass bestimmte biometrische Verfahren mit relativ einfachen Mitteln überlistet und dadurch falsche Identitäten vorgetäuscht werden konnten.

Sollen biometrische Daten in DV-Verfahren genutzt werden, so sind zuvor eine Reihe von Fragen des Datenschutzes und der IT-Sicherheit zu klären. Eine Erhebung und Speicherung biometrischer Daten ist überhaupt nur dann zulässig, wenn eine entsprechende Rechtsgrundlage oder die Einwilligung der Betroffenen vorliegt. In jedem Fall sind die Forderungen nach Datensparsamkeit und einer strengen Zweckbindung biometrischer Daten zu beachten. Dies gilt umso mehr, da einige biometrische Merkmale zusätzliche Informationen über den Betroffenen enthalten können (z. B. über Krankheitsbilder, Berufsgruppen, ethnische Gruppen). Für das beabsichtigte biometrische Verfahren ist nachzuweisen, dass es für den angestrebten Zweck geeignet und praxistauglich ist. Die Fehlerraten sind dabei zu berücksichtigen.

Da biometrische Verfahren Personen (mit großer Wahrscheinlichkeit) eindeutig bestimmen, können biometrische Daten auch als Referenzmerkmal für die Verknüpfung mit Daten zu diesen Personen aus anderen Systemen dienen.

Eine solche Profilbildung ist zu verhindern. Deshalb sollte, auf eine Speicherung biometrischer Daten in zentralen oder vernetzten Datenbanken verzichtet werden. Eine dezentrale Speicherung dieser Daten in der Obhut des Betroffenen ist demgegenüber zu bevorzugen.

Weiterhin ist bei der Konzeption eines DV-Verfahrens, in dem biometrische Daten genutzt werden sollen, darauf zu achten, dass durch Diebstahl oder Verlust dieser Daten Unberechtigte falsche Identitäten vortäuschen könnten. Um dem vorzubeugen, sind die biometrischen Daten durch geeignete Sicherheitsmaßnahmen vor unberechtigtem Zugriff zu schützen. Neben einer sehr restriktiven Zugriffskontrolle wird empfohlen, biometrische Daten nur verschlüsselt über Datennetze zu übertragen und sie nur verschlüsselt zu speichern. Weitere technische und organisatorische Maßnahmen sind im Ergebnis einer Risikoanalyse für das Verfahren zu bestimmen.

Letztlich ist darauf hinzuweisen, dass bei der beabsichtigten Nutzung biometrischer Daten in Unternehmen oder Behörden (z. B. zu Zwecken der Zutrittskontrolle) die jeweiligen Datenschutzbeauftragten sowie die Beschäftigtenvertretungen frühzeitig und umfassend zu beteiligen sind. Es ist das Gebot der Transparenz zu beachten: Betroffene müssen wissen, welche ihrer Daten warum und wie verarbeitet werden. Eine Diskriminierung einzelner Personen wegen fehlender oder unzureichend ausgeprägter biometrischer Merkmale und dadurch verursachte häufige fehlerhafte Zurückweisungen oder zusätzliche Kontrollen sind zu vermeiden.

Zu Problemen des Datenschutzes beim Einsatz biometrischer Verfahren haben wir im Berichtszeitraum gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ein Faltblatt erstellt, das in unserem Internetangebot abrufbar ist.[26]

Ist beabsichtigt, in einem Projekt ein biometrisches Verfahren zu nutzen, sind neben fachlichen Aspekten der Eignung biometrischer Merkmale oder der Leistungsfähigkeit des konkreten Verfahrens insbesondere Fragen des Datenschutzes sowohl aus rechtlicher als auch aus technisch-organisatorischer Sicht zu klären. Im Zweifel sollte auf die Nutzung der Biometrie verzichtet werden.

[26] siehe http://www.lda.brandenburg.de → Informationsmaterial

2.3 RFID – Was gibt's Neues?

Bereits in unserem letzten Tätigkeitsbericht[27] hatten wir ausführlich über die RFID-Technik berichtet. Dabei wurden die technischen Grundlagen, Anwendungsmöglichkeiten und Risiken aus Datenschutzsicht sowie Forderungen an Hersteller und Anwender dieser Technik dargestellt. Welche Entwicklungen sind seitdem zu beobachten?

RFID (Radio Frequency Identification) bezeichnet eine Technik, mit deren Hilfe sich Objekte durch Funkkommunikation eindeutig identifizieren lassen. Die Objekte werden dazu mit einem RFID-Chip (auch als RFID-Tag bezeichnet) ausgestattet, der über eine Antenne Signale von einem Lesegerät empfangen kann und daraufhin die auf ihm gespeicherten Daten zurückliefert. Einfache RFID-Chips können nur eine (weltweit eindeutige) Seriennummer speichern, fortgeschrittene Chips verfügen über die Fähigkeit, komplexe Berechnungen (z. B. zur Verschlüsselung) auszuführen und können mehrere Hundert Kilobyte speichern. Zu einem RFID-System gehört neben den RFID-Chips und den Lesegeräten für die Funkkommunikation immer auch ein sog. Hintergrundsystem zur Weiterverarbeitung der RFID-Daten. Je nach Anwendungsgebiet sind hier komplexe Datenbanken, Warenwirtschafts- und Logistiksysteme, Steuerungssysteme für Türöffner u. a. anzutreffen.

Die aktuellen Entwicklungen im Bereich der RFID-Technik sind einerseits gekennzeichnet durch eine zunehmende Miniaturisierung der Chips selbst. So begnügt sich der weltweit kleinste, von einer japanischen Firma vorgestellte RFID-Chip mit einer Grundfläche von 0,05 mm x 0,05 mm. Seine Dicke wird mit 5 Mikrometer angegeben. Er ist mit dem menschlichen Auge nicht mehr von einem Staubkorn zu unterscheiden. Der Chip kann eine 38-stellige Zahl als eindeutigen Identifikator speichern und einem Lesegerät in einer Entfernung bis zu 30 cm zurückliefern. Als potentielles Anwendungsgebiet wird die Integration in Papierdokumente zur Sicherung gegen Fälschungen angegeben. Ein ähnliches Beispiel der fortschreitenden Miniaturisierung konnten kürzlich Besucher einer Fachkonferenz in Frankfurt am Main erleben. Auf deren Eintrittskarten waren RFID-Chip und Antenne aufgedruckt. An den Eingängen wurde der auf dem Chip gespeicherte eindeutige Code zur Kontrolle der Zugangserlaubnis verwendet.

Andererseits werden aktuell zunehmend die Möglichkeiten der Anwendung der RFID-Technik und deren Akzeptanz beim Verbraucher erkundet. Folgende Beispiele sollen dies verdeutlichen:

[27] vgl. Tätigkeitsbericht 2004/2005, A 1.2

- Eine große Warenhauskette in Deutschland beginnt zurzeit damit, im Bereich der Herrenbekleidung Einzelprodukte mit Funkchips auszustatten. Es wird zugesichert, die Daten auf den RFID-Chips nicht mit Kundendaten zu verknüpfen und die Chips beim Bezahlen zu entfernen. Das muss jedoch nicht immer so bleiben. So könnten z. B. Gewährleistungsansprüche an die Existenz und Funktionstüchtigkeit eines RFID-Chips gekoppelt sein. Welche Anwendungsmöglichkeiten sich aus der Integration von Funkchips in Kleidung ergeben, zeigt eine Schule in Großbritannien: Dort wird die Anwesenheit von Schülern und ihr Aufenthaltsort im Schulgebäude über in Schuluniformen eingebrachte Funkchips kontrolliert.

- In mehreren Regionen Deutschlands laufen zurzeit Pilotprojekte, bei denen spezielle Mobiltelefone genutzt werden, um per Funkkommunikation an Haltestellen Fahrkarten für den Öffentlichen Personennahverkehr zu erwerben. Hierzu wird das NFC-Verfahren (Near Field Communication) verwendet, bei dem die Reichweite der Funkkommunikation auf wenige Zentimeter begrenzt ist. Auch in der Stadt Potsdam soll voraussichtlich ab 2009 ein ähnliches System unter dem Namen „Touch & Travel“ voll zum Einsatz kommen. Andere NFC-Anwendungen sind z. B. der Austausch von Visitenkarten zwischen Mobiltelefonen oder die Anzeige personalisierter und ortsbezogener Werbung beim Passieren von mit NFC-Technik ausgestatteten Orten.

- International gibt es in mehreren Ländern Projekte, die Nummernschilder von Kraftfahrzeugen mit (aktiven) RFID-Chips zu versehen. Die Reichweite der Funkkommunikation beträgt dabei zwischen 2 und 100 Metern. Offiziell sollen mit diesen Systemen z. B. Steuersünder, Mautpreller oder Autodiebe überführt werden. Sie lassen sich jedoch auch für eine Überwachung des Verkehrs bzw. des Bewegungsverhaltens einzelner Fahrer nutzen. Bereits heute gibt es außerhalb Deutschlands Kfz-Versicherungen, die ihren Kunden Rabatte einräumen, wenn sie sich verpflichten, technische Geräte zur Kontrolle des Fahrverhaltens einbauen zu lassen.

Die Beispiele zeigen, dass die RFID-Technik neben nützlichen Funktionen auch erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich trägt. Die Datenschutzbeauftragten des Bundes und der Länder haben sich deshalb auf ihrer 72. Konferenz im Oktober 2006 zum wiederholten Mal mit dem Problem beschäftigt und die Entwicklungen bewertet. Ihre Ergebnisse sind in einer Entschließung[28] zusammengefasst. Die wesentlichen Forderungen sind:

[28] siehe Anlage 3.4.2

- umfassende Information der Betroffenen über Einsatz, Verwendungszweck und Inhalt von RFID-Chips,

- Kennzeichnung von Produkten mit Funkchips und von Kommunikationsvorgängen, die durch diese ausgelöst werden,

- Verzicht auf die heimliche Bildung von Verhaltens-, Nutzungs- und Bewegungsprofilen,

- Einsatz technischer Maßnahmen, um eine unbefugte Kenntnisnahme von auf RFID-Chips gespeicherten und per Funk übertragenen Daten zu verhindern,

- Deaktivierung von RFID-Chips bzw. Löschen der darauf enthaltenen Daten, wenn diese nicht mehr für den ursprünglichen Zweck erforderlich sind.

Zu Problemen des Datenschutzes beim Einsatz der RFID-Technik haben wir im Berichtszeitraum gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ein Faltblatt erstellt, das in unserem Internetangebot abrufbar ist.[29]

Eine verbindliche Selbstverpflichtung der Hersteller bzw. Anwender von RFID-Technik zu einem datenschutzgerechten RFID-Einsatz existiert zurzeit noch nicht. Durch diese Verpflichtung und die Umsetzung der Forderungen des Daten- und Verbraucherschutzes könnte ein Eingreifen des Gesetzgebers zur Regulierung der Anwendung der RFID-Technik vermieden werden. Gleichzeitig ist jeder Einzelne gefordert, gegenüber RFID-Anwendern auf die Einhaltung seiner Persönlichkeitsrechte zu achten.

2.4 Wie viele neue Freunde hast du heute schon gewonnen? – Datenschutz im Web 2.0

Schon seit geraumer Zeit ist das Internet nicht mehr nur eine Einbahnstraße, über die Websurfer Informationen abrufen, in Versandhauskatalogen blättern und online einkaufen oder den nächsten Urlaub buchen. Zunehmend werden die Nutzer selbst zu Anbietern von Informationen, gestalten Webseiten und deren Inhalte aktiv mit oder versuchen, über das Medium Internet soziale Kontakte zu Gleichgesinnten aufzubauen.

Diese Entwicklung wird im Allgemeinen mit dem Schlagwort „Web 2.0“ bezeichnet und fasst eine Reihe verschiedener interaktiver und kooperativer Techniken bei der Nutzung des Internet zusammen. Zu den typischen Er-

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

scheinungsformen gehören z. B. Diskussionsforen zum Austausch von Meinungen über (fast) jedes beliebige Thema, Wikis zur gemeinsamen Erstellung und Bearbeitung von Dokumentensammlungen oder persönliche, jedoch öffentliche Internet-Tagebücher (so genannte Weblogs oder Blogs). Zunehmend beliebt sind insbesondere die technischen Nachbildungen sozialer Netze im Internet durch Plattformen wie MySpace, Facebook, Xing, StudiVz, SchülerVZ u. a.

Die ersten Anfänge des „Mitmach-Netzes“ waren etwa Mitte der 90er Jahre zu beobachten, der Begriff „Web 2.0“ wurde im Rahmen einer internationalen Konferenz 2004 geprägt. Seit dieser Zeit entwickeln sich die Angebote explosionsartig: MySpace hat nach eigenen Angaben ca. 200 Millionen Mitglieder (von denen jedoch nicht alle regelmäßig aktiv sind), Facebook ca. 50 Millionen weltweit. Bei den deutschsprachigen Plattformen Xing (für berufliche Kontakte) und StudiVZ (vorrangig für Studenten) gibt es jeweils ca. 4 Millionen Nutzer. Auf die zugehörigen Webseiten wird heute häufiger zugegriffen als auf etablierte, reine Informationsangebote im Internet wie z. B. große Nachrichtenportale.

Die hohe Attraktivität der Internetplattformen für soziale Netze liegt zunächst darin, dass jeder Nutzer selbst relativ einfach Webseiten mit persönlichen Informationen erstellen und veröffentlichen kann (so genannte Profile). Diese Selbstporträts enthalten häufig private Daten (Alter, Wohnort, Tätigkeit, Interessen, Freizeitaktivitäten, Kontaktmöglichkeiten) und werden ergänzt durch Fotos oder Videos der Nutzer. Studien haben ergeben, dass bereits ca. ein Viertel der Jugendlichen im Alter zwischen 12 und 19 Jahren in Deutschland sich auf diese Weise im Internet präsentiert.

Neben der reinen Selbstdarstellung ermöglichen die Plattformen für soziale Netze auch die Anbahnung und Gestaltung von Kontakten mit anderen Nutzern. So können z. B. Verweise auf die Präsentationen von Freunden und Bekannten aus der „Realwelt“ gesetzt, Verabredungen getroffen oder neue, virtuelle Freundschaften mit Unbekannten geschlossen werden. Anerkennung wird häufig allein schon durch die pure Anzahl von „Freundschaften“ gewonnen. Weiterhin kann man sich in offenen oder geschlossenen Diskussionsgruppen mit anderen Mitgliedern über gemeinsam interessierende Themen austauschen.

Viele Plattformen gestatten darüber hinaus, Verknüpfungen mit anderen Informationsangeboten oder Diensten im Internet herzustellen und bieten so neue, fortgeschrittene Dienste an. Ein Beispiel ist etwa die Integration von Kartenmaterial, um allen Kontaktpartnern im sozialen Netz den eigenen aktuellen Aufenthaltsort bekannt zu geben.

Die große Beliebtheit und die hohen Mitgliederzahlen der sozialen Netze im Internet dürfen jedoch nicht darüber hinweg täuschen, dass bei ihrer Nutzung auch Gefahren für die Einhaltung der Privatsphäre auftreten können. Beispielsweise ist es denkbar, mit Hilfe der persönlichen Daten, die im Internet z. B. in sozialen Netzen publiziert wurden, umfangreiche Persönlichkeitsprofile zu erstellen. Schon heute greifen viele Arbeitgeber auf Internetsuchmaschinen zurück, um zusätzliche Informationen über Bewerber für eine Stelle zu erhalten. Peinliche Jugendfotos oder Lästereien über ehemalige Chefs wirken dann sicher nicht Karriere fördernd. Aber auch die aktive Teilnahme an Diskussionsforen zu bestimmten Krankheiten oder zu politischen Themen können Nachteile im privaten oder beruflichen Leben bewirken. Zu beachten ist, dass die Bildung von Persönlichkeitsprofilen heute zunehmend technisch unterstützt wird, dabei verschiedene Quellen verknüpft werden und auch ein automatisierter Abgleich von veröffentlichten Fotos möglich ist. So lassen sich auch unterschiedliche Pseudonyme oder Mailadressen u. U. eindeutig einer Person zuordnen.

Eine weitere Gefahr kann daraus entstehen, dass sich persönliche Informationen der Nutzer im sozialen Netz für eine personalisierte, genau auf diesen Nutzer zugeschnittene Werbung verwenden lassen. Internetplattformen für soziale Netze finanzieren sich meist über Werbung, sodass die Plattformbetreiber die Daten ihrer Nutzer gern Partnerunternehmen für Werbezwecke zur Verfügung stellen. Allerdings funktioniert die Kooperation auch in die andere Richtung: Erst kürzlich begann z. B. Facebook damit, Daten über das (Einkaufs-)Verhalten seiner Mitglieder bei Partnerunternehmen automatisch auch an registrierte Freunde zu verteilen. Viele Nutzer waren jedoch nicht damit einverstanden, dass Nachrichten wie „Peter hat ein Selbsthilfebuch für Alkoholiker gekauft“ ungefragt an alle Kontaktpersonen geschickt wurden. Wegen der zahlreichen Proteste ist nun das explizite Freischalten dieser Benachrichtigungsfunktion erforderlich. Insgesamt lässt sich der Trend feststellen, dass mit Hilfe von Programmierschnittstellen ein Datenaustausch zwischen Plattformen für soziale Netze und Externen ermöglicht werden soll. Für den einzelnen Nutzer wird damit immer undurchsichtiger, wer welche persönlichen Daten kennt, wohin diese übermittelt oder für welche Zwecke sie verwendet werden.

Zu anderen Risiken, denen Nutzer im Web 2.0 ausgesetzt sind, gehören der Identitätsdiebstahl (also das gezielte Ausspähen von Identitätsinformationen durch Angreifer und das anschließende Agieren in fremdem Namen), das Hacking persönlicher Webseiten in sozialen Netzen durch Angreifer und das Verbreiten von Schadsoftware über die manipulierten Seiten sowie Mobbing und Cyber-Stalking. Bei letzteren werden technische Mittel (z. B. direkte Nachrichten, E-Mails, Diskussionsforen, Schwarze Bretter) für Nachstellungen, Belästigungen, Beleidigungen, Verleumdungen oder üble Nachrede

missbraucht. Dies ist sowohl innerhalb als auch außerhalb von Plattformen für soziale Netze möglich. Die Opfer können finanzielle, psychische oder gar körperliche Schäden davontragen.

Aus dem Gesagten lassen sich eine Reihe von Empfehlungen für Nutzer des „Web 2.0“ – insbesondere für den Umgang mit Plattformen für soziale Netze – ableiten:

- Seien Sie kritisch. Entwickeln Sie ein gesundes Misstrauen.

- Veröffentlichen Sie nur solche persönlichen Daten, die Sie auch Fremden gegenüber offenbaren würden. Verzichten Sie insbesondere auf die Angabe der vollständigen privaten Adresse, Telefonnummer usw.

- Beachten Sie, dass private Fotos, Videos oder Äußerungen in Diskussionsforen auch noch nach Jahren anderen Personen ein Bild von Ihnen vermitteln. Nicht alle sind Ihnen wohl gesonnen.

- Prüfen Sie Kontaktwünsche sorgfältig. Seien Sie vorsichtig bei unbekannten Personen und allzu vertraulicher Ansprache.

- Verwenden sie unterschiedliche Pseudonyme auf unterschiedlichen Plattformen. Wählen Sie Pseudonyme, die keinen Rückschluss auf Ihren wirklichen Namen zulassen. Entscheiden Sie entsprechend dem Zweck der Plattform über die publizierten persönlichen Daten.

- Konfigurieren Sie Ihr Profil wenn möglich so, dass persönliche Daten unbekannten Dritten nur eingeschränkt angezeigt werden und Schnittstellen zu anderen Plattformen oder Internetdiensten ausgeschaltet sind.

- Prüfen Sie die Plattform und den Betreiber, insbesondere die Aussagen zur Verwendung der Daten, zur Übermittlung an Dritte, zur Transparenz der Datenverarbeitung oder zu den Möglichkeiten, Missbrauch zu verhindern oder zumindest zu melden.

- Beachten Sie, dass einmal im Internet veröffentlichte Informationen nur sehr schwer zu löschen sind. Das Internet vergisst nichts.

- Suchen Sie von Zeit zu Zeit selbst nach Informationen über sich im Internet und kontrollieren Sie ggf. deren Herkunft und Verwendung.

Die Europäische Agentur für Netzwerk- und Informationssicherheit ENISA, ein Beratungs- und Kompetenzzentrum für die EU-Mitgliedsstaaten und EU-

Organisationen, hat im Oktober 2007 ein Positionspapier[30] veröffentlicht, in dem detailliert die Gefahren, die auf Internetplattformen für soziale Netze entstehen können, diskutiert und Empfehlungen für Anbieter solcher Plattformen sowie für staatliche Stellen abgeleitet werden.

Nutzer der neuen, interaktiven Möglichkeiten des Web 2.0, insbesondere der Plattformen für soziale Netze, sollten persönliche Daten nur sparsam veröffentlichen, wenn sie ihre Privatsphäre schützen möchten.

2.5 Voice over IP im Landesverwaltungsnetz 3.0

Unter der Federführung des Landesbetriebes für Datenverarbeitung und IT-Serviceaufgaben wurde mit unserer Beteiligung eine Arbeitsgruppe eingerichtet, deren Auftrag es war, Richtlinien und Empfehlungen für das Telefonieren über das Datennetz – Voice over IP (VoIP) – zu erarbeiten.

Die Konvergenz von Sprache und Daten in einem gemeinsamen Netzwerk gewinnt in der Landesverwaltung Brandenburg zunehmend an Bedeutung.

Sicherheitsprobleme der Netztechnologie können bei der Integration der Telefonie in die Datennetze auch den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können Netzwerke durch die automatisierte Versendung von Rundrufen blockiert, Inhalte der Kommunikation mangels Verschlüsselung ausgespäht oder kostenlose Anrufe durch Erschleichung von Authentifizierungsdaten auf Kosten des Betrogenen geführt werden. Auch besteht die Gefahr, dass Viren und Trojaner ihre schädliche Wirkung entfalten und das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflussen.

Für einen datenschutzgerechten und sicheren Betrieb eines VoIP-Dienstes in der Landesverwaltung müssen folgende Bedingungen erfüllt sein:

- Uneingeschränkte und generelle Ende-zu-Ende-Verschlüsselung der Sprachdaten,
- Verschlüsselung der Signalisierungsströme,
- Eindeutige Identifizierung der Endgeräte,
- IT-Sicherheitskonzeption für die eingesetzte VoIP-Middleware,
- Logische Trennung von Sprach- und Datennetz,

[30] siehe http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

- Übergreifende Sicherheits-Policy.

Die vom Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben eingesetzten und zur Verfügung gestellten technologischen Komponenten (Cisco Call Manager, Übergaberouter – Voice Gateway, Endgeräte) unterstützen diese Maßnahmen.

Auf Grund technologischer Beschränkungen der VoIP-Nutzung sollte darauf geachtet werden, dass sich die uneingeschränkte und generelle Ende-zu-Ende-Verschlüsselung der Sprachdaten nur auf das Datennetz (Landesverwaltungsnetz und Lokation) bezieht. Bei einer Kommunikation aus dem Landesverwaltungsnetz heraus mit einem externen Teilnehmer (herkömmliche Telefonie) wird bis zum Übergabepunkt (VoIP/ISDN Gateway) verschlüsselt. Hinter dem Gateway wird das Gespräch, wie üblich, über das ISDN-Netz leitungsvermittelt übertragen. Wegen der fehlenden Interoperabilität ist derzeit keine verschlüsselte Ende-zu-Ende Kommunikation zwischen Endgeräten in unterschiedlichen Netzen möglich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Studie „VoIPSec“[31] erstellt, welche detailliert die Bedrohungen auf Netzwerk-, Middleware- und Endgeräteebene untersucht und Lösungsvorschläge anbietet.

Um Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität bei der Sprachübertragung über das Datennetz gewährleisten zu können, sind angemessene Sicherheitsmaßnahmen umzusetzen. Der Schutz des Fernmeldegeheimnisses kann nur über eine Verschlüsselung der zu übertragenen Daten garantiert werden.

2.6 Der USB-Stick – Möglichkeiten und Gefahren

Der USB-Stick avanciert auf Grund seiner geringen Ausmaße, der hohen Speicherkapazität und des niedrigen Verkaufspreises zum Massenprodukt. Mit seinem Einsatz sind jedoch auch Risiken verbunden.

USB-Sticks sind permanent verfügbare, mobile Datenträger, die auf Grund ihrer Größe in jede Hosentasche passen. Neben der herkömmlichen Form findet man z. B. Uhren, Taschenmesser und Stifte mit integrierten USB-Systemen. Arbeitgeber müssen daher immer damit rechnen, dass Beschäftigte ihren privaten USB-Stick an den Dienstrechner anschließen und somit die Sicherheit der Datenverarbeitung gefährden. Aber auch dienstlich zur Verfügung gestellte USB-Sticks sind riskant, da die Integrität und Vertraulichkeit

[31] siehe http://www.bsi.de/literat/studien/VoIP/index.htm

der darauf gespeicherten Daten nicht gewährleistet werden kann. Wie bereits in unserem letzten Tätigkeitsbericht[32] erläutert, sollte unbefugte Nutzung von USB-Schnittstellen der IT-Geräte verhindert werden.

USB-Sticks der neusten Generation erlauben es, komplette Arbeitsumgebungen auf dem Stick abzulegen und von dort zu starten. Herkömmliche Windows-Programme sind allerdings dafür nicht immer geeignet. Daher hat sich dafür eine neue Softwarekategorie gebildet, so genannte „portable applications“, „portable apps“ oder auch „Stickware“. Solche Programme sind für fast jeden Anwendungszweck erhältlich. Stickware benötigt auf dem Rechner keinerlei Installation, sondern hat alle notwendigen Dateien auf dem USB-Stick. Häufig kann so die Beschränkung der Installationsrechte eines Anwenders umgangen werden. Auf der anderen Seite kann der Nutzer eines USB-Sticks ausgespäht werden. Schließt man den USB-Stick an einen unbekannten Rechner an, erstellt dieser in einem solchen Fall automatisch eine Sicherungskopie der gespeicherten Daten, ohne dass der Nutzer dies bemerkt. Die stetige Miniaturisierung der USB-Sticks ist zwar praktisch, birgt jedoch die Gefahr des Verlustes. Hier schützt eine Verschlüsselung der personenbezogenen Daten vor einem unberechtigten Zugriff. Eine konsequente Datensicherung verhindert den Verlust der Daten.

Die enorme Verbreitung dieser Technologie und der damit verbundenen Risiken hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewogen, einen neuen Baustein[33] zu kreieren, der sich mit den Gefahren mobiler Datenträger auseinandersetzt.

USB-Sticks ermöglichen es dem Anwender, seine eigene Systemumgebung mitzuführen und unterstützen den schnellen und einfachen Datenaustausch. Für den sicheren Betrieb müssen jedoch geeignete technisch-organisatorische Maßnahmen umgesetzt werden.

2.7 Werden Funknetze sicherer?

Bereits in zurückliegenden Tätigkeitsberichten[34] sind wir auf die Gefahren und Risiken und auf die erforderlichen technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten beim Einsatz von Funknetzen eingegangen. Die rasante Entwicklung im Bereich der Funknetze setzt sich kontinuierlich fort.

[32] vgl. Tätigkeitsbericht 2004/2005, A 2.13

[33] siehe IT-Grundschutzkataloge Version 2007, Baustein 5.14 Mobile Datenträger

[34] vgl. Tätigkeitsbericht 2001, A 2.2; Tätigkeitsbericht 2003, A 2.6 und Tätigkeitsbericht 2004/2005, A 2.2

Im Januar 2006 wurde der erste Entwurf des neuen Wireless Local Area Network (WLAN)-Standards IEEE 802.11n verabschiedet. Der Entwurf sieht Datenraten bis zu 600 MBit/s vor. Im Vergleich zum aktuellen Standard IEEE 802.11g ist das mehr als das Zehnfache der Übertragungsgeschwindigkeit. Auch werden nunmehr größere Reichweiten möglich.

Ein fester Bestandteil des Standards IEEE 802.11n ist die Unterstützung von Quality of Service (QoS), womit auch im WLAN Datenströme priorisiert werden können. Das ist eine grundlegende Voraussetzung, um zeitkritische Anwendungen wie Voice over IP (VoIP) oder Video-Streams im WLAN zu betreiben. Wird VoIP in einem Funknetz eingesetzt, so sind die übertragenen Daten mit sicheren kryptographischen Verfahren zu verschlüsseln.

Die im Standard IEEE 802.11n verwendete Sicherheitstechnik Wi-Fi[35] Protected Access 2 (WPA2) mit der Verschlüsselung nach dem Advanced Encryption Standard (AES) sorgt für einen deutlich verbesserten Schutz der übertragenen Daten. Auch die Zugangsschutztechnik nach IEEE 802.1x ist im neuen Standard enthalten. Damit erhält der Anwender erst nach erfolgreicher Authentifizierung an einem Radius-Server Zugang zum drahtlosen Netzwerk. Werden von einer öffentlichen Stelle personenbezogene Daten in einem Funknetz übertragen, so ist die Verwendung dieser Mechanismen unbedingt erforderlich.

Der Standard IEEE 802.11n liegt momentan immer noch als Entwurf vor. Der aktuelle Zeitplan sieht vor, diesen bis Ende 2008 zu verabschieden. Derzeit sind schon eine Reihe von Produkten auf dem Markt verfügbar, die die Sicherheitsmechanismen des zukünftigen Standards IEEE 802.11n unterstützen. Bei der Beschaffung von WLAN-Komponenten sollte man diesen neuen Standard unbedingt berücksichtigen.

Das Bundesamt für Sicherheit in der Informationstechnik hat in einer Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“[36] aktuelle Gefährdungen und Schutzmaßnahmen umfassend beschrieben.

Werden personenbezogene Daten in drahtlosen Netzen übertragen, so sind mindestens die Maßnahmen zur Verschlüsselung und Authentifizierung des im Entwurf vorliegenden Standards IEEE 802.11n umzusetzen. Bei der Verarbeitung von sensitiven personenbezogenen Daten sind zusätzliche Maßnahmen erforderlich.

[35] Die Wi-Fi Alliance ist eine Organisation, die Produkte verschiedener Hersteller auf der Basis des Standards IEEE-802.11 zertifiziert, um die Interoperabilität der WLAN-Komponenten zu gewährleisten.

[36] siehe http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf

2.8 Realisierung eines E-Mail-Push-Dienstes mit BlackBerry

Eine öffentliche Stelle fragte bei uns an, welche technisch-organisatorischen Maßnahmen bei der Realisierung eines E-Mail-Push-Dienstes mit BlackBerry zu berücksichtigen sind.

Bei BlackBerry handelt es sich um eine Lösung zur drahtlosen Übertragung von E-Mails und Daten des Personal Information Managers (PIM). Die Daten werden zwischen dem Server und dem BlackBerry-fähigen Endgerät per General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) oder Wireless Local Area Network (WLAN) übertragen.

Der BlackBerry Enterprise Server (BES) stellt die Schnittstelle zwischen dem mobilen BlackBerry-Endgerät und dem Mail-Server dar. Die übertragenen Daten werden zwischen den BlackBerry-Endgeräten und dem Enterprise Server mittels TripleDES bzw. AES verschlüsselt. Die verwendeten kryptographischen Verfahren entsprechen dem derzeitigen Stand der Technik und sind geeignet, personenbezogene Daten mittleren Schutzbedarfs über Weitverkehrsnetze sicher zu übertragen.

Werden sensitive personenbezogene Daten übertragen, sind zusätzliche Sicherheitsmaßnahmen zu ergreifen. So kann beispielsweise durch Verwendung des optional angebotenen S/MIME-Support-Package eine Ende-zu-Ende-Verschlüsselung (durchgängige Verschlüsselung der E-Mail vom Absender bis zum Empfänger) realisiert werden. Die Implementierung setzt eine Public Key Infrastruktur (PKI) voraus. Der Nachteil einer Ende-zu-Ende-Verschlüsselung besteht darin, dass beigefügte Dateien vom BlackBerry Enterprise Server nicht mehr konvertiert werden können. Eine Ende-zu-Ende-Verschlüsselung halten wir bei sensitiven Daten für zwingend erforderlich.

Bekommt ein Angreifer ein Endgerät unter seine Kontrolle, so hat er solange Zugriff auf die Daten des Benutzers, bis der Zugang systemseitig gesperrt wird.

Die BlackBerry-Endgeräte sollten daher zentral administriert werden, um ein einheitliches Sicherheitsniveau zu erreichen. Eine zentrale Administration sollte folgende Punkte berücksichtigen:

- Passwortschutz aktivieren,
- periodische Änderung des Passwortes erzwingen,
- Anzahl der Fehlversuche bei falscher Passworteingabe begrenzen,

- personenbezogene Daten nur verschlüsselt auf dem BlackBerry-Endgerät speichern (ab Version 4.0 möglich!),
- keine Installation von Fremdsoftware,
- periodischer Schlüsselaustausch (monatlich),
- Bildschirmschoner aktivieren (Periode nicht zu groß wählen),
- sämtliche Daten auf dem Endgerät nach mehrmaliger Fehleingabe des Passwortes löschen,
- externe Schnittstellen deaktivieren,
- Service zur Verfügung stellen, sodass der Nutzer das Endgerät sperren lassen kann.

Die erforderlichen Sicherheitsmaßnahmen sollten so eingerichtet werden, dass der Benutzer keine Möglichkeit hat, diese zu umgehen.

Die Sensibilisierung der Benutzer bezüglich der datenschutzgerechten Nutzung von BlackBerry-Endgeräten spielt eine wichtige Rolle. Folgende Empfehlungen sollten daher in einer Dienstanweisung berücksichtigt werden:

- der Benutzer darf das Gerät nicht aus der Hand geben,
- der Benutzer darf das Passwort nicht weitergeben,
- Verlust des Gerätes sollte umgehend gemeldet werden und
- personenbezogene Daten dürfen nur verschlüsselt gespeichert werden.

Auf Grund der hohen Missbrauchsmöglichkeiten bei der Übertragung von personenbezogenen Daten mittels E-Mail-Push-Diensten sind technisch-organisatorische Maßnahmen zu realisieren, die das Risiko auf ein Minimum reduzieren. Eine durchgängige Ende-zu-Ende-Verschlüsselung ist unabdingbar.

2.9 Intrusion-Detection-Systeme (Angriffserkennungssysteme)

Sichere Informationssysteme bilden die Voraussetzung für eine funktionierende Kommunikationsinfrastruktur. Die Installation von Firewall-Systemen und Virenscannern gehören zum Stand der Technik und wer-

den zum Schutz der lokalen Netze bereits seit längerem eingesetzt. In letzter Zeit gewinnen Intrusion-Detection-Systeme (IDS) immer mehr an Bedeutung. Mit diesen Systemen können u. a. Angriffsversuche erkannt und entsprechende Gegenmaßnahmen zeitnah eingeleitet werden.

Intrusion-Detection-Systeme filtern bestimmte Ereignisse, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten. Die Ereignisse werden dann genauer untersucht und entsprechende Gegenmaßnahmen ergriffen. So können beispielsweise beim Zugriffsversuch eines unberechtigten Nutzers auf einen Server im lokalen Netz die Aktivitäten ausgewertet und protokolliert werden. Bei besonders sicherheitsrelevanten Ereignissen kann auch eine Alarmierung in Echtzeit erfolgen.

Prinzipiell unterscheidet man netzbasierte IDS (NIDS) und hostbasierte IDS (HIDS). Bei netzbasierten IDS wird der Netzverkehr eines Rechners oder eines gesamten Teilnetzes auf verdächtige Datenpakete hin untersucht. So können netzbasierte Angriffe rechtzeitig erkannt und entsprechende Gegenmaßnahmen eingeleitet werden. Komplexe lokale Netze bestehen aus sog. Teilnetzen. Bei netzbasierten IDS besteht das Problem, dass aufgrund der Segmentierung und der damit verbundenen logischen Trennung der Netze nicht alle Datenpakete vom netzbasierten IDS erfasst werden können. Es gibt jedoch die Möglichkeit, in jedem Teilnetz sog. Netzsensoren (auch Netzagenten) zu installieren, die die gesammelten Datenpakete an das netzbasierte IDS zur Auswertung weiterleiten. Nicht zu vernachlässigen ist in diesem Fall der erhöhte Datenverkehr im Netz. Aus Verfügbarkeits- und Vertraulichkeitsgründen sollten daher Netzsensoren und netzbasierte IDS über ein separates Teilnetz (Administrationsnetz) miteinander kommunizieren.

Hostbasierte IDS können Angriffe auf Betriebssystem- und Anwendungsebene erkennen. Darunter fallen fehlgeschlagene Anmeldeversuche, Zugriffsverletzungen oder unzulässige Änderungen an Konfigurationsdateien. Auch die vom Betriebssystem erzeugten Protokolldateien können von einem hostbasierten IDS ausgewertet werden. Hostbasierte IDS müssen auf jedem zu überwachenden Host installiert werden.

Die vom jeweiligen IDS als kritisch eingeschätzten Ereignisse sollten in einem zentralen Managementsystem ausgewertet und revisionssicher protokolliert werden. Da beim Betrieb von IDS auch personenbezogene bzw. personenbeziehbare Daten, beispielsweise in Form von nutzerbezogenen IP-Adressen anfallen können, ist in jedem Fall eine Dienstvereinbarung mit dem Personalrat abzuschließen. Es ist dabei festzuschreiben, welche Daten konkret protokolliert werden, wer die Protokolldateien wann auswertet und bis zu welchem Zeitpunkt die Protokolldateien zu löschen sind.

Weiterhin ist zu berücksichtigen, dass gem. § 29 Abs. 4 Brandenburgisches Datenschutzgesetz (BbgDSG) die Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 BbgDSG gespeichert werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden dürfen.

Das Bundesamt für Sicherheit in der Informationstechnik hat in einem „Leitfaden zur Einführung von Intrusion-Detection-Systemen“[37] die technischen und rechtlichen Voraussetzungen ausführlich beschrieben. Auch die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation hat sich auf ihrer 34. Sitzung am 2./3. September 2003 in Berlin mit Intrusion-Detection-Systemen[38] beschäftigt.

Intrusion-Dection-Systeme können Sicherheitsverletzungen zeitnah erkennen und sind daher geeignet, die IT-Sicherheit in vernetzten Systemen zu erhöhen. Da u. U. auch personenbezogene Daten der Beschäftigten verarbeitet werden, ist der Personalrat rechtzeitig einzubeziehen.

2.10 Phishing-Attacken

Seit einiger Zeit versuchen Angreifer, die Passwörter von Nutzern auszuspähen. Nur wer die Risiken kennt, kann diese durch bewusstes Handeln auf ein Minimum reduzieren.

Das Wort „Phishing“ setzt sich aus den Wörtern „password“ und „fishing“ zusammen und bedeutet soviel wie „Angeln von Passwörtern“. Insbesondere Online-Banking-Nutzer werden immer häufiger Opfer von sog. Phishing-Attacken. Der Angreifer versendet E-Mails und versucht den Empfänger zu verleiten, vertrauliche Informationen wie z. B. Passwörter oder andere Zugangsdaten auf einer in der E-Mail verlinkten Website preiszugeben. Phishing-Mails tarnen sich z. B. als Sicherheitsmeldungen, Security-Updates und Sicherheitschecks. Bekommt man eine E-Mail von seiner Bank, in der die Preisgabe von Zugangsdaten aus angeblich „technischen Gründen“ erforderlich sei, so sollte man diese E-Mail ignorieren und die Bank über den Sachverhalt umgehend informieren. Man kann grundsätzlich davon ausgehen, dass solche E-Mails nicht von der Bank, sondern von einem Betrüger versandt wurden.

Zur Erhöhung der Sicherheit beim Online-Banking und zur Verhinderung von Phishing-Attacken sind sichere Verfahren wie iTAN oder HBCI zu verwenden.

---

[37] siehe http://www.bsi.bund.de/literat/studien/ids02/index.htm

[38] siehe http://www.lda.brandenburg.de → Infos zum Datenschutz → Zusammenarbeit der Datenschutzbeauftragten → Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation

Beim iTAN-Verfahren gibt die Bank mit einer Nummer vor, welche TAN einzugeben ist. Das Homebanking Computer Interface (HBCI) ist ein offener Standard für den Bereich Electronic Banking. Zur Teilnahme am HBCI-Verfahren benötigt der Nutzer eine HBCI-Chipkarte der Bank sowie einen Chipkartenleser, der die sichere PIN-Eingabe unterstützt. Das HBCI-Verfahren ist momentan das sicherste Verfahren, um der Bank Aufträge zu erteilen. So werden z. B. Kontostandsabfragen oder Überweisungen mit dem auf der Chipkarte befindlichen privaten Schlüssel signiert und zur Bank übertragen. Der private Schlüssel wird vom Nutzer durch die Eingabe einer PIN für die Verwendung frei geschaltet. Der Vorteil besteht u. a. darin, dass der private Schlüssel die Chipkarte nie verlässt und ein Angreifer daher nicht in seinen Besitz kommen kann.

Mit relativ einfachen Anti-Phishing-Regeln können Internet-Nutzer die Risiken weitest gehend minimieren:

- keine Bekanntgabe von vertraulichen Daten (Login-Daten, Passwörtern) per E-Mail,
- die Login-Adresse einer WebSite unter „Favoriten“ des Webbrowsers speichern und bei jedem Login überprüfen,
- für die Übertragung vertraulicher Daten ausschließlich SSL-verschlüsselte Seiten akzeptieren,
- Sicherheitsupdates des verwendeten Betriebssystems und des Browsers regelmäßig installieren,
- im E-Mail-Programm die HTML-Funktion deaktivieren (es sollte nur reiner Text angezeigt werden),
- Firewalls einsetzen und Virensuchprogramme ständig aktualisieren.

Beim Online-Banking sollten zusätzlich folgende Maßnahmen berücksichtigt werden:

- niemals PINs und TANs auf dem Computer speichern,
- nur sichere Verfahren wie iTAN oder HBCI nutzen,
- grundsätzlich nur den eigenen Rechner verwenden (z. B. kein Online-Banking im Internet-Café),
- in regelmäßigen Abständen das Sicherheitszertifikat der Bank überprüfen.

Das Risiko der Ausspähung von Passwörtern durch Kriminelle lässt sich durch gesundes Misstrauen und sicherheitsbewusstes Verhalten bei der Nutzung der Dienste des Internets auf ein Minimum reduzieren.

2.11 Datenschutz-Baustein in den IT-Grundschutzkatalogen

Die IT-Grundschutz-Kataloge[39] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verfügen ab der Version 2007 über einen speziellen Baustein zum Datenschutz. Dieser ist gemäß der Vorgehensweise nach BSI-Standard 100-2 ergänzend anzuwenden und ermöglicht die gezielte Untersuchung des zu betrachtenden IT-Verbundes aus Sicht des Datenschutzes.

Um der Bedeutung des Datenschutzes in den Grundschutzkatalogen ausreichend gerecht zu werden, wurden vom Arbeitskreis „Technische und organisatorische Fragen des Datenschutzes“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Vorschläge für den Entwurf eines speziellen Bausteins „Datenschutz“ erarbeitet. Die BSI-Standards wurden ebenfalls um wichtige Aspekte des Datenschutzes ergänzt. Nach Abstimmung mit den Datenschutzaufsichtsbehörden der Länder für den nicht öffentlichen Bereich und dem BSI liegen nun jeweils abschließende Versionen vor.

Die Struktur des Bausteins folgt der in den Katalogen verwendeten Systematik. Er beschreibt zur Sensibilisierung und Motivation einleitend das Anliegen des Datenschutzes, angefangen von den rechtlichen Rahmenbedingungen über die technischen und organisatorischen Maßnahmen bis hin zu den Rechten der Betroffenen. Insbesondere die Erläuterung der Zuständigkeiten der Aufsichtsbehörden unterstützt die Etablierung eines für den Datenschutz geeigneten Managementprozesses. In Anlehnung an die übrigen Bausteine folgt eine Übersicht der datenschutzrechtlich relevanten Gefährdungen (neuer Gefährdungskatalog G 6) und der zugehörigen Maßnahmen (neuer Maßnahmenkatalog M 7).

Der Datenschutz-Baustein richtet sich an die privaten und öffentlichen Anwender der IT-Grundschutz-Kataloge in Deutschland. Da dieser auf der deutschen Gesetzgebung basiert, kann er außerhalb der Bundesrepublik nur sinngemäß angewendet werden und wurde daher auch nicht fester Bestandteil der IT-Grundschutz-Kataloge, die auch international Anwendung finden. Sie verweisen lediglich auf den Baustein „Datenschutz“[40].

[39] alte Bezeichnung: IT-Grundschutzhandbuch

[40] siehe http://www.bsi.bund.de/gshb/baustein-datenschutz/index.htm

In Zusammenarbeit mit dem BSI wurden ebenfalls die BSI-Standards überarbeitet und um Datenschutzaspekte ergänzt. Der BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“ wird um folgende Themenbereiche erweitert:

- Datenschutz als Teil der Management-Prinzipien,
- Beteiligung des Datenschutzbeauftragten und
- Mitarbeiterschulung zum Datenschutz.

Im Standard 100-2 „IT-Grundschutz-Vorgehensweise“ wurde im Schutzstufenkonzept der Schutzbedarf unter Berücksichtigung des Datenschutzes konkretisiert. Besondere Bedeutung bekam hier der Datenschutzbeauftragte als Organisationseinheit und seine Anbindung als Stabsstelle bei der Behörden- bzw. Unternehmensleitung. Weiterhin wird der Standard ergänzt um die Aspekte:

- Aufgabenbeschreibung des Datenschutzbeauftragten,
- Datenschutzkontrolle als begleitende Aufgabe der Revision und
- datenschutzgerechte Dokumentation.

Das vom BSI vertriebene Software-Tool „GSTOOL“, mit dessen Hilfe IT-Sicherheitskonzepte auf der Basis von IT-Grundschutz erstellt und fortgeschrieben werden können, wird den Datenschutz-Baustein im nächsten Update beinhalten.

Durch den neuen Datenschutz-Baustein werden die Belange des Datenschutzes in den IT-Grundschutz-Katalogen besser als bisher berücksichtigt. Bei der Umsetzung der darin beschriebenen Maßnahmen müssen die datenschutzrechtlichen Regelungen der Länder beachtet werden.

3 Medien und Telekommunikation

3.1 Telemediengesetz

Am 1. März 2007 ist das neue Telemediengesetz in Kraft getreten[41]. In diesem Bundesgesetz wurden die Bestimmungen für alle Multimediadienste zu einem einheitlichen rechtlichen Rahmen zusammengefasst. Die bisher so

[41] Art. 1 des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetzes vom 26. Februar 2007 (BGBl. I S. 179)

komplizierte Abgrenzung zwischen Mediendiensten und Telediensten entfällt, da durch den Neunten Rundfunkänderungsstaatsvertrag[42] auch der Mediendienste-Staatsvertrag aufgehoben wurde und der Rundfunkstaatsvertrag unter dem Titel „Staatsvertrag für Rundfunk und Telemedien“ die Vorschriften des Telemediengesetzes für anwendbar erklärt. Damit sind die bisher in getrennten Gesetzen zu findenden Datenschutzregelungen nunmehr in einem Gesetz vereint.

Erfreulich ist, dass das hohe Datenschutzniveau im Bereich der Multimediadienste insgesamt beibehalten wurde. Auch künftig dürfen die Diensteanbieter nur solche Daten verarbeiten, die für die Erbringung des jeweiligen Dienstes erforderlich sind. Die Daten unterliegen zudem einer strengen Zweckbindung. Diese kann nur für bestimmte Zwecke, z. B. der öffentlichen Sicherheit oder der Verfolgung von Verstößen gegen das Urheberrecht, durchbrochen werden. Für die öffentlichen Stellen des Landes bedeutet dies, dass sie insbesondere bei der Bereitstellung von Internet-Angeboten die datenschutzrechtlichen Bestimmungen des Telemediengesetzes beachten müssen. Dazu gehört, dass beispielsweise eine Speicherung von IP-Adressen der auf ein Internet-Angebot einer Behörde zugreifenden Nutzer auf dem Webserver der Behörde grundsätzlich nicht zulässig ist.[43]

3.2 Mehr Datenschutz bei der Befreiung von der Rundfunkgebühr

Nachdem wir im letzten Tätigkeitsbericht die erheblichen datenschutzrechtlichen Defizite des Verfahrens der Rundfunkgebührenbefreiung kritisiert haben, konnten nun einige Fortschritte erreicht werden.

Zahlreiche Beschwerden richten sich gegen die Aufforderung, die vollständigen Sozialleistungsbescheide im Original oder in beglaubigter Kopie der Gebühreneinzugszentrale (GEZ) für die Prüfung der Befreiung von der Rundfunkgebührenpflicht vorlegen zu müssen. Um die damit verbundene massenhafte Erhebung von nicht erforderlichen Daten zu verhindern, haben wir mit dem Rundfunk Berlin-Brandenburg (RBB) und der GEZ vereinbart, dass Bescheinigungen des Sozialleistungsträgers, die bestätigen, dass die Voraussetzungen für eine Befreiung von der Rundfunkgebührenpflicht vorliegen, als ausreichend akzeptiert werden. Der vollständige Sozialleistungsbescheid, der darüber hinaus viele weitere für die Arbeit der GEZ nicht erforderliche Angaben enthält, muss dann nicht mehr eingereicht werden. Wir haben hierzu mit dem RBB und der GEZ abgestimmte Musterformulare entwickelt,

[42] in Brandenburg ratifiziert durch Gesetz vom 8. Januar 2007 (GVBl. I S. 26)

[43] Urteil des Landgerichts Berlin vom 6. September 2007, Az. 23 S 3/07, veröffentlicht unter http://www.daten-speicherung.de/data/Urteil_IP-Speicherung_2007-09-06.pdf

die in unserem Internetangebot zu finden sind[44] und von uns auf Wunsch auch verschickt werden.

Um diese datenschutzfreundliche Lösung auch gesetzlich zu verankern, hat eine gemeinsame Arbeitsgruppe aus Vertretern der Staats- und Senatskanzleien der Länder, der Datenschutzbeauftragten der Länder und der Rundfunkanstalten eine neue Formulierung für die einschlägige Vorschrift (§ 6 Abs. 2 des Rundfunkgebührenstaatsvertrages) entworfen. Diese Neufassung ist als Bestandteil des 10. Rundfunkänderungsstaatsvertrages von den Ministerpräsidenten im Dezember 2007 unterschrieben worden und soll am 1. September 2008 nach der Zustimmung durch die Landesparlamente in Kraft treten.

Für die Zukunft arbeiten Rundfunkanstalten und GEZ darüber hinaus an einer Lösung, bei der die für die Befreiung erforderlichen Daten direkt auf elektronischem Wege an die GEZ übermittelt werden können. Hierfür sind aber noch zahlreiche rechtliche, technische und organisatorische Hürden zu nehmen.

Die Sozialleistungsträger sind aufgefordert, Betroffenen eine Bescheinigung zur Vorlage bei der GEZ auszuhändigen, um damit ein datenschutzfreundlicheres Verfahren bei der Befreiung von der Rundfunkgebühr auf breiter Ebene zu unterstützen.

4 Videoüberwachung

4.1 Kameraattrappen − Eingriff in das Persönlichkeitsrecht?

Häufig erwägen öffentliche Stellen, Videokameras einzusetzen, um ihre Einrichtungen gegen Sachbeschädigung zu schützen und die Sicherheit ihrer Mitarbeiter zu erhöhen. Angesichts der damit verbundenen Kosten entscheiden sich einige für den Einsatz von Attrappen anstatt echter Kameras. Sie hoffen, dass diese allein durch den Abschreckungseffekt die gewünschten Ziele einer Überwachung erreichen.

Beim Einsatz von Attrappen findet objektiv gesehen keine Verarbeitung personenbezogener Daten und damit auch kein Eingriff in das Recht auf informationelle Selbstbestimmung statt. Insofern findet das Datenschutzrecht keine Anwendung. Auf der anderen Seite wird eine für echt gehaltene Attrappe von den betroffenen Bürgern ebenso als Eingriff empfunden wie eine tatsächlich funktionierende Kamera.

[44] siehe http://www.lda.brandenburg.de → Infos zum Datenschutz → Rundfunk

Hier wird ein Grundrechtseingriff vorgetäuscht, der in Wirklichkeit gar nicht stattfindet. In den uns bekannt gewordenen Fällen wurde diese Täuschung zusätzlich noch durch den unwahren Hinweis „Das Gebäude wird videoüberwacht“ unterstrichen. Das stellt eine Umkehrung des Transparenzgebots dar, das jedes hoheitliche Handeln bestimmen sollte: Das Brandenburgische Datenschutzgesetz fordert bei einer Videoüberwachung die Unterrichtung der Betroffenen, um diese über die Einschränkung ihres Rechts auf informationelle Selbstbestimmung zu informieren. Staatliche Stellen dürfen diese Vorschrift nicht für Täuschungen missbrauchen.

Im Übrigen halten wir es auch praktisch für unrealistisch, dass der Umstand, dass es sich nur um Attrappen handelt, besonders lange geheim bleibt. Spätestens dann, wenn ein „Betroffener“ von seinem Auskunftsrecht Gebrauch machen will, wird er von der Täuschung erfahren.

Der Einsatz von Kamera-Attrappen unterliegt zwar nicht den Bestimmungen des Datenschutzrechts. Es widerspricht jedoch den rechtsstaatlichen Vorstellungen, wenn Träger hoheitlicher Gewalt Eingriffe vortäuschen, die nicht stattfinden und damit letztlich die Bürger in die Irre führen. Wir empfehlen daher, von solchen Vorhaben generell Abstand zu nehmen und die Voraussetzungen für eine echte Videoüberwachung auf der Grundlage des Brandenburgischen Datenschutzgesetzes sorgfältig zu prüfen.

4.2 Zu viel Videoüberwachung im Maßregelvollzug?

Die Beschwerde eines im Maßregelvollzug Untergebrachten über den Umfang der Videoüberwachung im Freihof war für uns Anlass zu einem Besuch der betroffenen Klinik.

Aus Sicherheitsgründen werden bereits Bereiche vor dem Eingang zum Maßregelvollzug von Videokameras überwacht. Hinweisschilder hierzu wurden nach Mitteilung der Klinik aufgrund unserer Empfehlung inzwischen angebracht.

In Gebieten außerhalb des ummauerten Maßregelvollzugs werden Aufnahmen nur im Falle eines Alarms und somit sehr selten getätigt. Die zur Verfügung stehende Aufnahmekapazität von zwölf Stunden reichte aus, dass wir bei unserer Kontrolle noch Aufnahmen vorfanden, die länger als drei Jahre zurücklagen. So konnten Bilder bisher mehr als drei Jahre lang gespeichert werden. Diese Speicherdauer erschien nicht nur uns, sondern auch dem für die Aufsicht über den Maßregelvollzug zuständigen Landesamt für Soziales und Versorgung viel zu lang, sodass die Behörde aufgrund unserer Anregung auf eine deutliche Verkürzung der Aufzeichnungsdauer hinwirkte.

Neben der Einfahrtüberwachung durch eine schwenkbare Kamera findet eine Videoüberwachung im Freihof des Maßregelvollzuges vor allem entlang der Ummauerung statt. Aus therapeutischen Gründen wird aber zugleich versucht, den Patienten auch ein Freigelände ohne Videoüberwachung zur Verfügung zu stellen. Der Petent fühlte sich durch die schwenkbare Kamera besonders beeinträchtigt. Das Landesamt für Soziales und Versorgung hat sich nach Prüfung der Angelegenheit und eingehender Abwägung auch der therapeutischen Aspekte dafür ausgesprochen, den Schwenkbereich der Kamera im Freihof aus Sicherheitsgründen unverändert zu lassen, was wir für datenschutzrechtlich akzeptabel halten.

Müssen wie im Maßregelvollzug therapeutische Aspekte und Sicherheitsbelange beachtet werden, bedarf der Einsatz von Videokameras einer sorgfältigen Abwägung. Speicherfristen für Videoaufnahmen sind auf die erforderliche Dauer zu beschränken.

4.3 Datenschutzgerechter Einsatz von Webcams

Immer mehr öffentliche Stellen – vor allem Gemeinden – veröffentlichen im Rahmen ihrer Internet-Auftritte Bilder, die von Webcams aufgenommen werden. Die Kameras sind dabei an Orten installiert, bei denen die Betreiber der Kamera ein bestimmtes Publikumsinteresse voraussetzen: So sind Bilder von Marktplätzen, interessanten Baustellen, verkehrsreichen Kreuzungen, aber auch schon mal die eines städtischen Zoos im Internet zu sehen.

Angesichts der stetigen technischen Verbesserungen und der immer höheren Übertragungskapazitäten im Internet können Webcams inzwischen eine recht hohe Auflösung erreichen, sodass immer häufiger einzelne Personen, Kraftfahrzeuge oder andere personenbezogene Details identifiziert werden können. Außerdem ist insbesondere bei Dunkelheit nachvollziehbar, wann und wie lange sich jemand in abgebildeten Wohnhäusern aufhält.

Die Beobachtung mit der Kamera ist als Videoüberwachung im Sinne des Brandenburgischen Datenschutzgesetzes (BbgDSG) zu qualifizieren. Die Vorschrift (§ 33c BbgDSG) gilt für alle optisch-elektronischen Einrichtungen unabhängig von der eingesetzten Technologie, sodass nicht nur „klassische“ Videokameras, sondern auch Webcams unter diese Vorschrift fallen.

Die Videoüberwachung ist öffentlichen Stellen nur erlaubt, wenn es sich um öffentlich zugängliche Räume handelt und die Überwachung zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung des Hausrechts erforderlich ist.

Schon die erste Voraussetzung liegt in vielen Fällen nicht vor. Werden z. B. Marktplätze oder Straßenkreuzungen abgebildet, handelt es sich um öffentliches Straßenland. Ein öffentlich zugänglicher Raum muss nicht zwingend innerhalb eines Gebäudes liegen. Es muss sich bei ihm zumindest um eine abgrenzbare Fläche handeln, an der der öffentlichen Stelle ein Hausrecht zusteht. Dazu können auch Freiflächen städtischer Einrichtungen, Sportplätze oder ein Zoo gehören, nicht aber das öffentliche Straßenland. Eine Videoüberwachung ist hier nur der Polizei unter den strengen Voraussetzungen des Brandenburgischen Polizeigesetzes erlaubt. Aber auch in Fällen, in denen öffentlich zugängliche Räume betroffen sind, ist zu bezweifeln, dass die beiden weiteren Voraussetzungen für eine rechtmäßige Videoüberwachung vorliegen: Die Installation einer Webcam dürfte die Wahrung des Hausrechts in keiner Weise unterstützen. Es ist auch keine Aufgabe einer öffentlichen Stelle denkbar, die eine personenbezogene Veröffentlichung der Daten in dieser Weise erfordern würde.

Sobald auf den Bildern einzelne Personen identifizierbar sind, ist darüber hinaus das durch das Kunsturhebergesetz geschützte Recht am eigenen Bild betroffen. Dieses lässt eine Veröffentlichung von Bildern ohne Einwilligung der abgebildeten Personen nur in bestimmten Ausnahmefällen zu.

Beim Einsatz von Webcams sind Vorkehrungen zu treffen, die eine Veröffentlichung personenbezogener Bilder ausschließen. Dies könnte beispielsweise durch eine geringe Auflösung oder eine geschickte Wahl der Kameraposition erreicht werden. Ist dies nicht möglich, muss eine Veröffentlichung von Bildern im Internet unterbleiben. Grobe Überblicksaufnahmen, auf denen weder Personen noch personenbeziehbare Vorgänge (z. B. die Nutzung abgebildeter Wohnungen) erkennbar sind, sind dagegen ohne weiteres zulässig.

4.4 Bild- und Tonaufzeichnungen in Sitzungen kommunaler Vertretungen

Viele Gemeindevertretungen, Stadtverordnetenversammlungen und Kreistage sind unsicher, unter welchen Voraussetzungen und in welchem Umfang sie in ihren Sitzungen Bild- und Tonaufzeichnungen zulassen dürfen. Die Palette reicht dabei von der Tonaufzeichnung für die Anfertigung des Sitzungsprotokolls über Aufnahmen durch die Medien bis zu Aufzeichnungen durch Teilnehmer selbst.

Während nach geltendem Recht für jede Bild- und Tonaufzeichnung die Zustimmung aller anwesenden Vertreter eingeholt werden muss, enthält die

neue Kommunalverfassung abgestufte Regelungen zum Umgang mit solchen Aufzeichnungen.[45]

Tonaufzeichnungen zur Erleichterung der Niederschrift bedürfen in Zukunft keiner Zustimmung der Vertreter und sind daher ohne weiteres erlaubt. Die Aufzeichnungen müssen nach der darauf folgenden Sitzung gelöscht werden.

Wollen Vertreter von Presse, Rundfunk oder anderen Medien oder die Gemeindevertretung selbst in der öffentlichen Sitzung Bild- oder Tonaufnahmen anfertigen, kann zukünftig in der Geschäftsordnung geregelt werden, unter welchen Bedingungen dies zulässig ist. Die Gemeindevertretung ist dabei im Rahmen der Selbstverwaltung frei, zu entscheiden, ob ein einstimmiges oder mehrheitliches Votum der Vertreter eingeholt werden muss oder ob Aufnahmen generell erlaubt sein sollen. Deshalb kann es – im Gegensatz zur bisherigen Rechtslage – auch vorkommen, dass Aufzeichnungen durch Journalisten oder die Vertretung selbst auch dann zulässig sind, wenn einzelne Vertreter damit nicht einverstanden sind. Das Gleiche gilt für Ton- und Bildübertragungen, sodass beispielsweise auch die Übertragung von Sitzungen per Webcam im Internet in der Geschäftsordnung geregelt werden kann.

Für alle anderen Bild- und Tonaufzeichnungen bzw. -übertragungen bleibt es bei der geltender Rechtslage: Wollen beispielsweise anwesende Zuhörer eine öffentlichen Sitzung aufzeichnen, bedarf dies auch in Zukunft der Zustimmung aller anwesenden Vertreter, d. h. es darf keine Gegenstimmen oder Enthaltungen geben. Diese Regelungen gelten auch für die Ausschüsse, sodass selbst sachkundige Einwohner, die in diesem Gremium mitwirken, einer Aufzeichnung oder Übertragung zustimmen müssen.

Werden im Rahmen der Einwohnerfragestunde Äußerungen der anwesenden Einwohner aufgezeichnet oder übertragen, sind diese in angemessener Form über die Aufzeichnung zu informieren. Ein Recht, Aufzeichnungen oder Übertragungen zu unterbinden, haben die Einwohner hingegen nicht. Wer mit der Aufzeichnung oder Übertragung nicht einverstanden ist, hat deshalb lediglich die Möglichkeit, seine Fragen schriftlich einzureichen.

Die neue Kommunalverfassung enthält sinnvoll abgestufte und eindeutige Regelungen für die Aufzeichnung und Übertragung von Sitzungen in Bild und Ton. Damit hat der Gesetzgeber einen angemessenen Ausgleich zwischen den Persönlichkeitsrechten der Vertreter und dem öffentlichen Interesse an der Transparenz demokratischer Entscheidungsprozesse hergestellt.

[45] Gesetz zur Reform der Kommunalverfassung und zur Einführung der Direktwahl der Landräte sowie zur Änderung sonstiger kommunalrechtlicher Vorschriften (Kommunalrechtsreformgesetz – KommRRefG) vom 18. Dezember 2007 (GVBl. I, S. 286)

4.5 Videoüberwachung am Gebäude der Industrie- und Handelskammer

Durch einen Petenten wurden wir darauf aufmerksam gemacht, dass die am Gebäude der Industrie- und Handelskammer in Potsdam zum Objektschutz montierten Videokameras nicht nur das Gebäude selbst im Blickfeld hätten, sondern auch den Bereich der davor verlaufenden Strasse erfassen würden.

Die von uns durchgeführte Kontrolle ergab, dass eine Kamera an der Vorderfront des Gebäudes nicht nur dieses, sondern auch die davor verlaufende Strasse in beiden Fahrtrichtungen sowie den Geh- und Radweg vor der Industrie- und Handelskammer erfasste. Hierbei waren Personen und Fahrzeuge deutlich zu erkennen. Zwei weitere Kameras an der Rückseite des Gebäudes filmten den Gehweg vor dem Haus sowie die gesamte Breite der dort verlaufenden Straße personenscharf. Sogar die amtlichen Kennzeichen der parkenden Fahrzeuge waren deutlich erkennbar.

§ 33c Brandenburgisches Datenschutzgesetz (BbgDSG) erlaubt zwar die Videoüberwachung öffentlich zugänglicher Räume. Bei einem Raum handelt es sich um einen abgrenzbaren Bereich, an dem die jeweilige öffentliche Stelle – demnach auch die Industrie- und Handelskammer – ein Hausrecht hat. Nicht dazu gehören öffentliche Wege und Plätze. An diesen ist eine Videoüberwachung nur durch die Polizei unter den im Brandenburgischen Polizeigesetz geregelten Voraussetzungen zulässig. Zur Wahrung des Hausrechts ist eine Überwachung der Außenfassade nach § 33c BbgDSG somit ohne weiteres zulässig. Von der Rechtssprechung wird es aber allgemein für zulässig gehalten, einen Streifen von etwa 50 cm Abstand von der Außenwand mit zu überwachen. Dies ist ausreichend, um bei potenziellen Tätern den gewünschten Abschreckungseffekt zu erreichen.

Technisch war die Anlage der Industrie- und Handelskammer Potsdam so eingerichtet, dass die Bildinformationen aller Kameras im Raum des Haustechnikers aufliefen und auf einem gesonderten Rechner verarbeitet wurden. Dieser Rechner speicherte das gesamte Datenaufkommen auf einer Festplatte. Unsere stichprobenartige Überprüfung ergab, dass eine Speicherung der Aufzeichnung von 62 anstatt der zulässigen 48 Stunden erfolgte.

Außerdem haben wir festgestellt, dass an der Einfahrt zur Tiefgarage ein Hinweisschild auf die Videoüberwachung fehlte.

Auf Grund unserer Hinweise hat die Industrie- und Handelskammer die Kameras an den Außenseiten des Gebäudes neu justiert und an der Einfahrt zur Tiefgarage ein Hinweis auf die Videoüberwachung angebracht. Auch das

Abspeichern der Videoaufnahmen wurde umorganisiert, sodass die Aufnahmen nur noch 48 Stunden vorgehalten werden. Eine Dienstanweisung regelt jetzt den Zugriff auf die gespeicherten Aufnahmen. Danach hat nur noch ein eng begrenzter Mitarbeiterkreis einen kennwortgeschützen Zugriff auf die Videoaufzeichnungen.

Inhaber des Hausrechts öffentlicher Gebäude können zum Objektschutz Videoüberwachungsanlagen installieren. Auf die Videoüberwachung ist hinzuweisen und Aufnahmen sind nur zweckgebunden zu verwenden. Eine Überwachung öffentlicher Straßen und Wege ist nicht zulässig, sie bleibt der Polizei vorbehalten.

4.6 Videoüberwachung einer Gesamtschule

Nachdem wir nach der Videoüberwachung einer Gesamtschule fragten, informierte uns die zuständige Gemeinde nur sehr zögerlich, zumeist unvollständig und teilweise sogar fehlerhaft zur Überwachungsanlage. Bei einer Kontrolle vor Ort stellten wir zudem technische und organisatorische Mängel fest.

Zunächst erkundigte sich die Gemeinde bei uns nach der Zulässigkeit einer Videoüberwachung innerhalb des Schulgebäudes, um Sachbeschädigungen zu verhindern. Wir teilten ihr daraufhin mit, dass eine solche Maßnahme nur mit Einwilligung aller Schüler und Betroffenen statthaft ist. Hingegen ist eine Videoüberwachung außerhalb des Schulgebäudes zum Objektschutz möglich, sofern dabei öffentlich zugängliche Straßen und Wege ausgespart bleiben und die Überwachung nur in der unterrichtsfreien Zeit erfolgt. Ferner ist sicherzustellen, dass der Publikumsverkehr zur anliegenden Sporthalle überwachungsfrei bleibt.

Nachdem die Presse im August 2006 schließlich über die Videoüberwachungsanlage berichtete, baten wir um eine nähere Erläuterung des Projekts. Die Gemeinde teilte uns lediglich mit, dass sie die Überwachung durchführe, um eine Beschädigung des Schulgebäudes zu vermeiden.

Wegen ungeklärter Zuständigkeiten sowie des fehlenden Informationsflusses zwischen den Beteiligten auf Seiten der Gemeinde gelang die Kontrolle der Anlage vor Ort erst im Dezember 2006 nach mehreren Anläufen: Die Überwachungsanlage bestand aus drei Kameras und einer digitalen Videozentrale im Technik-Raum der Schule. Die Kameras waren so eingestellt, dass sie einen bestimmten Bereich der Fassade und der Umgebung erfassten. Die an der Vorderseite des Schulgebäudes installierte Kamera nahm unzulässigerweise den Gehweg der angrenzenden Straße auf. Die Bilder wurden auf einer Festplatte aufgezeichnet. Die digitale Videozentrale wurde mittels einer

Eingabeeinheit konfiguriert, die – um Manipulationen zu verhindern – demontiert und verschlossen aufbewahrt wurde. Der Zugriff auf die digitale Videozentrale und damit auf die Festplatte mit den gespeicherten Aufzeichnungen, erfolgte über einen externen Netzzugriff mittels eines Tools zur Fernadministration. Wir bemängelten, dass keine restriktive Vergabe von Zugriffsrechten möglich war. Daher kann nicht ausgeschlossen werden, dass unberechtigte Personen aufgezeichnete Daten exportieren können. Darüber hinaus hatte das lokale Netz weitere technische Schwachstellen, die unberechtigte Zugriffe befürchten ließen: Das Videoüberwachungssystem der Schule wurde durch den Systemadministrator der Gemeinde fernadministriert. Um dieses Verfahren angemessen abzusichern, wäre eine detaillierte Risikoanalyse erforderlich gewesen. Auch der Rechner des Hausmeisters hätte dieser unterworfen sein müssen, da auf ihm ebenfalls ein Administrationstool installiert war. Wir haben deshalb angeregt, die digitale Videozentrale vom Netz zu nehmen und mit einem gesonderten Rechner zu koppeln. Zudem schien es fraglich, ob die Anlage angesichts der schlechten Qualität der Nachtaufnahmen überhaupt geeignet war, das Ziel der Videoüberwachung zu erreichen. Trotz gegenteiliger Zusage waren zum Zeitpunkt der Kontrolle sämtliche Bilddaten der zurückliegenden drei Wochen gespeichert. Aus der erst später nachgereichten Dienstanweisung ergab sich, dass weder konkrete Nutzungszeiten der Anlage noch weitere Maßnahmen zum Schutz der Persönlichkeitsrechte von Schülern, Lehrern und Gästen geregelt waren.

Wir forderten die Gemeinde angesichts dieser Mängel auf, die Videoüberwachungsanlage abzuschalten. Vor ihrer erneuten Inbetriebnahme sollten die technischen und organisatorischen Mängel beseitigt und die rechtlichen Voraussetzungen erfüllt sein. Im Januar 2007 teilten wir der Gemeinde das Ergebnis unserer Kontrolle mit.

Zunächst reagierte die Gemeinde nicht. Erst einen Monat nach unserer Erinnerung vom März 2007 teilte sie mit, dass die Videoüberwachung wegen technischer Schwierigkeiten bei der Anpassung an die datenschutzrechtlichen Maßgaben nicht in Betrieb sei. Eine weitere Anfrage unsererseits vom September 2007 zum Sachstand blieb unbeantwortet. Daraufhin führten wir im Dezember 2007 eine unangekündigte Kontrolle durch. Diese ergab, dass sich an der Videoüberwachung weder in technisch-organisatorischer noch in rechtlicher Hinsicht etwas geändert hatte. Entgegen der ausdrücklichen Aussage der Gemeinde, war die Anlage seit Jahresbeginn 2007 in Betrieb und zeichnete widerrechtlich Bildmaterial auf. Aufgrund der Verletzung der Unterstützungspflicht der Gemeinde und des Verstoßes gegen technisch-organisatorische Vorschriften durch die Wiederinbetriebnahme der Videokamera ohne vorherige Durchführung der vorgeschlagenen Maßnahmen sprach die Landesbeauftragte daraufhin eine förmliche Beanstandung aus und informierte die Kommunalaufsicht hierüber.

Die Unterstützung und Kooperation der Gemeinde und der Schule bei der Beseitigung der festgestellten technischen und organisatorischen Mängel war von Anfang an unzureichend. Die Verantwortlichen nahmen die Rechtswidrigkeit des Betriebs der Videoüberwachungsanlage bewusst in Kauf.

5 Inneres

5.1 Polizei- und Ordnungsbehörden

5.1.1 Technische Kontrolle beim Zentraldienst der Polizei

Im Berichtszeitraum führten wir eine von den einzelnen Fachverfahren unabhängige Kontrolle der Informationstechnik beim Zentraldienst der Polizei durch. Sie ergab Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen.

Vor der Einführung oder bei wesentlichen Änderungen automatisierter IT-Verfahren, in denen personenbezogene Daten verarbeitet werden, ist die Erstellung eines IT-Sicherheitskonzeptes auf Grundlage der Standards 100-2 und 100-3 des Bundesamtes für Sicherheit in der Informationstechnik erforderlich. Das Ziel besteht darin, vorhandene Risiken und Gefährdungen bereits im Vorfeld zu ermitteln und durch geeignete Gegenmaßnahmen beherrschbar zu gestalten. Das uns während der Kontrolle vorgelegte IT-Sicherheitskonzept des Zentraldienstes der Polizei befand sich noch im Entwurfsstadium, obwohl schon seit Jahren IT-Verfahren mit höchst sensitiven personenbezogenen Daten betrieben wurden. Die Auswertung des vorgelegten Entwurfes ergab zum damaligen Zeitpunkt gute Ansätze bei der Etablierung eines ganzheitlichen IT-Sicherheitsprozesses. Im Zuge der Einführung eines computergestützten Vorgangsverwaltungssystems (ComVor) bei der Polizei[46] wurden die überwiegenden Bausteine der Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik im IT-Sicherheitskonzept berücksichtigt. Wir gehen davon aus, dass der eingeschlagene Weg konsequent fortgesetzt wird, und möglichst zügig alle betroffenen IT-Systeme im IT-Sicherheitskonzept des Zentraldienstes der Polizei abschließend betrachtet werden.

Die Gebäude- und Raumsicherung entsprach den Forderungen gem. § 10 Abs. 2 Nr. 1 Brandenburgisches Datenschutzgesetz. Die Serverräume sind nach dem Stand der Technik mit Brand- und Alarmmeldeanlagen ausgestattet. Die in einem Serverraum zwischengelagerten Verpackungsmaterialien wurden kurzfristig entfernt.

[46] vgl. A 5.1.2

Der zentrale Sicherungsserver befand sich zum Zeitpunkt der Kontrolle im selben Gebäude wie die zu sichernden Server. Über dem Sicherungsserver verliefen Wasser führende Leitungen. Diesen Zustand haben wir bemängelt und eine Umsetzung des Servers gefordert. Der Zentraldienstes der Polizei folgte unserer Auffassung und installierte den zentralen Sicherungsserver in einem anderen Gebäude.

Auf Grund der Vielzahl von Passwörtern (bis zu 8 Passwörter), die sich ein Nutzer für diverse Fachanwendungen merken muss, empfahlen wir zur Erhöhung der Sicherheit die Realisierung einer Single-Sign-On-Anmeldung unter Verwendung von Chipkarten. Der Zentraldienst der Polizei folgte unserer Empfehlung nicht, da seines Erachtens hierzu eine zentrale Nutzerverwaltung erforderlich sei, die erst mit der Einführung von ComVor zur Verfügung stehen werde.

Positiv ist hervorzuheben, dass im gesamten Polizei-Netz (POL1-Netz) eine Leitungsverschlüsselung mit LineCrypt-Geräten realisiert wurde. Die Administration der LineCrypt-Geräte erfolgt zentral beim Zentraldienst der Polizei. Die Verschlüsselung von personenbezogenen Daten mit sehr hohem Schutzbedarf (Schutzstufe D unseres Schutzstufenkonzeptes) im lokalen Netz (LAN) sowie eine Datenbankverschlüsselung erfolgen dagegen derzeit noch nicht. Nur durch Realisierung einer Ende-zu-Ende- und Datenbankverschlüsselung kann sichergestellt werden, dass insbesondere im LAN ein Missbrauch von personenbezogenen Daten ausgeschlossen ist.

Der Zentraldienst der Polizei sollte die Erstellung des IT-Sicherheitskonzeptes unter Berücksichtigung der BSI-Standards 100-2 und 100-3 zügig abschließen und den daraus resultierenden Maßnahmekatalog konsequent und zeitnah umsetzen.

5.1.2 Vorgangsbearbeitungssystem ComVor

Mit der flächendeckenden Inbetriebnahme löste das neue Datenverarbeitungssystem der brandenburgischen Polizei − ComVor − im November 2007 das bisherige „Polizeiliche Auskunftssystem Straftaten“ (PASS) ab. Gleichzeitig wurde die Anbindung an das „Informationssystem der Polizeien des Bundes und der Länder“ (INPOL) vollzogen. An der Einführung wurden wir seit Ende 2006 zunächst sporadisch beteiligt, seit Anfang 2007 nahmen wir regelmäßig an den Arbeitssitzungen der ComVor-Projektgruppe und der behördlichen Datenschutzbeauftragten der Polizei zu datenschutzrechtlichen Problemen teil.

Die **Com**putergestützte **Vor**gangsbearbeitung **ComVor** ermöglicht die Erfassung von Sachverhalts-, Objekt- und Personendaten innerhalb eines Vor-

gangs. Die Bearbeitung der Vorgänge in ComVor erfolgt nach dem Sachbearbeiterprinzip, d. h. nur der zuständige Sachbearbeiter kennt Inhalt und personenbezogene Daten innerhalb des ihm zugewiesenen Vorgangs.

Das gesamte neue Datenverarbeitungssystem besteht im Wesentlichen aus den Komponenten:

- ComVor Brandenburg als vollzugspolizeiliche Vorgangsbearbeitung und Tätigkeitsdokumentation,

- ComVor-Index als automatisiertes Abrufverfahren,

- Schnittstellen u. a. zu MESTA (Brandenburgisches Staatsanwaltliches Verfahrensregister), zur Internetwache und zu

- POLAS (Polizeiliches Auskunftssystem in der Version INPOL-Land) als Landesdatenbank „Strafsachen“ und als Anbindungsverfahren an INPOL sowie

- Benutzerverwaltung Brandenburg als Verwaltungssystem u. a. für die o. g. Komponenten und die Zugriffsrechte auf die Anwendungen.

Zu ComVor Brandenburg, ComVor-Index, POLAS und Benutzerverwaltung Brandenburg hat die Projektgruppe Verfahrensverzeichnisse erarbeitet, die in den o. g. Arbeitssitzungen besprochen wurden.

5.1.2.1 Verfahrensverzeichnis: Regelungen zum Löschen personenbezogener Daten

Teilweise hielten wir die Regelungen der Prüf- und Löschfristen für unzureichend, da sie sich auf die Aufzählung und Zitierung der einschlägigen Vorschriften des Brandenburgischen Polizeigesetzes und der Richtlinien zur Führung der Kriminalpolizeilichen Sammlungen beschränkten und damit den gesetzlichen Vorgaben des § 37 Abs. 1 Satz 2 Brandenburgisches Polizeigesetz (BbgPolG) nicht genügten. Danach müssen für jedes Verfahren konkrete Fristen sowie die Verantwortlichkeiten für deren Festlegung, Prüfung und Einhaltung festgelegt werden.

Mit einigen Änderungen wurde unserem Vorschlag zu den Prüf- und Löschfristen gefolgt. Danach gilt nun im Wesentlichen, dass beim ersten Anlegen eines Datensatzes zu einer Person stets eine Prüffrist von 13 Monaten festzulegen ist. In der danach erfolgenden Erforderlichkeitsprüfung muss bei Aufbewahrungsverlängerung eine neue Prüffrist vergeben und in der Kriminalakte begründet werden.

Eine Erforderlichkeitsprüfung ist im Übrigen nicht nur bei den festgelegten Prüfterminen durchzuführen, sondern auch anlässlich jeder Einzelfallbearbeitung eines Datensatzes zu einer Person. Ist die Erforderlichkeit der weiteren Speicherung nicht mehr gegeben, führt dies zur Löschung vor dem eigentlichen Fristablauf.

Ferner sind Daten über Kinder sowie über Kontakt-, Begleit- und Auskunftspersonen nun nach Ablauf von 2 Jahren zu löschen. Weiterhin sind Fälle geringer Bedeutung sowie solche, in denen der Verdacht einer Straftat entfallen ist, im Allgemeinen spätestens nach Ablauf der ersten Prüffrist zu löschen.

Eine Besonderheit der Vorgangsverwaltung in ComVor ist, dass Fehlerfassungen nicht gelöscht werden können. Das ist der ComVor-Philosophie geschuldet, der zu Folge das System einen lückenlosen Nachweis polizeilicher Tätigkeit – und eben auch der falschen Handlungen – ermöglichen soll. Dass auch als falsch erkannte Daten nicht gelöscht werden können, sondern, lediglich mit dem neuen Status „Fehlerfassung“ versehen, bis zum Einsetzen der Löschroutinen weitergespeichert werden sollten, wurde nicht nur von uns, sondern auch von den behördlichen Datenschutzbeauftragten kritisiert. Daraufhin wurde eine datenschutzrechtlich hinnehmbare Lösung geschaffen: Fehlerfasste Vorgänge werden nunmehr abgeschlossen und können in ComVor Brandenburg vom Sachbearbeiter oder anderen Zugriffsberechtigten nicht mehr aufgerufen werden. Diese Änderung wird im Vorgang in ComVor Brandenburg dokumentiert. In ComVor-Index können Personen oder Institutionen mit dem Status „Fehlerfassung“ nicht recherchiert werden.

Insgesamt ist mit diesen Regelungen zu erwarten, dass in ComVor die datenschutzrechtlichen Belange der Betroffenen besser gewahrt werden als im abgelösten Datenverarbeitungssystem.

5.1.2.2 IT − Sicherheitskonzept

Vor der Einführung automatisierter IT-Verfahren, in denen personenbezogene Daten verarbeitet werden, ist die Erstellung eines IT-Sicherheitskonzeptes auf der Basis einer Risikoanalyse erforderlich. Das Ziel besteht darin, vorhandene Risiken und Gefährdungen bereits im Vorfeld zu ermitteln und durch geeignete Gegenmaßnahmen beherrschbar zu gestalten. Im Januar 2007 erfolgte erstmals ein Treffen mit Vertretern der Projektgruppe ComVor, die u. a. die Erstellung eines IT-Sicherheitskonzeptes nach den Standards 100-2 und 100-3 des Bundesamtes für Sicherheit in der Informationstechnik[47] (BSI) von allen Beteiligten als erforderlich ansah. In den darauf folgenden Monaten

[47] siehe http://www.bsi.de/literat/bsi_standard/index.htm

wurde auf diversen Projektgruppensitzungen unter unserer Mitarbeit ein IT-Sicherheitskonzept für das System ComVor / POLAS erstellt. Es wurde während der IT-Strukturanalyse schnell klar, dass eine große Anzahl von IT-Systemen und Anwendungen zu betrachten sind. Die Schutzbedarfsfeststellung ergab zum überwiegenden Teil einen hohen bis sehr hohen Schutzbedarf (Schutzstufe C und D unseres Schutzstufenkonzeptes) in den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit. Daraus ergab sich die Notwendigkeit einer ergänzenden Risikoanalyse auf der Basis von IT-Grundschutz.

Nach der IT-Strukturanalyse, der Schutzbedarfsfeststellung und der Modellierung des IT-Verbundes schreibt der BSI-Standard 100-2 einen Basis-Sicherheitscheck vor. Ziel ist es, anhand eines Soll-Ist-Vergleichs herauszufinden, ob Standard-Sicherheitsmaßnahmen ausreichend umgesetzt sind. Der Basis-Sicherheitscheck, der ca. 500 Seiten umfasste, wurde uns in elektronischer Form zur Verfügung gestellt. Nur unter Zuhilfenahme des BSI Tools IT-Grundschutz[48] (GSTOOL) war es in angemessener Zeit möglich, eine Bewertung des Soll-Ist-Vergleichs vorzunehmen und die aus Sicht des Datenschutzes unbedingt vor Produktivsetzung zu realisierenden technisch-organisatorischen Maßnahmen herauszufiltern.

Nach Auswertung der Ergebnisse des Basis-Sicherheitschecks und der erweiterten Risikoanalyse wurden die umzusetzenden technischen und organisatorischen Maßnahmen von der Projektgruppe in einem Realisierungsplan zusammengefasst. Der größere Teil der erforderlichen Maßnahmen konnte vor der Produktivsetzung des Verfahrens ComVor realisiert werden. Es gibt jedoch auch Maßnahmen, die erst im Nachhinein umgesetzt wurden bzw. noch umgesetzt werden. Dazu zählen u. a. der Abschluss einer Dienstvereinbarung gem. § 65 Personalvertretungsgesetz, die Verschlüsselung von im lokalen Netz übertragenen Daten, die sichere Administration von aktiven Netzkomponenten, die datenschutzgerechte Protokollierung und die Verschlüsselung der in den Datenbanken gespeicherten sensitiven personenbezogenen Daten. Insbesondere die Realisierung der letztgenannten Maßnahme erweist sich als schwierig, da eine Umsetzung nur gemeinsam mit den an der Kooperation beteiligten Ländern erfolgen kann. Das Ministerium des Innern betrachtet die Maßnahme mit „höchster Priorität“ und werde sich innerhalb der Kooperation für eine zügige Realisierung der Datenbankverschlüsselung einsetzen.

[48] siehe http://www.bsi.de/gstool/index.htm

Im computergestützten Vorgangsbearbeitungssystem ComVor der Polizei des Landes werden personenbezogene Daten mit sehr hohem Schutzbedarf verarbeitet. Die Risiken wurden mit Hilfe eines umfassenden IT-Sicherheitskonzepts analysiert und entsprechende technisch-organisatorische Maßnahmen daraus abgeleitet. Die noch offenen Maßnahmen sind schnellstmöglich durch das Ministerium des Innern umzusetzen.

5.1.3 Akkreditierungsverfahren

Seit der Fußballweltmeisterschaft im Jahr 2006 steht der Begriff „Akkreditierungsverfahren" für die bei Staatsbesuchen, aber auch anderen Großveranstaltungen immer schon übliche polizeiliche Maßnahme, Personen, die dort einer beruflichen oder ehrenamtlichen Tätigkeit nachgehen wollen, anhand der polizeilichen Datensammlungen zu überprüfen. Damit sollen bereits im Vorfeld soweit wie möglich Gefahren für die Staatsgäste oder die Besucher ausgeschlossen werden. Vor der Fußballweltmeisterschaft wurden 180 000 Personen überprüft. In der Folge ist das Überprüfungsverfahren – nicht zuletzt auf Drängen der Datenschutzbeauftragten – nicht nur transparent, sondern auch in datenschutzrechtlicher Hinsicht verbessert worden.

Bei Staatsbesuchen und sportlichen Großereignissen handelt es sich um Anlässe, bei denen Gefahren für die öffentliche Sicherheit nicht auszuschließen sind, sodass die Polizei Maßnahmen zum Schutz der Veranstaltung treffen muss. Das geschieht auch durch die Überprüfung des Personenkreises, der vom Journalisten bis zum Würstchenverkäufer alle umfasst, die sich um eine der vom Veranstalter ausgeschriebenen Stellen bewerben oder die dort ehrenamtlich tätig werden wollen. Die dazu nötige Datenerhebung durch den Veranstalter oder Arbeitgeber und die Übermittlung an die Polizei zum Zweck der Überprüfung sollte mit ausdrücklicher Einwilligung des Betroffenen nach § 4 Abs. 1b Brandenburgisches Datenschutzgesetz erfolgen – auch wenn die Teilnahme an dem Ereignis natürlich ohnehin freiwillig ist.

Das daran anschließende polizeiliche Verfahren kann als hoheitliche Aufgabe nicht mehr auf der Grundlage einer Einverständniserklärung nach dem Datenschutzgesetz durchgeführt werden. Dazu bedarf es polizeirechtlicher Vorschriften. In Brandenburg sind dies die allgemeine Datenverarbeitungsbefugnis in § 39 Abs. 1 und 2 Brandenburgisches Polizeigesetz (BbgPolG) für erforderlichen Abgleiche der Daten der zu akkreditierenden Personen mit den polizeilichen Datenbeständen sowie die Befugnisse in §§ 43 und 44 BbgPolG für die Übermittlung der Überprüfungsergebnisse an den Veranstalter oder Arbeitgeber. Auf Bundesebene gelten die Spezialvorschriften zum Schutz von Staatsgästen des § 5 i. V. m. §§ 22, 24 und 25 Bundeskriminalamtgesetz

(BKAG) sowie die weiteren dortigen Vorschriften zur Zusammenarbeit der Polizeibehörden des Bundes und der Länder und zur Datenübermittlung.

Auch soweit die Verfassungsschutzbehörden des Bundes und der Länder in die Überprüfungen einbezogen werden, bedarf es ungeachtet der Einwilligung des Betroffenen entsprechender Befugnisse durch die Verfassungsschutzgesetze der Länder. Das Bundesverfassungsschutzgesetz enthält mit der in § 1 i. V. m. § 6 geregelten Zusammenarbeits- und Unterstützungspflicht sowohl Abgleichs- als auch Übermittlungsbefugnisse für die vom Bundeskriminalamt übermittelten Daten. Zulässig ist danach nur der Datenaustausch zwischen Bundesamt für Verfassungsschutz und Bundeskriminalamt bzw. den Verfassungsschutzbehörden untereinander, nicht aber mit den Polizeibehörden der Länder.

Die vor der Fußballweltmeisterschaft 2006 vom Deutschen Fußballbund (DFB) ausgearbeitete Einverständniserklärung, die den Betroffenen bei ihrer Bewerbung zur Verfügung gestellt werden sollte, entsprach nicht den gesetzlichen Anforderungen. Weder ging das Verfahren als solches noch die – bis dahin nicht übliche – Beteiligung der Verfassungsschutzbehörden an den Überprüfungen daraus hervor. Das Formular wurde den datenschutzrechtlichen Anforderungen zwischenzeitlich angepasst. Als sog. Datenschutzinformation weist die seither auch bei den folgenden Akkreditierungsverfahren verwendete Erklärung den Betroffenen auf die Freiwilligkeit der Teilnahme an dem Akkreditierungsverfahren hin. Sie klärt im Weiteren darüber auf, wer seine Daten speichert, welche Stellen anhand welcher Dateien seine Zuverlässigkeit überprüfen und welche Kriterien der Akkreditierungsentscheidung zu Grunde liegen. Schließlich erfährt man, an wen das Überprüfungsergebnis übermittelt wird und welche Information es über den Betroffenen enthält und dass die Daten ein Jahr nach dem Ende der Veranstaltung gelöscht werden.

Das Bundeskriminalamt richtete eine zentrale Unterstützungseinheit für den Datenabgleich zwischen den Landeskriminalämtern, der Bundespolizei und dem Bundesamt für Verfassungsschutz ein. Grundlage ihrer Arbeit war eine vom Deutschen Fußballbund geführte zentrale Datenbank für Akkreditierungsdaten.

Das Bundesamt für Verfassungsschutz übermittelte nur die negativ bewerteten Datensätze an die zuständigen Polizeistellen des Bundes und der Länder. Dort wurde ein sog. Gesamtvotum als Ergebnis der abgeschlossenen Zuverlässigkeitsüberprüfung eines Bewerbers gebildet, welches, wiederum vermittelt durch die Zentrale Unterstützungseinheit, an den Deutschen Fußballbund bzw. den Arbeitgeber weitergeleitet wurde. Eine ablehnende Entscheidung erfolgte immer dann, wenn eine der beteiligten Stellen ein Negativvotum getroffen hatte. Sowohl beim Deutschen Fußballbund als auch bei den an

den Zuverlässigkeitsüberprüfungen beteiligten Stellen sollten die Daten für eventuelle Nachfragen anschließend noch ein Jahr lang aufbewahrt werden.

Im Landeskriminalamt Brandenburg ist die Akkreditierungsdatenbank aufgelöst und der archivierte Datenbestand im Jahr 2007 gelöscht worden.

Die datenschutzrechtliche Prüfung der vom Landeskriminalamt und der Verfassungsschutzbehörde durchgeführten Akkreditierungsverfahren im Zusammenhang mit den diesjährigen Staatsbesuchen und Gipfeltreffen ergab keine Mängel.

Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungsverfahren erfolgen insoweit auf freiwilliger Basis, als niemand verpflichtet ist, sich aus beruflichen oder sonstigen Gründen zu einer Großveranstaltung akkreditieren zu lassen.

5.1.4 Ortung von Handys bei Notrufen

Eine gemeinnützige Stiftung hat allen Rettungsleitstellen in Deutschland ein Verfahren zur Ortung von Mobiltelefonen bei Notrufen angeboten. In Zusammenarbeit der Datenschutzbeauftragten von Bund und Ländern, Mobilfunknetzbetreibern, Stiftung und Leitstellen konnten datenschutzrechtliche Bedenken erörtert und eine vorläufige Lösung für die Nutzung dieses Angebots erarbeitet werden.

Zentraler Baustein des Verfahrens ist eine von der Stiftung betriebene Plattform, die an das Internet angebunden ist. Die Leitstellen können dadurch bei einem Notruf durch Eingabe der übermittelten Rufnummer Standortinformationen erhalten, die mittels der von den Netzbetreibern gelieferten Funkzelleninformationen geografisch abgebildet werden können. Zu diesem Zweck haben alle vier Handy-Netzbetreiber jeweils einen Vertrag mit der Stiftung abgeschlossen, in dem die Bedingungen für den Abruf der Standortinformationen festgelegt sind.

Die Datenübertragung erfolgt verschlüsselt, die Authentifizierung wird durch Einmal-Passworte mit sehr kurzer Gültigkeit sichergestellt. Sämtliche Zugriffe auf die Lokalisierungsdaten werden protokolliert.

Zwar sind die Netzbetreiber nach dem Telekommunikationsgesetz schon jetzt verpflichtet, bei einem Notruf der Leitstelle auch die Standortinformationen zu übermitteln, ohne dass es einer Einwilligung bedarf. Eine solche direkte Übermittlung an die Leitstellen ist zurzeit jedoch technisch nicht möglich. Deshalb ist die von der Stiftung entwickelte Lösung derzeit die einzige Möglichkeit.

Da die Vorschriften des Telekommunikationsgesetzes die Einschaltung eines Dritten bei der an sich notwendigen Übermittlung der Standortinformationen nicht vorsehen, bedarf es rechtlich der Einwilligung des Anrufers, damit die durch die Stiftung ermittelten geografischen Standortdaten an die Rettungszentralen weitergeben werden dürfen. Dieser wird bei einem Notruf zunächst befragt, ob er mit der Ortung seines Handys einverstanden ist. Ist ein Anrufer aufgrund seiner Notsituation nicht mehr in der Lage, eine Einwilligung zu erteilen, kommt nur eine mutmaßliche Einwilligung oder ein rechtfertigender Notstand als rechtliche Grundlage in Betracht. Die gefundene Lösung kann wegen der offensichtlichen Schwächen bei der Herleitung einer rechtlich wirksamen Einwilligung der Anrufer nur für eine Übergangszeit bis zur Schaffung der rechtlichen, technischen und organisatorischen Voraussetzungen für eine unmittelbare Übermittlung der notwendigen Informationen von den Netzbetreibern an die Leitstellen akzeptiert werden.

Neben der Ortung auf der Basis der zum Teil sehr ungenauen Funkzelleninformationen bietet die Stiftung auch die sehr viel genauere Ortung über das satellitengestützte Global Positioning System (GPS) an. Dies ist natürlich nur mit Mobilfunkgeräten möglich, die einen GPS-Empfänger haben. Um diese Möglichkeit im Notfall nutzen zu können, müssen sich die Nutzer im Voraus in einer entsprechenden Datenbank der Stiftung registrieren und in die Übermittlung der GPS-Koordinaten an die Leitstelle im Falle eines Notrufs einwilligen. Hiergegen bestehen aus datenschutzrechtlicher Sicht wegen der rechtlichen Eindeutigkeit der Einwilligung keine Bedenken. Die GPS-Ortung ist technisch unabhängig von den Netzbetreibern und wird allein von der Stiftung betrieben.

Die eingesetzte Technologie beinhaltet ein gewisses Missbrauchspotential, da es theoretisch möglich ist, beliebige Handys auch ohne Eingang eines Notrufs zu orten. Eine Ortung ist nach den Vertrag zwischen Netzbetreibern und Stiftung allerdings auch dann unzulässig, wenn ein Anrufer behauptet, ein Dritter befinde sich in einer Notlage. Eine Missbrauchskontrolle ist aufgrund der Protokollierung bei der Stiftung selbst möglich. Außerdem werden alle Notrufe bei den Leitstellen aufgezeichnet und für maximal sechs Monate gespeichert. Die Einhaltung dieser Löschungsfristen muss auch die Stiftung vertraglich zusichern.

Die Einbindung eines Dienstleisters für die Übermittlung von Standortinformationen bei Notrufen von Mobiltelefonen ist datenschutzrechtlich unter bestimmten Bedingungen möglich. Wegen der rechtlichen Schwächen und der Gefahr des Missbrauchs der Ortungsmöglichkeiten sollten solche Verfahren jedoch nur solange eingesetzt werden, bis das Bundesministerium für Wirtschaft und Technologie und die Bundesnetzagentur die notwendigen rechtlichen und organisatorischen Voraussetzungen für eine unmittelbare Übermittlung der Daten an die Leitstellen geschaffen haben.

5.1.5 Beweisfoto im Verwarngeldverfahren

Vielen Ordnungsbehörden ist unklar, inwieweit sie die bei Geschwindigkeitsübertretungen stets als Beweismittel hergestellten Fotos zur Fahrerermittlung im Verwarn- bzw. Bußgeldverfahren verwenden dürfen. In Brandenburg gibt es weder hierfür, noch für den Umgang der Meldebehörden mit entsprechenden Anfragen eine einheitliche Verfahrensweise. Wir baten daher das die Fachaufsicht führende Ministerium des Innern eine verbindliche, einheitlich anzuwendende Regelung zu treffen.

Rechtsgrundlage für den Abgleich von Beweisfotos mit den bei den Meldebehörden im Pass- und Personalausweisregister gespeicherten Bilder ist § 9 Brandenburgisches Personalausweisgesetz i. V. m. § 2b Bundespersonalausweisgesetz. Danach dürfen die Personalausweisbehörden bzw. nach § 22 Passgesetz die Passbehörden anderen Behörden Daten aus ihren Registern zu deren Aufgabenerfüllung übermitteln. Voraussetzung ist, dass diese Behörden die Daten beim Betroffenen selbst nicht oder nur mit unverhältnismäßigem Aufwand erheben können.

Betroffener in Verkehrssachen ist zuerst der Fahrzeughalter, sodass zunächst auch nur er als Adressat von Maßnahmen zur Feststellung des für die Geschwindigkeitsübertretung verantwortlichen Fahrers in Frage kommt. Der Abgleich von Beweisfotos ist somit auch nur zu dem Zweck zulässig, den Halter als verantwortlichen Fahrer festzustellen oder auszuschließen. Also darf ein Beweisfoto zur Fahrerermittlung auch nur mit dem Antragsfoto des Halters im Personalausweisregister abgeglichen werden. Wegen des zu beachtenden Grundsatzes der Erforderlichkeit muss der Abgleich unterbleiben, wenn Alter und/oder Geschlecht der auf dem Beweisfoto abgebildeten Person nicht den festgestellten Halterdaten entspricht. Es ist unzulässig, eine Registerabfrage zur Suche nach als Fahrer infrage kommenden Familienangehörigen des Halters oder anderen, mit dem Halter namensgleichen Personen – sozusagen „ins Blaue hinein“ – durchzuführen, um dann deren Antragsfotos mit dem Beweisfoto abzugleichen. Zur Sachaufklärung ist es aber stets zulässig, das Beweisfoto im nachbarschaftlichen Umfeld oder im Fami-

lienkreis des Halters vorzulegen, um so den verantwortlichen Fahrer festzustellen.

In der Praxis finden die Beschränkungen der Vorschrift häufig keine Beachtung. Nur wenigen Meldebehörden scheint die Beschränkung des Abgleichs auf die Feststellung, ob der Fahrzeughalter auch der verantwortliche Fahrer ist und somit auch nur dessen Registerfoto mit dem Beweisfoto abgeglichen werden darf, bekannt zu sein. Bei vielen wird das Abgleichsersuchen der Verfolgungsbehörden häufig ganz selbstverständlich auch auf die Familienangehörigen erstreckt. Bleibt das ohne Erfolg, wird dieser Kreis oft über Familienangehörige hinaus dann auch noch auf Personen erweitert, die lediglich denselben Nachnamen wie der Halter tragen.

Nach geltender Rechtslage dürfen Registerdaten zum Zweck des Abgleichs jedoch nur ausnahmsweise und erst wenn andere Ermittlungsmethoden erfolglos waren, übermittelt werden. Die bloße Vermutung, dass es sich bei dem abgebildeten Fahrer um ein Familienmitglied des Halters oder gar um eine Person handelt, von der nichts weiter bekannt ist, als dass sie den gleichen Nachnamen trägt, erlaubt keinen Abgleich mit der Passfotodatei.

Das Ministerium der Innern teilt im Wesentlichen unsere Rechtsauffassung. Eine landeseinheitliche Regelung für die hiesigen Verfolgungsbehörden und die Meldestellen soll jedoch erst erlassen werden, wenn Einvernehmen über die zulässige Amtshilfe der Meldestellen mit den anderen Bundesländern hergestellt worden ist.

Ein Abgleich zwischen den Beweisfotos der Ordnungsbehörden zum Zweck der Verfolgung von Geschwindigkeitsübertretungen mit den Fotos aus dem Pass- oder Personalausweisregister der Meldebehörden ist ausschließlich zulässig, um festzustellen, ob der Halter des Fahrzeuges am Steuer saß.

5.1.6 Nutzung des Gewerberegisters zur Verfolgung von Verkehrsordnungswidrigkeiten

Ein Petent wunderte sich, wie die Bayerische Polizei ihn als verantwortlichen Fahrer eines in Brandenburg zugelassenen Firmenwagens ermitteln konnte, obwohl er weder in Bayern noch in Brandenburg wohnte und schon einige Zeit vor der hier verfolgten Geschwindigkeitsübertretung seine Firmenanteile veräußert hatte.

Nach der Geschwindigkeitsübertretung auf der Autobahn wurde von der Bayerischen Polizei als zuständiger Verfolgungsbehörde durch Kennzeichenabfrage im Zentralen Verkehrsinformationssystem (ZEVIS) beim Kraftfahrtbundesamt die brandenburgische Firma als Fahrzeughalterin festgestellt.

Nachdem der Zeugenfragebogen zur Ermittlung des verantwortlichen Fahrers durch die Firma mit ungenügenden Identifizierungsangaben und ohne ladefähige Anschrift beantwortet worden war, hat die Verfolgungsbehörde die zuständige Polizeidienststelle in Brandenburg um Amtshilfe gebeten. Die daraufhin durchgeführten Ermittlungen blieben allerdings ergebnislos. Daraufhin wurde die Brandenburgische Polizei ersucht, die vollständigen Personalien, einschließlich Privatanschrift des Geschäftsführers zu ermitteln, da die Bayerische Polizei aufgrund „polizeilicher Erfahrungen“ den Verdacht hatte, der verantwortliche Fahrer sei im Bereich der Geschäftsleitung zu finden. Jetzt wandte sich die hiesige Polizei an das zuständige Gewerbeamt, bat um erweiterte Auskunft aus dem dortigen Gewerberegister und übermittelte der Verfolgungsbehörde die dort erfassten Personalien der Geschäftsführer. So ist die bayerische Verfolgungsbehörde an die Privatanschrift des Petenten gekommen.

Die Nutzung des örtlichen Gewerberegisters war rechtmäßig, nachdem die Versuche erfolglos geblieben waren, den verantwortlichen Fahrer durch mehrmalige Vorlage des Beweisfotos in der Firma zu ermitteln.

Gem. § 14 Gewerbeordnung (GewO) muss jedes Gewerbe beim örtlichen Gewerbeamt angezeigt werden. Bei Personengesellschaften (wie OHG, GbR und KG) ist jeder geschäftsführende Gesellschafter anzeigepflichtig soweit er persönlich haftet. Anzuzeigen ist ferner jede Veränderung des Standortes, der Gewerbeart, der Produkte und bei einer KG auch das Ausscheiden eines Gesellschafters sowie im Übrigen eines Kommanditisten soweit er Geschäftsführungsbefugnis hat. Öffentlichen Stellen dürfen nach § 14 Abs. 6 GewO Name, betriebliche Anschrift und angezeigte Tätigkeit aus der Gewerbeanzeige übermittelt werden. Nach Satz 3 ist darüber hinaus auch die Übermittlung weiterer Daten zulässig, wenn es zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich ist.

Die Speicherung und Übermittlung des falschen – weil schon aus der Firma ausgeschiedenen – Datums „Geschäftsführung der in Rede stehenden Firma“ war keine unrechtmäßige Datenverarbeitung des Gewerbeamts, weil Petent und Firma es versäumt hatten, die Änderung in der Geschäftsführung auch dem örtlichen Gewerbeamt gegenüber anzuzeigen.

Das Vorgehen der Verfolgungsbehörde und der um Amtshilfe ersuchten Brandenburgischen Polizei zur Feststellung des für die Verkehrsordnungswidrigkeit verantwortlichen Fahrers war rechtmäßig. Geschwindigkeitsübertretungen werden nach herrschender Rechtsauffassung als Ordnungswidrigkeiten von erheblicher Bedeutung betrachtet, zu deren Verfolgung aus dem Gewerberegister Privatanschriften an öffentliche Stellen übermittelt werden dürfen.

5.2 Verfassungsschutz

IT-Sicherheitskonzept beim Verfassungsschutz

Verfahren öffentlicher Stellen dürfen nur freigegeben werden, wenn ein IT-Sicherheitskonzept vorher gewährleistet, dass die von diesem Verfahren ggf. ausgehenden Risiken für die Rechte und Freiheiten der Betroffenen beherrschbar sind. Der Verfassungsschutz in Brandenburg betreibt seit Jahren alle seine Verfahren, ohne diese Untersuchung im Vorfeld durchgeführt zu haben. Dies ist besonders schwerwiegend, da die Behörde hoch sensitive personenbezogene Daten verarbeitet.

Mit der Änderung des Brandenburgischen Verfassungsschutzgesetzes im Jahre 2004 bekam die Verfassungsschutzbehörde die Möglichkeit, ihre Aufgabenerfüllung ausschließlich auf automatisierte Datenverarbeitung zu stützen. Dazu wurde ein Jahr später ein Verfahren „Content-Management System – VIPER (Verfassungsschutz-Informationsportal für Ermittlung und Recherche)“ eingeführt und freigegeben. Die Freigabe erfolgte, obwohl wir den Verfassungsschutz mehrfach darauf aufmerksam gemacht haben, dass die erforderlichen Unterlagen zur Risikoanalyse und zum IT-Sicherheitskonzept nicht vorlagen. Wir drängten auf eine baldige Umsetzung, zumal das Verfahren produktiv gesetzt wurde und sensitive personenbezogene Datensätze seither gespeichert, verknüpft und ausgewertet werden. Die uns daraufhin übermittelten Dokumentationen erfüllten nur in Teilen unsere Forderungen nach einem vollständigen und ganzheitlichen IT-Sicherheitskonzept. Im Rahmen eines Workshops erläuterten wir die strukturierte Vorgehensweise, die in den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik beschrieben ist. Begleitend zum Workshop wurden Gesprächsrunden bei der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht organisiert, die dazu dienten, den Verfassungsschutz in Abhängigkeit vom Fortschritt der Sicherheitskonzeption Schritt für Schritt zu begleiten und Hinweise zu geben.

Trotz umfassender Begleitung und Unterstützung sowie Kontaktaufnahme des Verfassungsschutzes mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben war es bis heute nicht möglich, ein vollständiges IT-Sicherheitskonzept zu erstellen. Den Verweis der Behörde auf fehlende Ressourcen können wir nach fast drei Jahren Wirkbetrieb nicht nachvollziehen. Ende September 2007 legte uns der Verfassungsschutz die letzte Version der Arbeiten an dem IT-Sicherheitskonzept zu dem Verfahren „VIPER“ vor, der nach wie vor datenschutzrechtliche Mängel aufweist und überarbeitungsbedürftig ist. Das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung muss auch von der Verfassungsschutzbe-

hörde respektiert werden. Ein möglicher Datenmissbrauch, z. B. Aufdeckung von Informationen zu V-Leuten, könnte erhebliche Risiken für Leib und Leben der Betroffenen darstellen.

Seit drei Jahren betreibt der Verfassungsschutz die automatisierte Datenverarbeitung ohne ausreichende Sicherheitskonzepte. Mit diesem schwerwiegenden Verstoß gegen die Vorschriften des Brandenburgischen Datenschutzgesetzes gefährdet die Behörde die Persönlichkeitsrechte Betroffener in nicht hinnehmbarer Weise.

5.3 Datenverarbeitung, Statistik und Wahlen

5.3.1 Outsourcing des SAP-Systembetriebs im Projekt Neues Finanzmanagement und seine Auswirkungen auf das Landesverwaltungsnetz

Das Ministerium der Finanzen entschied in seiner Funktion als Projektverantwortlicher, den Betrieb der zentralen SAP-Systemkomponenten für das Projekt Neues Finanzmanagement (NFM) vom Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben zu einem externen privaten Dienstleister, der Firma T-Systems, auszulagern.[49] Bei der Umsetzung dieser Entscheidung wurden jedoch Belange der IT-Sicherheit des Landesverwaltungsnetzes nur unzureichend beachtet.

Mit der Auslagerung der zentralen Systemkomponenten des SAP-Systems in das Rechenzentrum der Firma T-Systems nach Frankfurt am Main war zwingend eine Öffnung des Landesverwaltungsnetzes (LVN) verbunden. Während vor dem Outsourcing alle Daten des NFM-Projekts innerhalb dieses Netzes blieben und auf Servern im Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben verarbeitet wurden, müssen die Daten nunmehr das LVN verlassen. Damit ändert sich auch die Rolle des Landesbetriebes als Dienstleister in diesem Verfahren: Er ist nun nicht mehr für den Betrieb der SAP-Applikations- und Datenbankserver zuständig, sondern realisiert nur noch einen zentralen Übergabepunkt im LVN für die NFM-Daten und sorgt für deren Weiterleitung über das Weitverkehrsnetz zum Rechenzentrum von T-Systems. Konsequenz dieser Änderung ist auch, dass die Leitungsverschlüsselung der NFM-Daten[50] im Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben unterbrochen und eine Neuverschlüsselung vor der Übertragung zu T-Systems vorgenommen wird. Geht man von einem mittleren Schutzbedarf der im NFM-Projekt verarbeiteten Daten aus, ist diese Entscheidung tragbar. Betrachtet man jedoch die Weiterentwicklung des

[49] vgl. A 9.4

[50] vgl. Tätigkeitsbericht 2004/2005, A 1.3.3

Projekts[51] und insbesondere die beabsichtigte Modernisierung des Verfahrens für das Haushalts-, Kassen- und Rechnungswesen, das auf derselben technischen Plattform laufen soll, muss unter Berücksichtigung des dann hohen Schutzbedarfs eine durchgängige Ende-zu-Ende-Verschlüsselung realisiert werden.

Durch die Öffnung des LVN zum Weitverkehrsnetz können Risiken für die Datenverarbeitung innerhalb anderer Verfahren, die im Landesverwaltungsnetz betrieben werden, sowie für das LVN selbst entstehen. Denkbar sind z. B. Angriffe oder Einbrüche von außen, die Übermittlung von internen Daten an unberechtigte Dritte oder das Eindringen und die Verbreitung von Schadsoftware über geöffnete Netzwerkports. Mehrfach haben wir die Projektverantwortlichen im Ministerium der Finanzen sowie das Ministerium des Innern wegen seiner Aufsichtsfunktion über den Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben als Betreiber des LVN darauf hingewiesen, dass aus unserer Sicht mit der Auslagerung der zentralen SAP-Systemkomponenten auch eine Fortschreibung des Sicherheitskonzepts für das LVN erforderlich ist. Insbesondere sind Sicherheitsmaßnahmen zu realisieren, mit denen die mit der Öffnung des LVN verbundenen Risiken wirksam beherrscht werden können.

Nachdem die Verlagerung zu T-Systems durchgeführt wurde, haben wir vom Ministerium des Innern die Unterlagen angefordert, die die Umsetzung der für die Absicherung des LVN erforderlichen Sicherheitsmaßnahmen im Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben dokumentieren. Leider erhielten wir keine Antwort. Es stellte sich heraus, dass derartige Unterlagen nicht in hinreichendem Umfang existierten. Wir haben deshalb gegenüber dem Ministerium des Innern eine Beanstandung ausgesprochen.

In seiner Antwort auf diese Beanstandung teilte uns der Minister mit, dass er die Weisung zur Öffnung des LVN im Zuge der Umsetzung einer Entscheidung der Landesregierung zum SAP-Outsourcing getroffen hat und davon auszugehen sei, dass die mit der Öffnung verbundenen Risiken bereits ausreichend beherrscht würden. Gleichzeitig regte er jedoch eine Zusammenarbeit an, um eine Verbesserung des Sicherheitsniveaus und die Schließung noch vorhandener Lücken zu erreichen. Zu den in Aussicht gestellten technischen Maßnahmen gehören die Einrichtung eines Einbruchserkennungssystems (Intrusion Detection System, IDS)[52] zur Erkennung und Abwehr illegaler Datenpakete, eine Überprüfung der Struktur des LVN und der Absicherung zwischen verschiedenen Netzsegmenten sowie eine detaillierte Analyse der

[51] vgl. A 9.3
[52] vgl. A 2.9

Kommunikation zwischen zentralen SAP-Systemkomponenten und dezentralen Clients in den Landesbehörden.

Wir haben diese Anregung begrüßt und dem Vorschlag zugestimmt, dass das neu zu bildende IT-Sicherheitsmanagementteam[53] des Landes die Arbeiten zu diesen Themen begleitet.

Eine Öffnung des Landesverwaltungsnetzes nach außen ist stets nur unter sehr strengen Voraussetzungen möglich. Insbesondere sind Sicherheitsmaßnahmen zur Beherrschung der mit der Öffnung verbundenen Risiken für die Datenverarbeitung im LVN festzulegen. Die Maßnahmen sind vor der Netzöffnung vollständig und nachweisbar umzusetzen.

5.3.2 Einführung eines einheitlichen Dokumentenmanagement- und Vorgangsbearbeitungssystems in der Landesverwaltung

Die IT-Strategie des Landes Brandenburg für die Jahre 2004 bis 2008 sieht die Einführung eines landesweit einheitlichen Dokumentenmanagement- und Vorgangsbearbeitungssystems innerhalb der Landesverwaltung vor. Damit sollen u. a. die Voraussetzungen für eine stärkere Automatisierung von Verwaltungsvorgängen und die Einführung elektronischer Bürgerdienste geschaffen werden. Mit der Umsetzung dieser Zielstellung wurde begonnen.

Ein Dokumentenmanagement- und Vorgangsbearbeitungssystem (DMS/VBS) dient der Verwaltung elektronisch und nicht elektronisch erzeugter Dokumente über deren gesamten Lebenszyklus hinweg. Es unterstützt technisch die Erstellung, Bearbeitung, Weitergabe und Verteilung von Dokumenten, das Auffinden, Ablegen oder Löschen sowie die Übergabe an ein Archiv. Eine Anpassung an Strukturen bzw. Festlegungen der einzelnen Verwaltungen ist für einen erfolgreichen Einsatz des DMS/VBS erforderlich. Insbesondere soll die Abwicklung von Geschäftsprozessen mit Hilfe eines solchen Systems elektronisch gesteuert und überwacht sowie effizient, fehlerarm, revisionssicher und weit gehend medienbruchfrei vollzogen werden. Die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) hat mit dem DOMEA-Konzept[54] einen Leitfaden für die Einführung und den Betrieb von DMS/VBS in der öffentlichen Verwaltung herausgegeben.

Im Land Brandenburg liegen seit einigen Jahren in ausgewählten Bereichen Erfahrungen mit dem Einsatz von DMS/VBS vor. Beispielhaft seien an dieser

[53] vgl. A 5.3.3

[54] siehe http://www.kbst.bund.de

Stelle das Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz sowie das Ministerium des Innern genannt, die solche Systeme im Ressort bzw. pilothaft in einer Abteilung nutzen. Darüber hinaus wurden im Rahmen eines Projektes Möglichkeiten zum Austausch elektronischer Akten und Vorgänge zwischen verschiedenen DMS/VBS über die XML-Schnittstelle XDOMEA getestet. Aufbauend auf diesen Vorarbeiten hat eine Arbeitsgruppe unter Leitung des Ministeriums des Innern im zweiten Halbjahr 2007 die Ausschreibung zur landesweiten Einführung eines DMS/VBS in der Landesverwaltung vorbereitet. Unsere Behörde wirkte in dieser Arbeitsgruppe beratend mit.

Auf diese Weise war es uns möglich, bereits in der Phase der Ausschreibung des zukünftigen DMS/VBS die wesentlichen Anforderungen an Datenschutz und IT-Sicherheit bei der Einführung und beim Betrieb dieses Systems einzubringen. Hierzu gehören u. a.

- Festlegung von Rahmenbedingungen für den DMS/VBS-Einsatz, z. B. zur Aufbau- und Ablauforganisation, Zuständigkeiten, Verfahrens- und Bearbeitungsregeln, Einschränkung der Art der zu verarbeitenden Dokumente, Sicherung der Rechtsverbindlichkeit der Datenverarbeitung im DMS/VBS, Speicherdauer von Dokumenten und Protokolldaten der DMS/VBS-Nutzung,

- Feststellung des Schutzbedarfs der im DMS/VBS zu verarbeitenden Dokumente, Ermittlung von potentiellen Risiken durch den Einsatz des Systems,

- Ableitung eines verfahrensspezifischen Sicherheitskonzepts mit Maßnahmen, die dem Schutzbedarf der Dokumente und dem aktuellen Stand der Technik entsprechen,

- Erarbeitung eines umfassenden Rechte- und Rollenkonzepts nach dem Prinzip minimaler Rechtezuweisungen, Einschränkung der Rechte des Administrationspersonals,

- Einsatz von Verschlüsselungsverfahren zur Sicherung der Vertraulichkeit von Dokumenten beim Transport über Netze, ggf. Nutzung einer Ende-zu-Ende-Verschlüsselung sowie einer verschlüsselten Datenspeicherung (bei hohem Schutzbedarf),

- Sicherung der Integrität und Authentizität von Dokumenten und Bearbeitungsschritten im DMS/VBS durch den Einsatz von digitalen Signaturen, Anbindung an eine Public-Key-Infrastruktur, sichere Verwaltung privater Schlüssel z. B. auf Chipkarten,

- Erarbeitung von Konzepten zur Datensicherung und -wiederherstellung, Beschreibung von Notfallszenarien,

- datenschutzgerechte Protokollierung der Aktivitäten im DMS/VBS, Festlegungen zur Auswertung und Verwendung von Protokolldaten, Beteiligung der Personalvertretung.

In diesem Zusammenhag ist auch auf die Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ der Datenschutzbeauftragten des Bundes und der Länder zu verweisen, die über unser Internetangebot abrufbar[55] ist.

Die Ausschreibung zur landesweiten Einführung eines DMS/VBS enthält wesentliche Anforderungen an die Gewährleistung von Datenschutz und IT-Sicherheit. Wir werden im Rahmen der Entscheidung für einen Anbieter bzw. bei der Erstellung des Landesreferenzmodells sowie der ressortspezifischen Einführung des DMS/VBS in der Landesverwaltung auf deren Einhaltung achten.

5.3.3 Arbeitsgruppe „IT-Sicherheit“ der Landesverwaltung

In unserem letzten Tätigkeitsbericht[56] hatten wir über die Erarbeitung einer zentralen Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg (IT-Sicherheitsleitlinie) informiert. In der Zwischenzeit wurde diese Leitlinie vom Kabinett verabschiedet.

Zur Fertigstellung des Textes der IT-Sicherheitsleitlinie und zur Vorbereitung der Entscheidung der Landesregierung setzte der Interministerielle Ausschuss für Informationstechnik (IMA-IT) die Arbeitsgruppe „IT-Sicherheit“ unter Leitung des Ministeriums des Innern ein. Unsere Dienststelle wirkte in dieser Arbeitsgruppe beratend mit.

Die IT-Sicherheitsleitlinie beschreibt den Aufbau und den Betrieb eines zentral koordinierten, ressortübergreifenden Managementsystems zur Informationssicherheit, dessen Ziel die Erfüllung der grundlegenden IT-Sicherheitsziele (Vertraulichkeit, Integrität und Verfügbarkeit von Daten und IT-Diensten) in der Landesverwaltung ist. Hierzu sind ressortübergreifend Vorgehensweisen, Regelwerke und Aktivitäten zur Herstellung und Aufrechterhaltung von IT-Sicherheit abzustimmen und zu koordinieren. Wesentliche Festlegungen der IT-Sicherheitsleitlinie sind:

---

[55] siehe Anlage 5

[56] vgl. Tätigkeitsbericht 2004/2005, A 2.9

- Aufbau einer Organisationsstruktur für das Management zur Informationssicherheit: Bestellung von IT-Sicherheitsbeauftragten der Ressorts, Bildung eines IT-Sicherheitsmanagementteams unter Leitung eines IT-Sicherheitsmanagers des Landes, Aufbau eines CERT Brandenburg (Computer Emergency Response Team) als Anlaufstelle für präventive und reaktive Maßnahmen für IT-Sicherheit,

- Durchsetzung von Mindeststandards für IT-Sicherheit: Grundsatz der Angemessenheit von Sicherheitsmaßnahmen entsprechend dem Schutzzweck und dem Stand der Technik, Erarbeitung von Sicherheitskonzepten vor Einsatz eines Verfahrens, regelmäßige Prüfung und Fortschreibung der Sicherheitskonzepte, Orientierung an Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik bzgl. Vorgehensweisen (BSI-Standards 100-2, 100-3) und Schutzmaßnahmen (Grundschutzkataloge),

- Etablierung eines landesweiten IT-Sicherheitsprozesses: Planung und Umsetzung ressortspezifischer Sicherheitsrichtlinien und -konzepte entsprechend den konkreten Rahmenbedingungen, Anforderungen und Verantwortlichkeiten, Überwachung und Prüfung der Wirksamkeit von Sicherheitsmaßnahmen, Auswertung von Sicherheitsvorfällen und Verbesserung des Sicherheitsmanagements.

Bei der Umsetzung der Sicherheitsleitlinie kommt der Sensibilisierung aller Mitarbeiter der Landesverwaltung für die Belange der IT-Sicherheit und zugehörigen Schulungsmaßnahmen eine besondere Bedeutung zu.

Mit der Verabschiedung der IT-Sicherheitsleitlinie durch das Kabinett im Oktober 2007 wird sie für die Staatskanzlei, die Landesministerien und die ihnen nachgeordneten Behörden, Einrichtungen und Landesbetriebe sowie für die Gerichte und Staatsanwaltschaften des Landes unmittelbar verbindlich. Eine Ausdehnung auf den kommunalen Bereich kann im Rahmen von gemeinsam mit der Landesverwaltung durchgeführten E-Government-Vorhaben erfolgen. Wir empfehlen bereits jetzt allen Kommunen, sich bei der Gewährleistung von IT-Sicherheit an der Leitlinie des Landes oder vergleichbaren Regelwerken zu orientieren.

Die Arbeitsgruppe „IT-Sicherheit“ befasste sich unter unserer Beteiligung im Berichtszeitraum mit einer Reihe weiterer Themen wie z. B. der Nutzung von mobilen Datenträgern (USB-Speicher)[57] und Personal Digital Assistants (PDA), dem Einsatz von Terminalserver-Lösungen sowie der Notfallvorsorge für IT-Verfahren.

[57] vgl. A 2.6

Das IT-Sicherheitsmanagementteam des Landes ist zügig zu bilden. Wir erwarten, dass dieses Team die Arbeit der AG „IT-Sicherheit“ kontinuierlich fortsetzt und die Umsetzung der Sicherheitsleitlinie konsequent vorantreibt. Unsere Beratungsfunktion in diesem Gremium werden wir wahrnehmen.

5.3.4 Volkszählung 2011

Im August 2006 hat die Bundesregierung beschlossen, dass sich Deutschland an der kommenden Volkszählung („Zensus“) der Europäischen Union im Jahre 2011 mit einem registergestützten Zensus beteiligt.

Staatliche Einrichtungen sind auf hinreichend zuverlässige Informationen über die Bevölkerung und die Wohnsituation im Land angewiesen. Von den Einwohnerdaten hängen z. B. die Einteilung der Wahlkreise, die Planung von Kindergärten, Schulen und Einrichtungen für ältere Menschen ab. Auch für den Länderfinanzausgleich oder für die Zuweisungen von Mitteln an die Kommunen wird auf diese Zahlen zurückgegriffen. Die letzte Volkszählung im Gebiet der ehemaligen DDR fand 1981 und in den alten Bundesländern 1987 statt.

Zur Entlastung der Bevölkerung von Auskunftspflichten und um die Kosten möglichst gering zu halten, wurde mit einem Zensustest im Jahre 2001 geprüft, ob aus bestehenden Registern zuverlässige Zahlen für eine Volkszählung gewonnen werden können. Der Zensustest bewies die grundsätzliche Geeignetheit des Verfahrens, er brachte aber auch ans Licht, dass die durchschnittliche Fehlerquote in den Melderegistern bei fünf Prozent liegt.

Die Bundesregierung hat entschieden, im Jahre 2011 eine registergestützte Volkszählung einschließlich einer postalischen Gebäude- und Wohnungszählung durchzuführen. Die Erhebung soll sich im Wesentlichen auf Daten stützen, die bei Behörden bereits vorhanden sind, vor allem sollen die Daten der Melderegister, der Register der Bundesagentur für Arbeit und der Vermessungsbehörden herangezogen werden. Der registergestützte Teil wird stichprobenartig durch eine direkte Befragung von weniger als zehn Prozent der Bevölkerung ergänzt. Die Stichprobe soll außerdem zur Erhebung von Merkmalen und Bevölkerungsgruppen genutzt werden, die nicht in Registern enthalten sind (z. B. Daten zur Bildung und erwerbsstatistische Daten für Selbstständige).

Das Verfahren zur Verknüpfung der Daten mehrerer Register wird im Zensusvorbereitungsgesetz 2011 geregelt. Zu dem Entwurf, der einige datenschutzrechtlich bedenkliche Sachverhalte enthielt, nahmen die Datenschutzbeauftragten des Bundes und der Länder Stellung. Insbesondere muss kri-

tisch beobachtet werden, inwieweit der entscheidende Grundsatz der Trennung der Statistik vom Verwaltungsvollzug bei dem Bereinigungsverfahren der Register aufrechterhalten wird.

Aus datenschutzrechtlicher Sicht bestehen gegen einen registergestützten Zensus mit ergänzender Stichprobe keine grundsätzlichen Bedenken. Auf die Einhaltung der Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts von 1983 ist zu achten. Die Vorbereitung und Durchführung des Zensus werden wir weiterhin kritisch begleiten.

5.4 Personaldaten

5.4.1 Umgang mit Bewerberdaten – Kontrolle staatlicher Schulämter

Die staatlichen Schulämter erhalten eine Vielzahl von Bewerbungen von Lehrkräften. Wir haben uns in zwei staatlichen Schulämtern umgesehen und die Einhaltung datenschutzrechtlicher Vorschriften geprüft.

Die staatlichen Schulämter nutzen für die Verwaltung der Bewerberdaten ein spezielles Modul des Datenverarbeitungsverfahrens APSIS (Automatisierte Personal- und Stellenverwaltung im Schulamt), in welchem sie alle eingehenden Bewerbungen erfassen. Die Bewerberakten selbst werden verschlossen aufbewahrt.

Grundsätzlich wäre aus datenschutzrechtlicher Sicht eine unverzügliche Löschung von Bewerberdaten für den Fall, dass kein Dienstverhältnis zustande kommt, erforderlich. Aus Rationalisierungsgründen werden die Daten in APSIS für ein Jahr gespeichert, weil die Bewerbungen der Lehrkräfte meist auch für das Folgeschuljahr (Schuljahresplanung) Bestand haben sollen. Die Bewerber erhalten mit der schriftlichen Eingangsbestätigung ihrer Bewerbung gleichzeitig den Hinweis, dass der Speicherfrist von einem Jahr widersprochen werden kann. Darüber hinaus können sie ihre Einwilligung darin erteilen, dass die Bewerbungen über die Jahresfrist hinaus auch für zukünftige Regeleinstellungstermine gespeichert bleiben. Andernfalls werden sie im System APSIS nach einem Jahr gelöscht und die Akten vernichtet. Insgesamt ist das Verfahren aus datenschutzrechtlicher Sicht akzeptabel.

Aufgrund festgestellter technisch-organisatorischer Mängel gaben wir folgende Empfehlungen:

- Anpassung der Regelungen zu Passwörtern für das lokale Netz an die Empfehlungen der BSI-Grundschutzkataloge, Maßnahme M 2.11 (z. B. mindestens acht alphanumerische Zeichen, 90 Tage Gültigkeit),

- Ergänzung der Dienstanweisung um Festlegungen hinsichtlich der sparsamen Nutzung des zentralen Tausch-Verzeichnisses, Durchsetzen des regelmäßigen Löschens dieses Verzeichnisses,

- Einsatz von Software zur Verschlüsselung der auf Festplatten in Laptops gespeicherten Daten,

- Update der Systemsoftware der Server auf aktuelle Versionen.

Im Ergebnis unserer Kontrollen sind bei den von uns kontrollierten Schulämtern beim Umgang mit Bewerberdaten keine Datenschutzverletzungen, die zu einer Beanstandung geführt hätten, festzustellen gewesen.

5.4.2 Kein Ausbildungsplatz bei der Polizei infolge zweifelhafter Datenspeicherung

Die Polizei eines anderen Bundeslandes lehnte eine Bewerbung um einen Ausbildungsplatz ab, nachdem die Brandenburgische Polizei ein Ermittlungsverfahren gegen die Bewerberin wegen Straftaten mit rechtsradikalem Hintergrund mitgeteilt hatte. Die Betroffene hatte zwar ein Ermittlungsverfahren wegen Fahrens ohne Fahrerlaubnis angegeben, war ihres Wissens in dem eingestellten Verfahren jedoch nur als Zeugin vernommen worden und hatte es deshalb bei der Bewerbung nicht angegeben.

Die Bearbeitung der Eingabe der Petentin gestaltete sich sehr schwierig, weil die Datenspeicherungen über ihre Person bereits vor längerer Zeit gelöscht worden waren. Die Datenübermittlung an die Einstellungsbehörde ließ sich daher auch nicht vollständig aufklären, obwohl das von uns um Unterstützung gebetene Polizeipräsidium der Sache mit Beharrlichkeit und Engagement nachging.

Zur Sachverhaltsaufklärung wurde der aktuelle Bestand des Polizeilichen Auskunftssystems Strafsachen (PASS), der aktuelle Landesbestand des Informationssystems der Polizeien des Bundes und der Länder (INPOL Land), die PASS-Protokolldateien über den Zeitraum der Bearbeitung der Bewerbung der Petentin geprüft und die staatsanwaltlichen Ermittlungsakten angefordert sowie die mit der Bewerbung befassten Polizeidienststellen befragt. Im Ergebnis der Recherchen zeigte sich, dass die Petentin zu diesem Zeitpunkt weder in PASS noch in INPOL Land erfasst war und dass es ausweislich der PASS-Protokolldatei während des Bearbeitungszeitraums ihrer Bewerbung nur eine Abfrage mit den Identdaten durch einen Polizeibeamten ihrer Heimatgemeinde gegeben habe, die jedoch ohne Treffer geblieben war.

Die Einstellungsbehörde gab zum Sachverhalt an, dass ihr von der befragten Dienststelle telefonisch mitgeteilt worden sei, dass zu dem angegebenen Ermittlungsverfahren wegen Fahrens ohne Fahrerlaubnis keine Daten mehr gespeichert seien. Allerdings sei ein weiteres Ermittlungsverfahren wegen Sachbeschädigung unter Verwendung von Kennzeichen verfassungswidriger Organisationen anhängig gewesen. Da auch das staatsanwaltliche Aktenzeichen genannt wurde, hat die Polizei die Ermittlungsakte von der Staatsanwaltschaft angefordert. Die Staatsanwaltschaft konnte lediglich bestätigen, dass ein Verfahren gegen die Petentin eingestellt worden war. Die Akte war zum Zeitpunkt der Anfrage bereits vernichtet, sodass eine Auskunft zu deren Inhalt nicht mehr erfolgen konnte.

Es ließ sich somit nicht mehr feststellen, woher der mit dem Vorgang betraute Polizeibeamte zum Zeitpunkt der Anfrage der Einstellungsstelle das staatsanwaltliche Aktenzeichen hatte und aufgrund welcher Datenspeicherungen oder Information er den darunter abgelegten Tatvorwurf mit der Petentin in Verbindung bringen konnte.

Gem. § 39 Abs. 2 Brandenburgisches Polizeigesetz darf die Polizei die im Rahmen von strafrechtlichen Ermittlungen erlangten Daten auch zur Gefahrenabwehr verarbeiten und an andere Stellen übermitteln. Sie sind zu löschen, wenn der Verdacht der Straftat gegen den Betroffenen entfallen ist und die Daten zur polizeilichen Aufgabenerfüllung nicht mehr erforderlich sind. Dass der Anfangsverdacht zur Eröffnung der Hauptverhandlung nicht ausreicht und die Staatsanwaltschaft das Verfahren daher gem. § 170 Abs. 2 Strafprozessordnung einstellt, bedeutet allerdings nicht, dass damit auch der „polizeiliche Verdacht“ aufgehoben ist und die Daten zu löschen sind. Vielmehr darf die Polizei die Daten nach Prüfung weiter aufbewahren und nutzen – bei Jugendlichen höchstens fünf Jahre lang, gerechnet vom Zeitpunkt der Tat.

Mit Einwilligung des Betroffenen ist die Übermittlung der Daten an andere Polizeidienststellen im Rahmen eines Bewerbungsverfahrens nur innerhalb der gesetzlichen Aufbewahrungsfrist zulässig. Da die Frist abgelaufen und die Daten bereits gelöscht worden waren, war es deshalb unrechtmäßig, der Einstellungsbehörde das Ermittlungsverfahren mitzuteilen, auch wenn der Auskunft erteilende Beamte sich daran einschließlich des staatsanwaltlichen Aktenzeichens erinnerte. Schon gar nicht hätte die Mitteilung telefonisch erfolgen dürfen.

Zwar haben wir die zuständige Polizeidienststelle über diesen datenschutzrechtlichen Mangel informiert, von einer förmlichen Beanstandung aufgrund des letztlich nicht mehr aufzuklärenden Sachverhalts jedoch abgesehen. Des Weiteren haben wir angeregt, in vergleichbaren Fällen künftig nur schriftliche

Auskunftsersuchen entgegen zu nehmen bzw. solche Ersuchen zumindest nur schriftlich zu beantworten. Sie sollten nur durch eine der Dienststellenleitung direkt unterstellte Kraft bearbeitet werden, die auch die schriftlichen Unterlagen führt. Diese sind nach Ablauf des auf den Bearbeitungsabschluss folgenden Kalenderjahres zu vernichten. Das Verfahren ist durch eine interne Anweisung bekannt zu gegeben.

Die betroffene Polizeidienststelle hat den Sachverhalt mit ihren Mitarbeitern ausgewertet, unsere Vorschläge zur Bearbeitung der Leumundsanfragen im Rahmen der Bewerbungen übernommen und in einer Hausverfügung umgesetzt.

Die Nutzung polizeilicher Daten im Rahmen des Einstellungsverfahrens ist zulässig, wenn der Bewerber eingewilligt hat. Dazu dürfen die eigenen Datenbestände genutzt sowie Anfragen bei den Polizeibehörden anderer Bundesländer gestellt bzw. beantwortet werden. Daten, deren gesetzliche Aufbewahrungsfrist abgelaufen ist, dürfen nicht mehr mitgeteilt werden.

5.4.3 Kontrolle von Dienstzimmer und E-Mail-Korrespondenz bei Verdacht illoyalen Verhaltens eines Angestellten

Im Rahmen arbeitsrechtlicher Maßnahmen sind in einem Ministerium dienstliche und private Unterlagen mit personenbezogenen Daten teilweise ohne Anwesenheit des betroffenen Angestellten aus seinem Dienstzimmer verbracht sowie dessen Dienst-PC und der E-Mail-Verkehr kontrolliert worden.

Die Maßnahmen erfolgten im Zusammenhang mit den Untersuchungen gegen einen Mitarbeiter wegen des Verdachts der Weitergabe dienstlicher Informationen an Dritte und unerlaubter Nebentätigkeit.

Das Verbringen der Unterlagen aus dem Dienstzimmer des betroffenen Mitarbeiters war gemäß § 29 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) zulässig. Nach dieser Vorschrift dürfen Daten von Beschäftigten verarbeitet werden, wenn dies zur Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses oder zur Durchführung personeller Maßnahmen erforderlich ist. Die Mitnahme war erforderlich, um arbeitsrechtliche Verstöße belegen und beweisen zu können. Bei der Frage, welche Unterlagen als Beweismittel genutzt werden, muss der Arbeitgeber allerdings den Grundsatz der Verhältnismäßigkeit beachten. So hätten wir erhebliche Bedenken, wenn offensichtlich private Unterlagen mitgenommen und im Rahmen der arbeitsrechtlichen Prüfung genutzt worden wären. Das Ministerium hatte sich aber auf solche Dokumente beschränkt, die grundsätzlich dazu

geeignet waren, die Vorwürfe zu belegen und nicht ohne weiteres der privaten Sphäre des Betroffenen zugerechnet werden konnten.

Allerdings halten wir das Vorgehen des Ministeriums insoweit für datenschutzrechtlich bedenklich, als der Betroffene bei der Verbringung der Unterlagen nicht anwesend war, die Erhebung der Daten ohne seine Kenntnis erfolgte und auch seitens der Personalvertretung niemand hinzugezogen wurde. § 12 Abs. 2 Satz 1 BbgDSG verlangt, dass personenbezogene Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben sind. Nur ausnahmsweise ist eine Erhebung ohne Kenntnis des Betroffenen statthaft. Auch teilte man ihm keine Übersicht der mitgenommenen Unterlagen mit.

Dennoch führt diese rechtlich zumindest fragwürdige Datenerhebung nicht zu einem Verwertungsverbot, da die Datenerhebung und anschließende -nutzung für die Durchführung der arbeitsrechtlichen Prüfung nach § 29 BbgDSG erforderlich und damit prinzipiell rechtmäßig war. Ein generelles Verwertungsverbot sieht das Datenschutzrecht nicht vor. Der Betroffene hat lediglich den Anspruch, Unterlagen zurückzuerhalten, die für die arbeitsrechtliche Entscheidung nicht bzw. nicht mehr benötigt werden. Dies gilt bereits vor Abschluss des Verfahrens auch für solche Unterlagen, bei denen sich herausstellt, dass sie für dessen Durchführung nicht mehr erforderlich sind.

Auch gegen die erfolgte Auswertung der E-Mails im Rahmen eines arbeitsrechtlichen Verfahrens durch den Arbeitgeber bestehen keine datenschutzrechtlichen Bedenken, wenn deren Versand ausschließlich für dienstliche Zwecke erlaubt war. Anders wäre dies nur dann zu bewerten, wenn die private Kommunikation mittels E-Mail vom Arbeitgeber erlaubt oder geduldet worden wäre, da dann der Arbeitgeber als Anbieter von Telekommunikationsdiensten den Bindungen des Fernmeldegeheimnisses unterliegt und er (private) Mails nicht beliebig kontrollieren darf. Eine Überprüfung eines E-Mail-Postfachs aus Anlass einer konkreten arbeitsrechtlichen Prüfung ist jedoch zulässig, wenn es gerade Zweck der Maßnahme ist, die Einhaltung des Verbots der privaten Nutzung von ausschließlich zu dienstlichen Zwecken überlassenen Gerätschaften durchzuführen.

Um arbeitsrechtliche Verstöße belegen und beweisen zu können, darf der Arbeitgeber Unterlagen aus dem Dienstzimmer eines Beschäftigten verbringen. Unterlagen, die offensichtlich dessen Privat- und Intimsphäre betreffen, gehen den Arbeitgeber dagegen nichts an.

5.4.4 Rechtssicherer Einsatz von Spamfiltern

Den durch die E-Mail möglichen unkomplizierten Versand von Nachrichten an einen beliebig großen Empfängerkreis machen sich zum Ärger vieler Nutzer auch Versender unverlangter Werbung (Spam) in einem ungeheuren Ausmaß zunutze. Damit wächst das Bedürfnis, diese Nachrichten möglichst frühzeitig, aber auch datenschutzgerecht herauszufiltern.

Der Anteil von Spam an der gesamten E-Mail-Kommunikation liegt derzeit bei über 80 Prozent. Dies bleibt vielen Nutzern des Landesverwaltungsnetzes verborgen, da der Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben wie auch andere IT-Dienstleister mit hohem Aufwand einen großen Teil dieser Nachrichten herausfiltern.

Für die Filterung unverlangter Nachrichten wird in der Regel ein Mix aus verschiedenen technischen Möglichkeiten eingesetzt, um einerseits möglichst viele Spam-Nachrichten auszusondern und andererseits alle erwünschten Nachrichten dem Empfänger zuzustellen. Der größte Teil des Spam-Aufkommens wird bereits durch den Einsatz so genannter Blacklisting- und Greylisting-Verfahren erkannt, bei denen E-Mails aufgrund der Adressinformationen generell vom Weitertransport ausgeschlossen werden. Ein viel kleinerer Teil unverlangter Werbung wird durch so genannte Content-Filter-Systeme, die eine automatisierte Prüfung des Inhalts selbst vornehmen, einer weiteren Filterung unterzogen. Als Resultat dieser inhaltlichen Prüfung können die Nachrichten automatisch in einen gesonderten Ordner verschoben oder auch gelöscht werden.

Automatisierte Systeme zum Abweisen oder Filtern unverlangter E-Mails greifen in die persönliche Kommunikation des Nutzers ein und sind deshalb auch datenschutzrechtlich relevant. Zudem ist die E-Mail-Kommunikation durch das Fernmeldegeheimnis geschützt. Der Einsatz von Spamfiltern kann selbst dann einen Eingriff in das Fernmeldegeheimnis bedeuten, wenn die Filter ohne jeden menschlichen Zugriff automatisiert arbeiten. Bei der Konzeption der Filterung von Spam sollte daher von vornherein Wert darauf gelegt werden, dass diese möglichst an einem Punkt ansetzt, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.

Ist die Nutzung dienstlicher E-Mail-Anschlüsse bei öffentlichen Stellen ausschließlich zu dienstlichen Zwecken erlaubt, endet das Fernmeldegeheimnis bereits mit Empfang der E-Mails auf dem Mailserver. In dieser Konstellation ist der Einsatz von Spamfiltern ohne Einwilligung grundsätzlich akzeptabel. Beim Einsatz von Content-Filtern ist die Markierung der spamverdächtigen Nachrichten der zentralen Löschung vorzuziehen, da dem Empfänger die

Möglichkeit erhalten bleibt, selbst über den Umgang mit den Nachrichten zu entscheiden.

Rechtlich unsicherer ist die Lage, wenn auch die private Nutzung des dienstlichen E-Mail-Anschlusses erlaubt wird. Das Fernmeldegeheimnis endet bei der privaten Kommunikation nämlich erst, wenn der Empfänger die vollständige Verfügungsgewalt über die eingegangene E-Mail erlangt hat. Damit ist jede Filterung, die auf der Prüfung von Adressinformationen oder des Inhaltes beruht, als Eingriff in das Fernmeldegeheimnis anzusehen. Bei erlaubter privater Nutzung dürfen Filter deshalb nur mit Einwilligung der Beschäftigten zum Einsatz kommen. Diese kann zusammen mit der Kenntnisnahme und Zustimmung zu den Nutzungsbedingungen eingeholt werden. Ausgehend davon, dass ein Empfänger bestimmen kann, was mit der an ihn gerichteten Post passieren soll, halten wir eine Einwilligung des Absenders für entbehrlich. Wird auf die Einwilligung ganz verzichtet, besteht für den Arbeitgeber das Risiko einer strafbaren Verletzung des Fernmeldegeheimnisses oder der strafbaren Datenveränderung.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf Vorschlag der Landesbeauftragten als Vorsitzender des Arbeitskreises Medien die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz um Empfehlungen zum Einsatz von Spamfiltern ergänzt.[58]

Bei der Konzeption eines Spamfilters sollten öffentliche Stellen dafür Sorge tragen, dass die automatische Prüfung von Adressen oder Inhalt elektronischer Post auf unerwünschte Nachrichten erst an einem Punkt erfolgt, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt. Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten selbst über den Umgang mit den an sie gerichteten E-Mails entscheiden können. Bei erlaubter privater Nutzung des dienstlichen E-Mail-Anschlusses ist zusätzlich eine Einwilligung in die Filterung der Nachrichten einzuholen.

5.4.5 PERIS adé? Pilotprojekt Integrierte Personal- und Stellenverwaltung

Im Februar 2006 wurden wir durch das Ministerium des Innern als Projektleitung über das Projekt iPSv – Integrierte Personal- und Stellenverwaltung – unterrichtet. Ziel des Projekts war es, in drei ausgewählten Pilotbereichen der Landesverwaltung (Staatskanzlei, Ministerium für Infrastruktur und Raumordnung, Landesbetrieb Straßenwesen) ein neues

[58] siehe Anlage 5

DV-System zur Personal- und Stellenverwaltung einzuführen. Darüber hinaus sollte ein Referenzmodell für die landesweite Nutzung des Verfahrens und damit für die mittelfristige Ablösung des aktuellen Personalinformationssystems PERIS erarbeitet werden.

Entsprechend der Ausschreibung des Projekts sollte das iPSv-System zum bereits existierenden, unter der Verantwortung des Ministeriums der Finanzen betriebenen System der Kosten- und Leistungsrechnung (KLR) bzw. des Neuen Finanzmanagements (NFM) kompatibel und mit diesem interoperabel sein. Wegen der Festlegung, im Bereich KLR/NFM ein SAP-System[59] mit den entsprechenden Modulen zu nutzen, entschied sich die iPSv-Projektleitung ebenfalls für SAP R/3 als technische Basis. Für die Zwecke der Personalverwaltung sollte das SAP-Modul HR/HCM (Human Resources/Human Capital Management) zum Einsatz kommen. Die Entscheidung für ein SAP R/3-System reflektiert auch das Ziel in der IT-Strategie des Landes, ein einheitliches ERP-System (Enterprise Resource Planning) für die gesamte Landesverwaltung anzustreben.

Bereits frühzeitig, stellten wir gegenüber der Projektleitung und den drei Pilotbehörden die wesentlichen Anforderungen bezüglich Datenschutz und IT-Sicherheit für die Realisierung des Systems dar. Dabei erörterten wir sowohl rechtliche als auch technisch-organisatorische Aspekte. Aus rechtlicher Sicht enthält das Beamtengesetz des Landes Brandenburg strenge Vorgaben zur Einschränkung des Zugriffs auf Personalaktendaten und zur Zweckbindung der Daten ausschließlich für die Personalverwaltung und Personalwirtschaft. Insbesondere ist festgelegt, dass nur Beschäftigte, die mit der Bearbeitung von Personalangelegenheiten betraut sind, Zugang zu den Daten haben dürfen. Das Brandenburgische Datenschutzgesetz fordert darüber hinaus, die Datenverarbeitung so zu organisieren, dass eine Trennung nach den verfolgten Zwecken und unterschiedlichen Betroffenen möglich ist.

Aus technischer Sicht ist zu beachten, dass die in iPSv verarbeiteten Personaldaten einen hohen Schutzbedarf bezüglich der Schutzziele Vertraulichkeit und Integrität haben. Mehrfach wiesen wir die Projektvertreter darauf hin, dass die konkreten technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und IT-Sicherheit in einem projektspezifischen Sicherheitskonzept umfassend darzulegen sind. Die Sicherheitsmaßnahmen sind dabei ausgehend von einer detaillierten Analyse der möglichen Risiken der Datenverarbeitung in iPSv zu bestimmen. Sie müssen sowohl dem hohen Schutzbedarf der Daten gerecht werden als auch dem aktuellen Stand der Technik entsprechen. Aus unserer Sicht war auch klar, dass das in

[59] vgl. A 9.3

iPSv erreichte Sicherheitsniveau nicht hinter dem Niveau des Altverfahrens PERIS zurückbleiben durfte. Unter Beachtung der Weiterentwicklung des Standes der Technik sollte es sogar höher sein.

Das endgültige Sicherheitskonzept für das iPSv-Verfahren wurde uns im Dezember 2006 durch die Projektleitung zur Prüfung übergeben. Kritikpunkte, die wir bereits zu Entwürfen und Vorversionen dieses Konzepts geäußert hatten, wurden in der endgültigen Version leider nur zum Teil berücksichtigt. In unserer Stellungnahme kamen wir zu dem Schluss, dass ein datenschutzgerechter Betrieb auf Basis dieses Sicherheitskonzepts nicht möglich war. Dabei berücksichtigten wir auch den Pilot- und Referenzcharakter des Projekts für die Personalverwaltung in allen Landesbehörden. Zu den gravierendsten Mängeln zählten folgende Punkte:

- keine durchgängige Berücksichtigung des hohen Schutzbedarfs der Personaldaten bei der Ableitung von Sicherheitsmaßnahmen im iPSv-Verfahren,

- fehlende Ende-zu-Ende-Verschlüsselung von Personaldaten bei ihrer Übertragung über Netzwerke,

- keine verschlüsselte Speicherung sensitiver Daten in der Datenbank,

- zu weit gehende Zugriffsmöglichkeiten für das Administrationspersonal,

- unzureichende Trennung der Datenbestände nach Betroffenengruppen; statt dessen befinden sich die Personaldaten aller Beschäftigten unverschlüsselt in derselben Datenbank,

- unzureichende Aussagen über Sicherheitsmaßnahmen auf der Ebene des Betriebssystems und der Datenbank,

- unzureichende oder widersprüchliche Aussagen zur Konfiguration des SAP-Systems sowie zum Umgang mit SAP-Sondernutzern und Berechtigungen für kritische Transaktionen,

- fehlende Vorstellungen zur Berücksichtigung der Rechte der betroffenen Beschäftigten.

Von besonderer Bedeutung ist, dass mit der fehlenden Ende-zu-Ende-Verschlüsselung und dem Verzicht auf eine verschlüsselte Datenspeicherung nicht nur Sicherheitsmaßnahmen des Altverfahrens PERIS nicht berücksichtigt oder durch vergleichbare Maßnahmen ersetzt wurden, sondern auch wesentliche Anforderungen der Ausschreibung des iPSv-Projekts nicht erfüllt

wurden. Dort waren die genannten beiden Punkte als Kriterien formuliert, deren Nichtbeachtung zum Ausschluss des jeweiligen Bieters führen sollte.

Zu berücksichtigen war auch die Absicht, den Betrieb des Verfahrens für alle Behörden bei einem externen Dienstleister zu zentralisieren – nach damaligen Vorstellungen der Projektleitung beim Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben, zukünftig evtl. bei einem privaten Dienstleister.[60] Vor diesem Hintergrund kommt der Abschottung und Verschlüsselung der Datenbestände sowie der zuverlässigen Verhinderung unberechtigter Zugriffe auf die Daten z. B. durch Administratoren eine besondere Bedeutung zu.

Unsere Kritikpunkte zu dem von der Projektleitung vorgelegten iPSv-Sicherheitskonzept wurden im Februar 2007 auf einem Workshop an der Universität Potsdam unter Einbeziehung eines externen Moderators sehr kontrovers diskutiert. An dem Workshop waren neben den Projektverantwortlichen auch die Personalräte der Pilotbehörden, der Projektdienstleister sowie der zukünftige Betreiber des Verfahrens beteiligt. Im Ergebnis der Diskussion wurde das Sicherheitskonzept überarbeitet, dabei jedoch nur einige der oben genannten Mängel beseitigt. Insbesondere blieb auch in der überarbeiteten Version unsere Kritik an der mangelnden Abschottung und Verschlüsselung der Datenbestände sowie der Möglichkeit unberechtigter Datenzugriffe bestehen.

Im April 2007 wurde uns von der Projektleitung mitgeteilt, dass das Ministerium des Innern auf der Basis des neuen Sicherheitskonzepts zwar die Freigabe des Verfahrens erteilt habe, es jedoch u. a. wegen der fehlenden Zustimmung der Personalräte der Pilotbehörden nicht zur Produktivsetzung käme. Im Juni 2007 erreichte uns dann die Nachricht von der vorläufigen Einstellung des Projekts.

An Verfahren zur Personaldatenverarbeitung sind auf Grund der hohen Sensitivität der Daten besonders hohe Anforderungen an Datenschutz und IT-Sicherheit zu stellen. Bei der Modernisierung eines bestehenden Verfahrens darf sich das Sicherheitsniveau nicht verschlechtern. Die Sicherheitsmaßnahmen müssen stets sowohl dem hohen Schutzbedarf der Daten als auch dem aktuellen Stand der Technik entsprechen.

[60] vgl. A 5.3.1 und A 9.4

6 Bildung, Jugend und Sport

6.1 „Kinderschutz und Datenschutz“ – Beratung der Jugendämter

Bereits im Oktober 2005 haben der Bildungsminister und die Sozialministerin die Landesbeauftragte gebeten, eine Broschüre zu den datenschutzrechtlichen Aspekten des Kinderschutzes zu erstellen. Gemeinsames Ziel war es, den Jugendämtern eine Hilfestellung bei konkreten Schwierigkeiten mit der Datenübermittlung im Falle eines Verdachts auf Kindeswohlgefährdungen zu geben.

Um diese Schwierigkeiten konkret benennen und in der zu erstellenden Broschüre Lösungsmöglichkeiten aufzeigen zu können, baten wir sämtliche Jugendämter des Landes um Zusendung anonymisierter Fälle. Von den insgesamt 18 Behörden erhielten wir neun Rückmeldungen: Nur drei stellten uns die erbetenen Informationen zur Verfügung, während die übrigen erklärten, keine konkreten Probleme zu haben. Der Staatssekretär des Ministeriums für Bildung, Jugend und Sport erläuterte, dass es schwierig sei, immer wiederkehrende Fallgestaltungen zu finden. Auch habe das Ministerium keine Informationen über generelle datenschutzrechtliche Schwierigkeiten der Jugendämter. Es erhalte allenfalls durch Bürger, die sich unmittelbar beim Minister beschweren, Kenntnis von Einzelfällen.

Am Beratungsbedarf der Jugendämter, der durch vermehrte Anfragen nach wie vor an uns herangetragen wird, änderte dies nichts. Da offenbar die praktischen Fallgestaltungen in jedem Einzelfall unterschiedlich sind, mussten wir von der Erstellung einer naturgemäß zu theoretischen Broschüre absehen. Stattdessen wurde zwischen der Landesbeauftragten und dem Bildungsministerium vereinbart, Fortbildungsveranstaltungen stärker für Informationen zum Datenschutz zu nutzen. Ein von der Landesbeauftragten zu entwickelnder Baustein „Datenschutz im Kinderschutz“ soll es nun ermöglichen, auch konkrete Praxisprobleme zu erörtern. Im Ergebnis dieser Vereinbarung hat die Landesbeauftragten den Umgang der Jugendämter mit personenbezogenen Daten auf Fortbildungsveranstaltungen erläutert. Im Rahmen des elften Jugendhilfetages in Frankfurt (Oder) erhielten wir schließlich die Gelegenheit zum Thema „Spannungsfeld zwischen Datenschutz- und Kinderschutzinteressen“ zu referieren. Die sich anschließende Diskussion zeigte, dass es in der Praxis vor allem um Unsicherheiten bei der Umsetzung der datenschutzrechtlichen Vorschriften geht. Werden diese eingehalten, nutzt der Datenschutz auch dem Schutz der Kinder.

Da die Erstellung einer Broschüre zum Thema „Datenschutz und Kinderschutz“ vor allem aus Darstellungsgründen nicht zu Stande gekommen ist, bemüht sich die Landesbeauftragte nunmehr vermehrt durch Fortbildungsveranstaltungen um eine Beratung der Jugendämter.

6.2 Schweigepflicht der Erziehungsberatungsstellen

Ist die Verpflichtung der Träger einer Beratungsstelle, gegenüber dem Jugendamt Privatgeheimnisse offen zu legen, mit der Schweigepflicht ihrer Mitarbeiter vereinbar?

Nach § 8a Abs. 2 Sozialgesetzbuch Achtes Buch (SGB VIII) verpflichtet sich der Träger der freien Jugendhilfe, einen eigentlich dem Jugendamt obliegenden Schutzauftrag wahrzunehmen. Dies bedeutet, dass die Erziehungsberatungsstellen mit dem Jugendamt Vereinbarungen treffen sollen, in der sie sich dazu verpflichten, dieses über Kindeswohlgefährdungen zu informieren, insbesondere auch für den Fall, dass die den Eltern angebotene Hilfe nicht ausreichend erscheint bzw. sie nicht angenommen wird. Fraglich ist, inwieweit in dieser Offenlegung von Sozialdaten gegenüber dem Jugendamt eine „gesetzliche Anzeigepflicht“ zu sehen ist.

Bei der Weitergabebefugnis der Erziehungsberatungsstellen ist zwischen den in allgemeiner Erfüllung der dienstlichen Aufgaben bekannt gewordenen und somit nicht besonders anvertrauten Daten gemäß § 64 SGB VIII und den – etwa in einem besonderen Vertrauens- und Beratungsverhältnis – ausdrücklich anvertrauten Daten gemäß § 65 SGB VIII zu unterscheiden.

§ 64 Abs. 2 SGB VIII konkretisiert § 69 Abs. 1 (Nr. 1 Alt. 2) Sozialgesetzbuch Zehntes Buch (SGB X) für den Bereich der öffentlichen Jugendhilfe dahingehend, dass eine Übermittlung von nicht ausdrücklich anvertrauten Sozialdaten zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch möglich ist, „soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird“. Werden dagegen vertrauliche Daten von einer Person übermittelt, die der Schweigepflicht nach § 203 Abs. 1 Strafgesetzbuch (StGB) unterliegt, kann dies nach § 35 Sozialgesetzbuch Erstes Buch (SGB I) zulässig sein. Die Voraussetzungen sind hier enger. Es bedarf einer besonderen Risikoabwägung, nach der eine Weitergabe der Informationen nur dann erlaubt ist, wenn eine erhebliche Gefahr der (zukünftigen) Verletzung von Rechtsgütern (Dritter) besteht.

Die Übermittlung von Sozialdaten durch freie Träger der Jugendhilfe an das Jugendamt ist gemäß § 8a SGB VIII bei Vorliegen gewichtiger Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen zulässig. Diese Rechtsgrundlage erlaubt das Durchbrechen der durch § 203 StGB geschützten Schweigepflicht.

6.3 Datenschutz im Unterricht – ein Schulprojekt für Kinder und Jugendliche

Zwar stellt das Bearbeiten von Anfragen und Eingaben einen wichtigen Teil unserer Tätigkeit dar. Eine frühzeitige Sensibilisierung für den Datenschutz kann jedoch dazu beitragen, dass es gar nicht erst zu Beschwerden kommt. Wir haben deshalb ein Projekt auf den Weg gebracht, um den Datenschutz als Unterrichtsbestandteil an den Schulen zu etablieren.

Mit dem Schulprojekt „Datenschutz für Lehrer und Schüler“ haben wir gemeinsam mit dem Ministerium des Innern Lehrmaterial erstellt, das die Schüler an Beispielen aus ihrem täglichen Leben auf datenschutzrechtliche Anliegen aufmerksam macht. Ziel ist, ihnen zu vermitteln, dass sowohl die eigenen Persönlichkeitsrechte als auch die anderer schutzwürdig sind. Das als Handreichung für Lehrer erstellte Material soll helfen, dies in anschaulicher und altersgerechter Form im regulären Unterricht zu vermitteln.

Schwerpunkte des Projekts sind Themen wie Mobiltelefonie und Internet. Das Material zeigt, wie personenbezogene Daten in diesen Kommunikationsmedien verbreitet werden und welche Konsequenzen der sorglose Umgang mit ihnen für den Einzelnen hat. Die Schüler erfahren schließlich auch, wie man sich gegen das ungewollte Verbreiten seiner eigenen Daten und somit gegen deren Missbrauch schützen kann. Die Unterrichtsvorschläge befassen sich auch mit der Datenverarbeitung bei Gewinnspielen, mit den Kundenkarten von Handelsunternehmen oder mit Fragen zur ärztlichen Schweigepflicht.

Wir bieten einzelne Module zu diesen Themen an, um den Lehrkräften eine flexible Unterrichtsgestaltung zu ermöglichen. Das Schulprojekt haben wir bereits in ausgewählten Schulen vorgestellt. Es ist im Januar 2008 anlässlich des Zweiten Europäischen Datenschutztages der Öffentlichkeit präsentiert worden. Interessierte können sich das Material von unserer Website herunterladen. Gerne versenden wir die Handreichung auch auf CD-ROM.

Ein Bewusstsein für die Gefährdungen der eigenen Persönlichkeitsrechte beim Umgang mit modernen Medien und Kommunikationsmitteln sollte Kindern und Jugendlichen bereits in der Schule vermittelt werden. Das Schulprojekt der Landesbeauftragten leistet hierzu einen Beitrag.

6.4 Neuerungen im Schulgesetz und in der Schulstatistik

Nach einer fast zwei Jahre währenden Beratung ist das neue Brandenburgische Schulgesetz[61] in Kraft getreten. Unter anderem wurde darin die Grundlage für eine Änderung der Schulstatistik gelegt.

Von datenschutzrechtlicher Bedeutung ist die neue Vorschrift des § 4 Abs. 3 Sätze 2 und 3 Brandenburgisches Schulgesetz (BbgSchulG). Danach sind die Schulen ausdrücklich aufgefordert, zur Wahrung des Wohls von Kindern und Jugendlichen jedem Anhaltspunkt für Vernachlässigung oder Misshandlung nachzugehen, wobei die Schulen selbstständig über die Einbeziehung des Jugendamtes oder anderer Stellen entscheiden.

§ 46 Abs. 4 BbgSchulG stellt nunmehr klar, dass Eltern volljähriger Schüler Auskünfte über persönliche schulische Angelegenheiten – insbesondere zum Leistungsstand – nur mit Einwilligung der Schüler zu erteilen sind. Die Schüler müssen angehört und darauf hingewiesen werden, dass sie das Recht haben, die Einwilligung zu verweigern. Diese Regelung trägt dem Umstand Rechnung, dass die Eltern mit Eintritt der Volljährigkeit ihrer Kinder kein Sorgerecht mehr über sie haben. Andererseits berücksichtigt das Brandenburgische Schulgesetz auch, dass Kinder trotz Volljährigkeit in ihrem Verhältnis zu den Eltern nicht als Fremde zu betrachten sind. Nach § 46 Abs. 5 BbgSchulG wird den Schulen die Möglichkeit eröffnet, die Eltern volljähriger Schüler auch ohne deren Einwilligung über wichtige persönliche und schulische Angelegenheiten zu informieren. Hierzu zählen beispielsweise die Verweisung von der Schule bei schwerwiegendem Fehlverhalten, die Androhung oder Verhängung einer schweren Ordnungsmaßnahme oder lang anhaltende unentschuldigte Fehlzeiten sowie die (vorzeitige) Beendigung des Schulverhältnisses.

Schließlich ist die Regelung zu wissenschaftlichen Untersuchungen des § 66 BbgSchulG geändert worden. Neu ist, dass bei Bestehen eines öffentlichen Interesses an der Durchführung des Forschungsvorhabens auch Ton- und Bildaufzeichnungen von Schülern ohne Einwilligung durchgeführt werden können. Deren wissenschaftliche Erforderlichkeit ist gesondert zu begründen. Selbstverständlich dürfen solche Aufzeichnungen nur offen erfolgen; verdeckte Aufnahmen mit dem Ziel, von der Kamera unbeeinflusstes Verhalten einfangen zu wollen, bleiben weiterhin tabu.

Die Kultusministerkonferenz hat beschlossen, durch die Änderung der Schulstatistik die Schulbesuchsverläufe einzelner Schüler zu erheben und einen

[61] Gesetz zur Änderung des Brandenburgischen Schulgesetzes und weiterer Rechtsvorschriften vom 8. Januar 2007 (GVBl. I S. 2)

entsprechenden bundeseinheitlichen Kerndatensatz einzuführen. Für dieses Vorhaben wäre es erforderlich, Daten zu verarbeiten, die über die bisherige Datenerhebung im Rahmen der Schulstatistik hinausgeht. Hierfür fehlte in Brandenburg zunächst eine Rechtsgrundlage. Beispielsweise bedarf es einer solchen zur Übermittlung von Einzeldatensätzen aus dem Verwaltungsvollzug an den Landesbetrieb für Datenverarbeitung und Statistik, der für das Führen der Statistik verantwortlich ist. Wir haben gefordert, das Brandenburgische Schulgesetz entsprechend zu ergänzen. Entweder muss das Schulgesetz oder eine auf diesem basierende Rechtsverordnung festlegen, welche statistischen Daten über schul- und ausbildungsbezogene Tatbestände zu erheben sind. Außerdem ist sicherzustellen, dass Daten, die zu statistischen Zwecken erhoben wurden, lediglich in anonymisierter Form weiterzugeben sind. Entsprechend dem Brandenburgischen Statistikgesetz dürfen sie nicht reanonymisiert, d. h. konkreten Personen zugeordnet werden.

Nachdem unsere Anregung zunächst nicht in das novellierte Brandenburgische Schulgesetz eingeflossen war, griff das Ministerium für Bildung, Jugend und Sport die Gelegenheit später jedoch auf. Der Gesetzgeber verabschiedete schließlich eine entsprechende Regelung im Zusammenhang mit dem durch ein Artikelgesetz geänderten Brandenburgischen Datenschutzgesetz. Artikel 4 dieses Gesetzes[62] fügt nun den neuen § 65a über eine automatisierte zentrale Schülerdatei und Schülerlaufbahnstatistiken in das Schulgesetz ein. Mit der automatisierten zentralen Schülerdatei wird die Kontrolle der Schulpflichterfüllung, sowie die Kontrolle der Teilnahme an schulärztlichen Untersuchungen und an den gesetzlich geregelten Sprachstandsfeststellungen erleichtert. Sie ermöglicht außerdem die Speicherung individueller schulischer Bildungsverläufe für Zwecke der Schulaufsicht. Einzelheiten sind in einer Rechtsverordnung des Ministeriums zu regeln.

Die Lehrer haben jedem Anhaltspunkt für Vernachlässigung oder Misshandlung ihrer Schüler nachzugehen und nach Bedarf das Jugendamt oder andere Fachstellen einzuschalten. Eltern erhalten in der Regel nur Auskünfte zum Leistungsstand ihrer volljährigen Kinder, wenn diese eingewilligt haben. Ton- und Bildaufzeichnungen von Schülern sind möglich, wenn die wissenschaftliche Erforderlichkeit begründet wird. Eine landeseindeutige Schülernummer wird eingeführt, um individuelle schulische Bildungsverläufe statistisch zu erfassen. Abwesenheitsdaten der Schüler werden zwecks Durchsetzung der Schulpflicht künftig an zentraler Stelle verarbeitet.

[62] Drittes Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 30. November 2007 (GVBl. I S. 193)

6.5 Weiterreichen von Gutachten bei der Bewerbung für eine Begabungsklasse

Ein Schüler wollte in eine Leistungs- und Begabtenklasse wechseln. Zu diesem Zweck wählte der Vater ein Gymnasium aus, das die Aufnahme des Kindes nach der Durchführung des Bewerbungsverfahrens jedoch ablehnte. Einen Zweitwunsch hatte er nicht angegeben. Dennoch informierte ihn eine aus seiner Sicht völlig unbeteiligte Schule über die Gründe des Scheiterns der ersten Bewerbung. Woher wusste diese Schule so gut Bescheid?

Das staatliche Schulamt führte Ausgleichskonferenzen durch, weil den Wünschen der Eltern im Aufnahmeverfahren durch die einzelnen Schulen nicht immer entsprochen wurde. Dies betraf sowohl solche Anträge, in denen nur ein einziger Wunsch als auch solche, in denen Erst- und Zweitwunsch angegeben waren. In diesem Zusammenhang wurde auch jenen Eltern, die keine Zweitwunschschule angegeben haben, eine weitere Schule angeboten. Die Ergebnisse der Aufnahmeprüfung einschließlich des prognostischen Tests, die zum Scheitern der Bewerbung an der zunächst gewünschten Schule führten, wurden der Zweitwunschschule übermittelt.

Bei der Bewerbung um einen Platz in einer Leistungs- und Begabungsklasse („Ü-5-Verfahren“) handelt es sich um eine freiwillige Entscheidung der Betroffenen; eine Verpflichtung, solche Klassen zu besuchen, besteht nicht. Das Verfahren unterscheidet sich dadurch wesentlich von dem Wechsel der Schülerinnen und Schüler in die Jahrgangsstufe 7 einer weiterführenden Schule („Ü-7-Verfahren“). Im Rahmen dieses letztgenannten, obligatorischen Verfahrens erhalten auch die Schulen, die nicht als Erst- oder Zweitwunsch aufgeführt wurden, im Rahmen der Ausgleichskonferenzen generell Einsicht in die Bewerbungsunterlagen.

Das Prinzip der Freiwilligkeit einer Bewerbung für eine Leistungs- und Begabungsklasse muss sich auch in der Datenübermittlung widerspiegeln und die Gutachten zur Aufnahmeprüfung nur auf Wunsch der Eltern weitergegeben werden. Nach ausführlicher Beratung durch die Landesbeauftragte hat das Ministerium für Bildung, Jugend und Sport ein standardisiertes Antragsformular entwickelt, das diesen Anforderungen Rechnung trägt. Es differenziert zwischen Erstwunsch, Zweitwunsch und Ausgleichskonferenz und ermöglicht es den Antragstellern, selbst über die Verarbeitung der personenbezogenen Daten in dem jeweiligen Verfahrensschritt zu entscheiden.

Lehnt eine Schule den Antrag auf Aufnahme eines Kindes in eine Leistungs- und Begabungsklasse ab, dürfen die personenbezogenen Ergebnisse der Aufnahmeprüfung nicht ohne Einwilligung der Eltern an eine andere Schule weitergegeben werden.

7 Wissenschaft, Forschung und Kultur

Fotos zur Durchsetzung der Parkordnung in den Gärten der preußischen Schlösser

Von Personen, die Verstöße gegen die Parkordnungen begingen, fertigte die Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg Fotos an, die an das Parkpersonal verteilt werden sollten. Anhand der Bilder, sollten Personen, denen ein Hausverbot erteilt wurde, erkannt werden, um ihnen den Zutritt zu den Anlagen zu verwehren.

Die Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg ist als Ordnungsbehörde für die Durchsetzung der Parkordnung in ihren Gärten verantwortlich. Sie kann Verwarn- und Bußgelder verhängen, um das Verbot des Betretens von Rasenflächen sowie des Radfahrens durchzusetzen. Auch Hausverbote können ausgesprochen werden.

Entgegen anfänglichen Presseberichten hatte die Stiftung von vornherein nicht vor, eine Täterdatei von allen Personen anzulegen, gegen die wegen des Verstoßes gegen die Vorschriften der unterschiedlichen Parkordnungen ein Verwarn- oder Bußgeldverfahren angestrengt wurde. Sie wollte mit Hilfe von Digitalkameras vielmehr die Verstöße dokumentieren oder die Betroffenen nach der Tat bildlich festhalten. Das Bildmaterial sollte im Verfahren als Beweismittel dienen.

Zwar darf die Stiftung als Ordnungsbehörde auch Personalien feststellen, sie hat darüber hinaus aber keine eigenen Zwangsbefugnisse und müsste, wenn sich jemand weigert, seine Personalien anzugeben, die Polizei einschalten. Zum Zweck der Identifizierung einer noch fremden Person ist es somit nicht erforderlich, sie zu fotografieren. Ein Foto, das aber erst nach dem Übertreten der Parkordnungen vom Täter gemacht wird, ist auch als Beweismittel untauglich, da ihm der Bezug zur Ordnungswidrigkeit fehlt. Die Verfolgung solcher Taten kann deshalb nur durch das Stiftungspersonal selbst geschehen. Es muss den Verstoß gegen die Parkordnung feststellen, die betreffende Person ansprechen und ggf. weitere Schritte einleiten. Der Nachweis der vorgeworfenen Tat geschieht dann durch die Aussage des auch als Zeugen fungierenden Stiftungsmitarbeiters. Fotos helfen hier nicht weiter. Sie sind weder erforderlich noch verhältnismäßig und daher rechtwidrig.

Der Umstand der körperlichen Präsenz des Ordnungspersonals vor Ort unterscheidet diese Fälle vom zulässigen Einsatz von auf Videokameras gestützten Überwachungsanlagen. Nach § 33c Abs. 1 Brandenburgisches Datenschutzgesetz können öffentliche Stellen – zu denen auch die Stiftung Preußische Schlösser und Gärten zu zählen ist – mit „optisch-elektronischen Einrichtungen öffentliche zugängliche Räume“ beobachten und bei Vorliegen der übrigen Tatbestandsmerkmale auch Aufzeichnungen herstellen. Die Kamera dient hier quasi als verlängertes Auge der Ordnungskräfte, die im Augenblick der Aufnahme oder Aufzeichnung gerade nicht unmittelbar am Tatort sind. Das Bildmaterial hat im Gegensatz zu dem vorher geschilderten Fall den Zweck, eine Person überhaupt erst einmal zu ermitteln, und ist damit zulässig.

Ungeeignet und damit unzulässig ist es, zur Durchsetzung eines Hausverbots eine Bildkartei anzulegen, mit deren Hilfe der Ordnungsdienst aus dem Kreis der Besucher jene Personen herausfiltern soll, gegen die ein Hausverbot ausgesprochen wurde. Die Zugänge zu den Parkanlagen unterliegen keiner generellen Einlasskontrolle. Das Erkennen einer bestimmten Person bleibt somit dem Zufall überlassen. Außerdem ist die Wahrscheinlichkeit hoch, die falsche Peron anzusprechen und zu einer Überprüfung der Personalien zu zwingen. Auch wäre es jeder mit einem Hausverbot belegten Person ein Leichtes, Ihr äußeres Erscheinungsbild zu verändern und so jede Kontrolle ins Leere laufen zu lassen.

Wir haben vorgeschlagen, auf eine Bilddatei für Hausverbote völlig zu verzichten. Die Personalien sollten vielmehr erst dann festgestellt und mit der Liste derjenigen, gegen die ein Hausverbot ausgesprochen wurde, abgeglichen werden, wenn eine Ordnungswidrigkeit begangen wird. Wird auf diese Weise jemand dabei ertappt, einem Hausverbot zuwiderzuhandeln, kann Strafanzeige wegen Hausfriedensbruchs gestellt werden. Das gesamte Verfahren kommt völlig ohne Fotos aus und birgt auch nicht die Gefahr, unbeteiligte Parkbesucher zu belästigen.

Die Stiftung zeigte sich unseren Vorschlägen weit gehend aufgeschlossen und erklärte, auf Fotos von Personen zu Beweiszwecken zu verzichten und hinsichtlich der Durchsetzung von Hausverboten einen Listenabgleich durchzuführen.

Das Erstellen von Bildmaterial ist häufig nicht geeignet, einen Verstoß gegen die Parkordnung zu beweisen. Ist Personal vor Ort, so reicht dessen Aussage als Zeuge zu Beweiszwecken aus. Hausverbote lassen sich ohne Bildkarteien und aufwändige Gesichtskontrollen durchsetzen.

8 Arbeit, Soziales, Gesundheit und Familie

8.1 Hausbesuch – Immer schön lächeln!

Während des Kontrollbesuchs bei einer Leistungsempfängerin brachte das JobCenter ein Kamerateam des Fernsehens mit. Der Bitte, die Kamera abzuschalten wurde nicht gefolgt. Die Betroffene ließ die Behördenmitarbeiter in ihre Wohnung, die sich erst beim Verlassen der Wohnung als Mitarbeiter des Job-Centers auswiesen. Das Kamerateam wartete noch immer vor der Tür und filmte weiter.

Die gesetzliche Grundlage zur Durchführung von Hausbesuchen zu Kontrollzwecken durch Mitarbeiter eines Sozialleistungsträgers findet sich in § 20 i. V. m. § 21 Abs. 1 Nr. 4 Sozialgesetzbuch Zehntes Buch (SGB X). Nach § 67 SGB X, dürfen allerdings nur die zur Erfüllung der Aufgabe erforderlichen Daten erhoben werden. Unter Beachtung des Grundsatzes der Verhältnismäßigkeit ist daher vor jedem Hausbesuch zu prüfen, ob andere, den Betroffenen weniger belastende Möglichkeiten bestehen, um den Sachverhalt zu klären. Die bloß routinemäßige Durchführung von Hausbesuchen ohne Indizien für das Vorliegen einen Leistungsmissbrauchs zur „Verdachtsfindung“ ist unzulässig. Der im Einzelfall vorliegende Grund für den Hausbesuch ist durch einen Vermerk in der Akte zu dokumentieren. Die Entscheidung, ob ein Hausbesuch durchgeführt wird, sollte der jeweilige Leiter des Trägers der Grundsicherung für Arbeitsuchende treffen.

Die Mitarbeiter des JobCenters haben sich durch die unaufgeforderte Vorlage ihres Dienstausweises zu identifizieren, die Gründe für die Durchführung des Hausbesuchs zu erläutern und die Betroffenen darüber zu belehren, dass diese ihnen den Zutritt zur Wohnung verweigern können. Dies schließt auch die Information über die Folgen der Verweigerung des Zutritts – etwa eine mögliche Leistungskürzung – ein.

Von der Zustimmung zum Betreten der Wohnung ist die Durchsicht der Schränke nicht umfasst. Hierfür bedarf es einer gesonderten Einwilligung. Wird die Zustimmung erteilt, ist lediglich ein kurzer Blick in die Schränke, nicht jedoch ein „Wühlen“ in dessen Inhalt erlaubt.

Bei der Durchführung von Hausbesuchen ist zu beachten, dass von einer Befragung dritter Personen, wie z. B. Nachbarn, Abstand zu nehmen ist. Sozialdaten sind grundsätzlich vorrangig beim Betroffenen zu erheben. Unter Beachtung des Grundsatzes der Verhältnismäßigkeit kann eine Befragung ohne Wissen des Betroffenen allerdings dann unumgänglich sein, wenn eine Sachverhaltsaufklärung auf andere Weise aussichtslos ist oder begründete Zweifel an der Richtigkeit der Angaben des Betroffenen bestehen. Generell

ist die Befragung Minderjähriger ohne Einverständnis des gesetzlichen Vertreters unzulässig; sie darf ausnahmsweise nur dann erfolgen, wenn das Kind unmittelbar betroffen ist.

Fernsehteams und andere Pressevertreter haben auch dann keine Zutrittsberechtigung zur Wohnung der Betroffenen, wenn den Behördenmitarbeitern das Betreten der Wohnung gestattet wird. Bei Filmaufnahmen im häuslichen Bereich in Begleitung von Amtspersonen ist die Einwilligung der Betroffenen spätestens am Vortag der Filmaufnahmen einzuholen. Schon das bloße Hinzuziehen eines Kamerateams stellt für den Betroffenen eine Offenbarung des Umstandes gegenüber Dritten dar, dass er Sozialleitungen bezieht. Damit erfolgt eine unbefugte Weitergabe von Sozialdaten und ein Verstoß gegen das Sozialgeheimnis nach § 35 Sozialgesetzbuch Erstes Buch, der dienstrechtlich zu ahnden ist.

Um den Verhältnismäßigkeitsgrundsatz zu wahren und die Entscheidung der Behörde transparent zu machen, müssen sämtliche Verfahrensschritte in der Akte schriftlich niedergelegt werden. Die datenschutzrechtliche Prüfung der Unterlagen des Ermittlungsdienstes ergab im vorliegenden Fall eine äußerst lückenhafte Dokumentation durch die Behörde. So fehlten Angaben darüber, dass sich die Mitarbeiter des Amtes vor Betreten der Wohnung mittels ihres Dienstausweises ausgewiesen hätten. Mangels entsprechender Dokumentation mussten wir davon ausgehen, dass eine Information der Betroffenen über den Zweck des Hausbesuchs, ihre Rechte (Zutrittsverweigerungsrecht) und über die möglichen Konsequenzen nicht erfolgt war. Das anwesende Kamerateam wurde nicht erwähnt, eine Abschrift des Prüfprotokolls den Betroffenen im Anschluss an den Besuch nicht ausgehändigt. Dem Vorgang ließen sich auch die Entscheidungsgründe, aus denen ein Hausbesuch als letztes Mittel in der Sachverhaltsaufklärung notwendig war, nicht entnehmen. Anhaltspunkte für einen Leistungsmissbrauch wurden nicht erwähnt.

Das JobCenter räumte Mängel bei der Dokumentation und dem Verfahren ein. Es änderte die künftige Verfahrensweise und erarbeitet zurzeit eine Dienstanweisung, um eine datenschutzgerechte Durchführung von Hausbesuchen zu gewährleisten. Hausbesuche werden zudem nicht mehr in Begleitung von Kamerateams durchgeführt.

Bei Filmaufnahmen im häuslichen Bereich in Begleitung von Amtspersonen ist rechtzeitig die Einwilligung der Betroffenen einzuholen.

Eine routinemäßige Durchführung von Hausbesuchen zur Feststellung von Leistungsmissbrauch ohne konkreten Verdacht ist unzulässig. Hausbesuche sind sorgfältig zu dokumentieren.

8.2 Profilbogen der Bedarfsgemeinschaft – Vermittlung von Berufstätigen

Der berufstätige Ehepartner einer Arbeitslosengeld-II-Empfängerin wurde aufgefordert, einen Profilbogen auszufüllen sowie einen Lebenslauf einzureichen. Die Behörde erklärte, seine Daten zu benötigen, um ihn in eine besser bezahlte Position zu vermitteln, obwohl er selbst gar keine Sozialleistungen bezog.

Um die Chancen des Betroffenen auf dem Arbeitsmarkt zu ermitteln, werden Fragebögen („Profilbögen“) zu Angaben über Schul- und Berufsausbildung sowie zu absolvierten Weiterbildungen verwendet. Es können detaillierte Aufstellungen zu Sprach- und PC-Kenntnissen sowie zur örtlichen und überregionalen Mobilität verlangt werden, ebenso Angaben zur Arbeitszeitverteilung und zur Annahme von Schichtarbeit. Gesundheitliche und soziale Gesichtspunkte dürfen nur angesprochen werden, wenn dies für die Eingliederung in Arbeit im Einzelfall relevant ist. Die Bewertung hat nach objektiven Kriterien zu erfolgen. Datenschutzrechtlich gänzlich unzulässig hingegen sind Fragen nach Werten/Idealen, Spannungen/Konflikten, dem Zustand der Wohnung, der Nachbarschaft und dem Umfeld, den Beziehungen außerhalb der Familie und zu Freunden sowie nach der Freizeitgestaltung oder Auffälligkeiten in der Kindheit.

Grundsätzlich sind sämtliche Mitglieder der Bedarfsgemeinschaft verpflichtet, ihr Vermögen und Einkommen zur Deckung des Bedarfs der gesamten Gemeinschaft einzusetzen. Gemäß Sozialgesetzbuch Zweites Buch (SGB II) müssen sie alle Möglichkeiten nutzen, ihren Lebensunterhalt aus eigenen Mitteln zu bestreiten. Die Behörde teilte uns mit, dass sich daraus die Pflicht ergebe, stets die gesamte Bedarfsgemeinschaft zu prüfen, um auch durch Neuvermittlung eines bereits Erwerbstätigen alle Möglichkeiten zur Beendigung und Verringerung der Hilfebedürftigkeit auszuschöpfen. Die damit im Zusammenhang stehende Datenerhebung sei deshalb zulässig.

Wir teilen diese Rechtsauffassung nicht. Zwar ist der Leistungsempfänger zur Mitteilung der im § 51b Abs. 2 Nr. 4 SGB II angegebenen Daten verpflichtet, nicht jedoch sind es in der Regel die Mitglieder der Bedarfsgemeinschaft, die sich bereits in einem Beschäftigungsverhältnis befinden.

Die Neuvermittlung in ein anderes Arbeitsverhältnis würde nicht nur in die grundgesetzlich geschützte Berufsfreiheit eingreifen sondern ggf. arbeitsrechtliche Streitigkeiten auslösen, denn der Betroffene müsste das bestehende Arbeitsverhältnis kündigen. Allein die mit der Abwicklung des bestehenden Arbeitsverhältnisses verbundenen Fragen haben wohl auch in der Praxis dazu geführt, dass in den meisten Fällen keine Vermittlung in ein neues

Beschäftigungsverhältnis erfolgt. Somit ist die pauschale Erhebung der Daten aller Mitglieder der Bedarfsgemeinschaft unabhängig vom Beschäftigungsstatus in der Regel nicht nur unverhältnismäßig, sondern auch zur Aufgabenerfüllung nicht geeignet und daher unzulässig.

Zwar ist eine Anstellung im Vollzeitverhältnis anders zu bewerten, als eine geringfügig entlohnte Beschäftigung (z. B. „Minijob“ auf 400-Euro-Basis). Doch ist auch nicht pauschal davon auszugehen, dass ein geringfügig beschäftigtes Mitglied der Bedarfsgemeinschaft der Vermittlung in ein neues Beschäftigungsverhältnis überhaupt bedarf. Beispielsweise stehen Mütter in Elternzeit, die wegen des geringen Elterngeldes zusätzliche Leistungen nach Sozialgesetzbuch Zweites Buch beantragen müssen, in einem Arbeitsverhältnis, das nicht ohne weiteres aufgelöst werden kann und sollte. Gleichfalls ist die regionale Arbeitsmarktsituation zu berücksichtigen.

Für Fälle, in denen ein Mitglied der Bedarfsgemeinschaft einer sozialversicherungspflichtigen Vollzeitbeschäftigung nachgeht, die seinen Fähigkeiten entspricht und aus der es ein adäquates Einkommen bezieht, konnten wir erreichen, dass die Behörden künftig nicht mehr von der Verpflichtung zur Beantwortung der Profilbögen ausgehen.

8.3 Dauerthema Kontoauszüge

Nach wie vor strittig ist, inwieweit bei der Beantragung von Sozialleistungen, insbesondere Arbeitslosengeld II, Kontoauszüge vorzulegen sind. Auseinandersetzungen gibt es auch darüber, ob teilweise Schwärzungen vorgenommen werden können und ob sie zu den Akten gegeben werden müssen.

Die Zahlung von Arbeitslosengeld II ist einkommens- und vermögensabhängig. Der Leistungsträger muss daher die Möglichkeit haben, Einkommen und Vermögen des Antragstellers verlässlich festzustellen. Ein wichtiges Mittel hierfür sind Kontoauszüge. Sie gelten als Beweisurkunden i. S. des § 60 Abs. 1 Sozialgesetzbuch Erstes Buch (SGB I), deren Vorlage die Behörde verlangen kann.

Voraussetzung ist jedoch, dass die Urkunden zum Beweis einer für die Leistung erheblichen Tatsache dienen. So mag es zwar im Einzelfall notwendig sein, sich bei der Stellung eines Folgeantrages die Kontoauszüge der letzten drei Monate vorlegen zu lassen, in den meisten Fällen wird jedoch die Angabe, dass sich an den Verhältnissen nichts geändert hat, genügen.

Die Vorlage von Kontoauszügen kann in folgenden Fällen verlangt werden:

- erstmalige Beantragung von laufenden Leistungen,
- Beantragung von einmaligen Beihilfen,
- während des laufenden Hilfebezuges frühestens nach Ablauf von zwölf Monaten,
- bei zu begründenden Zweifeln an der Vollständigkeit oder Richtigkeit der Angaben oder zur Klärung einer konkreten Einkommens- und Vermögenssituation.

Aus der Pflicht zur Vorlage von Kontoauszügen folgt jedoch kein Recht auf Speicherung sämtlicher auf den Auszügen vorhandener Daten.

Einige Sozialleistungsbehörden nehmen Kopien der Kontoauszüge zu den Akten, um die korrekte Sachbearbeitung jederzeit nachprüfen zu können. Aus unserer Sicht spricht nichts gegen die Speicherung von Kopien von Kontoauszügen, sofern sich darauf nur solche Daten befinden, die für die Leistungsberechnung unerlässlich sind. Nicht erforderliche Angaben müssen geschwärzt werden.

Beim Schwärzen muss der Betroffene beachten, dass eine Prüfung der Einnahmen bzw. Ausgaben möglich bleibt. Sollten sich aus den geschwärzten Auszügen Unklarheiten ergeben, hat der Betroffene die Originale zum Vergleich vorzulegen.

Um das Procedere der Schwärzung von Kontoauszügen zu umgehen, gibt es auch noch andere Möglichkeiten. So reicht es meist aus, die relevanten Angaben mit dem Vermerk „Auszug hat vorgelegen“ in einer Tabelle einzutragen. Eine solche Verfahrensweise halten wir für sinnvoll, da keine überschüssigen Daten in den Akten gesammelt werden.

Die Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein haben gemeinsame Hinweise zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen veröffentlicht. Diese sind auf unserer Internetseite[63] abrufbar.

[63] siehe http://www.lda.brandenburg.de → Infos zum Datenschutz → Arbeit, Soziales, Gesundheit und Familie / Frauen

Die Sozialleistungsbehörden sollten nicht routinemäßig vollständige Kontoauszüge für lange zurückliegende Zeiträume verlangen, sondern stattdessen mit Augenmaß nur die im Einzelfall erforderlichen Informationen erheben und speichern.

8.4 Aktenprüfung im Grundsicherungsamt

Um einen Überblick über die Verfahrensweise bei der Beantragung von Leistungen nach dem Sozialgesetzbuch Zweites Buch zu erhalten und dabei die Einhaltung der datenschutzrechtlichen Anforderungen bei der Datenerhebung und -speicherung zu begutachten, prüften wir die Aktenführung in einer optierenden Kommune.

Der Zugang zu den Akten wurde uns gewährt, allerdings weigerte sich die Geschäftsleitung zunächst, uns die bestehenden Dienstanweisungen bzw. Arbeitsrichtlinien auszuhändigen. Erst nach wiederholter schriftlicher Aufforderung und ausdrücklichem Hinweis auf seine Mitwirkungspflicht gemäß § 26 Brandenburgisches Datenschutzgesetz übergab das Grundsicherungsamt die geforderten Unterlagen.

Die Aktenführung genügte nicht den datenschutzrechtlichen Anforderungen. Änderungen in der Verfahrensweise bzw. die Umsetzung bereits vorhandener Regelungen sind notwendig. Insbesondere muss der Umgang mit Gesundheitsdaten verbessert werden.

Geprüft wurden nach dem Zufallsprinzip ausgewählte Leistungsakten und Akten aus dem Bereich der Vermittlung mit jeweils unterschiedlichem Bearbeitungsstand.

In 24 von 26 Fällen erfolgte die Antragstellung mit den im Sommer 2004 von der Bundesagentur für Arbeit herausgegebenen Antragsformularen. Die damit verbundene Datenerhebung genügte teilweise dem Prinzip der Erforderlichkeit nicht. Bei einigen Angaben fehlte der Hinweis auf die Freiwilligkeit.

Kopien der Personalausweise bzw. Reisepässe sämtlicher Mitglieder der Bedarfsgemeinschaft lagen − teilweise unlesbar − den Akten bei. In der Mehrzahl der Fälle wurden die Krankenversicherungskarten, Sozialversicherungs- und Schwerbehindertenausweise sowie die Sparkassenkarten, Sparbücher, Geburtsurkunden, vollständige Vaterschaftsanerkennungen und Unterhaltstitel in Kopie zur Akte genommen. Komplette Wohngeldbescheide oder Kopien von Kontoauszügen der letzten drei Monate waren gleichfalls ungeschwärzt in den Vorgängen abgeheftet. Es fanden sich vollständige Mietverträge nebst Betriebskostenabrechnung in einem Fall sogar im Original.

Ablichtungen des Mutterpasses wurden gespeichert, die neben dem voraussichtlichen Entbindungstermin weitere Gesundheitsdaten der Betroffenen, beispielsweise bestehende Allergien, erkennen ließen. Des Weiteren waren ärztliche Gutachten zum Gesundheitszustand der Betroffenen oder deren Angehörigen unverschlossen in den Akten. Die Masse an Kopien machte es teilweise erforderlich, dass die Bearbeiter die wenigen wirklich erforderlichen Positionen hervorheben mussten, um den Überblick zu erhalten.

Auffallend war, dass Teilnehmerlisten beispielsweise von durchgeführten Fortbildungen, die Daten Dritter enthielten, zur Akte genommen wurden. Teilweise enthielten die Listen nicht nur den Namen der anderen Teilnehmer, sondern auch einen Vermerk über deren Beruf bzw. Abschluss. Die Daten Dritter sind für die Antragsbearbeitung jedoch nicht erforderlich und dürfen nicht verarbeitet werden. Statt der Kopie der gesamten Listen genügt auch ein kurzer Vermerk, dass der Antragsteller an der Maßnahme teilgenommen hat.

Unvollständig hingegen blieb die Dokumentation von einschneidenden Eingriffen in die Grundrechte der Betroffenen. In fünf Vorgängen gab es zwar Hinweise auf Hausbesuche, teilweise fehlte aber der Nachweis der Prüfung, dass kein milderes Mittel als der Hausbesuch zur Sachverhaltsaufklärung möglich war. Es war nicht ersichtlich, dass der Vorgesetzte den Hausbesuch angeordnet hatte. Die Dokumentation entsprach weder den datenschutzrechtlichen Erfordernissen noch der Dienstanweisung des Amtes.

Im Bereich der Vermittlung wurden nicht erforderliche Daten teilweise aufgrund einer ausdrücklichen Dienstanweisung erhoben. Beispielsweise fragten die Behördenmitarbeiter nach der Zufriedenheit mit den bestehenden Wohnverhältnissen; Interessen, Wünsche und Hobbys sollten genannt werden. Kopien des Allergiepasses und Schwerbehindertenausweises nahmen sie zur Akte.

Nach dem Sozialgesetzbuch sind alle Sozialleistungen Beantragenden zur Mitwirkung verpflichtet. Klare gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger in diesem Zusammenhang beispielsweise die Vorlage von Kontoauszügen verlangen darf und welche Angaben geschwärzt werden dürfen, enthalten diese Vorschriften jedoch nicht. Grundsätzlich dürfen die Leistungsträger Sozialdaten nur dann erheben, wenn ihre Kenntnis für die Erfüllung einer ihnen im Gesetz zugewiesenen Aufgabe erforderlich ist (§ 67a Absatz 1 Satz 1 SGB X), um den Anspruch auf die Leistung dem Grunde und der Höhe nach feststellen zu können.

Viele Angaben waren im konkreten Fall jedoch offensichtlich nicht leistungsrelevant und hätten somit nicht erhoben werden dürfen. Die Anfertigung von

Kopien ist im Regelfall nicht erforderlich, der Betroffene kommt seiner Nachweispflicht auch durch bloße Vorlage der Unterlagen, in die dann Einsicht genommen werden kann, nach. Häufig reicht es aus Einzelangaben zu vermerken. Insbesondere Informationen über die Gesundheit sind ggf. in einem gesonderten, verschlossenen Umschlag zu den Akten zu nehmen.

Eine korrekte Aktenführung gibt sowohl den Betroffenen als auch der Behörde die Möglichkeit, sich einen umfassenden Überblick über die Entscheidungsgrundlagen zu verschaffen. Insbesondere bei Ermessensentscheidungen wird erkennbar, welche Sachverhalte in die Entscheidungsfindung eingeflossen sind.

Zum Schutz des Sozialgeheimnisses ist es unerlässlich, dass die Möglichkeit der Kenntnisnahme von Sozialdaten durch unbefugte Dritte ausgeschlossen wird. Bei unserer Prüfung mussten wir jedoch feststellen, dass die Kopiergeräte, die von den Mitarbeitern genutzt werden, sich in frei zugänglichen Räumen bzw. direkt auf den Fluren neben den Wartezonen befinden. Besucher haben jederzeit die Möglichkeit, Kenntnis sensitiver Daten Dritter zu erlangen. Das widerspricht eindeutig § 78a SGB X, nach dem Leistungsträger verpflichtet sind, durch technische und organisatorische Maßnahmen die Einhaltung der Datenschutzvorschriften des Sozialgesetzbuchs zu gewährleisten. Dies kann auch durch Dienstanweisungen geschehen.

Im Ergebnis unserer Prüfung hat die optierende Kommune bereits einige Veränderungen in ihrer Verfahrensweise vorgenommen. Längst sind jedoch noch nicht alle datenschutzrechtlichen Mängel behoben. In weiteren Gesprächen werden wir auf die Einhaltung der gesetzlichen Vorschriften dringen und zu gegebener Zeit erneut darüber berichten.

Das Erforderlichkeitsprinzip verlangt vom Leistungsträger, sich auf das zur rechtmäßigen Erfüllung seiner Aufgaben unerlässliche Minimum zu beschränken. Dies bedeutet zugleich, dass nur entscheidungserhebliche Tatsachen erhoben werden dürfen. „Überschüssige“ Daten sind zu löschen.

8.5 Hartz IV − Arbeitsgemeinschaften mit Grundgesetz nicht vereinbar

Das Sozialgesetzbuch Zweites Buch sieht eine geteilte Verantwortlichkeit für die Grundsicherung für Arbeitssuchende innerhalb der Arbeitsgemeinschaften vor. Die Arbeitsagentur und die Kommunen sind in ihrem jeweiligen Aufgabenbereich als Träger verantwortlich. Nach außen treten sie jedoch als eine Behörde auf. Mangels eindeutiger gesetzlicher Regelungen führte dies zu Unklarheiten bei den Zuständigkeiten – auch

bezüglich der datenschutzrechtlichen Aufsicht durch die Datenschutzbeauftragten des Bundes und der Länder.

Elf Landkreise aus dem gesamten Bundesgebiet hatten Verfassungsbeschwerde gegen die Verpflichtung erhoben, Arbeitsgemeinschaften mit der Bundesagentur für Arbeit bilden zu müssen. Die Landkreise sahen darin eine unzulässige Mischverwaltung.

Am 20. Dezember 2007 entschied nun das Bundesverfassungsgericht[64], dass die Zusammenlegung der Aufgaben von Kommunen und der Bundesagentur für Arbeit in gemeinsamen Arbeitsgemeinschaften verfassungswidrig ist. Das Grundgesetz fordert eine klare Zuordnung von Verwaltungsaufgaben an den jeweiligen Aufgabenträger. Der Grundsatz eigenverantwortlicher Aufgabenwahrnehmung ist einzuhalten, eine Mischverwaltung, wie sie in den Arbeitsgemeinschaften praktiziert wurde, nicht vorgesehen. Bei den Arbeitsgemeinschaften ist nicht gewährleistet, dass eigenständige und unabhängige Entscheidungen über die Vergabe von Arbeitslosengeld II – Leistungen getroffen werden können. Für die Bürger sei im Einzelfall nicht erkennbar, welche Stelle für welche Aufgaben letztlich zuständig ist.

Optionskommunen, die die Langzeitarbeitslosen eigenständig betreuen, sind hiervon nicht betroffen. Sie gehören keinen Arbeitsgemeinschaften an. Für sie bestehen klare Verantwortlichkeiten, die rechtlich nicht zu beanstanden sind. In Brandenburg haben sich fünf Kommunen für diese Option entschieden. Grundlegend neu organisiert werden müssen aufgrund der Entscheidung des Verfassungsgerichts dagegen die Arbeitsgemeinschaften, an denen die überwiegende Zahl der Gemeinden beteiligt ist. Dafür hat der Gesetzgeber längstens bis zum 31. Dezember 2010 Zeit.

Die Entscheidung eröffnet auch die Möglichkeit, die datenschutzrechtlichen Zuständigkeiten für die Zukunft eindeutig zu regeln. Auch das Bundesverfassungsgericht hat auf die Folgeprobleme hingewiesen, die sich aus der Mischverwaltung ergeben, so auch auf die unklaren datenschutzrechtlichen Zuständigkeiten.

Das Bundesverfassungsgericht erklärte die einheitliche Aufgabenwahrnehmung von Kommunen und der Bundesagentur für Arbeit in gemeinsamen Arbeitsgemeinschaften für verfassungswidrig. Der Gesetzgeber muss bis spätestens Ende 2010 eine Neuorganisation vornehmen. Damit kann auch die datenschutzrechtliche Zuständigkeit normenklar geregelt werden.

[64] Urteil des Bundesverfassungsgerichts vom 20. Dezember 2007 (2 BvR 2433/04 und 2434/04)

8.6 Netzwerk gesunde Kinder

Angesichts der hohen Anzahl von verwahrlost vorgefundenen und misshandelten Kindern wurden Netzwerke geschaffen, um Familien mit neugeborenen Kindern zunächst drei Jahre lang Berater zur Verfügung zu stellen. Diese „Paten" oder „Lotsen" weisen auf rechtliche Möglichkeiten und Angebote für Familien in der Region hin, erinnern aber auch an Früherkennungsuntersuchungen und ärztliche Beratungen zu empfohlenen Impfungen. Außerdem sorgen sie dafür, dass personenbezogene Daten der Datenbank des Netzwerkes zur Verfügung gestellt werden, soweit dies mit den Familien vereinbart wurde.

Seit Anfang 2006 beraten wir das Ministerium für Arbeit, Soziales, Gesundheit und Familie, das nur datenschutzgerechte Konzepte fördern will, bei drei Netzwerken. In Zusammenarbeit mit dem Ministerium konnten wir für ein Musterprojekt beim Klinikum Niederlausitz erreichen, dass der Umfang der Daten, die von deren Kinderklinik in der Datenbank erfasst werden, deutlich eingeschränkt und die vorgesehenen Übermittlungen von personenbezogenen Angaben auf ein Minimum reduziert wurden.

Das rechtliche Konzept aus der Niederlausitz wurde in Eberswalde praktisch vollständig übernommen. Bei beiden Projekten werden speziell geschulte ehrenamtliche Paten auf Wunsch und mit Einverständnis insbesondere der Mütter tätig. Sie nehmen bei Besuchen Einblick in ein so genanntes Familienbuch, in dem Ärzte, Therapeuten oder Beratungsstellen auf von ihnen geführten Einzelblättern abstempeln, wann eine Untersuchung, Maßnahme oder Beratung durchgeführt wurde und vermerken, ob es dabei Probleme gab. Diese Informationen gibt der Pate mündlich an den Netzwerkkoordinator weiter, der sie in eine Datenbank übernimmt. Später soll das Projekt anhand anonymisierter Angaben aus dieser Datensammlung evaluiert werden.

Im Havelland ist vorgesehen, statt ehrenamtlicher Paten Mitarbeiter aus der öffentlichen Verwaltung bzw. Hebammen als „Verwaltungslotsen" bzw. „Familienlotsen" einzusetzen. Die Informationen aus dem Familienbuch werden vom Familienlotsen in ein Protokollformular übertragen, das mit einem verschlossenen Umschlag an den Netzwerkkoordinator weitergeleitet wird. Auch in anderen Punkten gibt es Abweichungen von dem Niederlausitzer Vorläufer. So wird dokumentiert, ob bei Problemen geholfen werden konnte oder nicht. Darüber hinaus bestehen Überlegungen, auch die sozialen Umstände der Familie in der Datenbank zu erfassen.

Von allen drei Projekten forderten wir ein Sicherheitskonzept für das neu eingeführte Verfahren an. Die beteiligten Stellen müssen darlegen, wie sie die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen

Informationen mit angemessenen Sicherheitsmaßnahmen gewährleisten können. Erst die Kombination aus rechtlichen, technischen, organisatorischen, personellen und infrastrukturellen Maßnahmen gewährleistet ein ausreichendes Sicherheitsniveau.

Zum heutigen Zeitpunkt muss festgestellt werden, dass zwei der drei Netzwerke nicht über eine fachgerechte IT-Sicherheitskonzeption verfügen, obwohl die Projekte schon angelaufen sind. Dieser Zustand ist aus unserer Sicht nicht tragbar, zumal die teilnehmenden Kliniken auch sensitive Gesundheitsdaten in ihren Arbeitsprozessen verarbeiten.

Die Einhaltung von Standards der technischen Datensicherheit ist neben der Freiwilligkeit der Teilnahme der Eltern eine wesentliche Vorraussetzung für das Gelingen der Projekte. Teilnehmende Familien müssen sich sicher sein können, dass ihre zum Teil sehr persönlichen Angaben mit der gebotenen Sorgfalt behandelt werden.

8.7 Entwicklungen im brandenburgischen Gesundheitswesen

Neue oder noch geplante Regelungen des Heilberufsgesetzes, Landeskrankenhausgesetzes, Gesundheitsdienstgesetzes, Psychisch-Kranken-Gesetzes und Rettungsdienstgesetzes werden erhebliche Änderungen im Gesundheitswesen des Landes Brandenburg nach sich ziehen. Neben datenschutzrechtlichen Verbesserungen gibt es dabei auch Regelungsvorschläge, die uns nicht überzeugen.

8.7.1 Heilberufsgesetz (HeilBerG) und Gesundheitsberufeanerkennungsgesetz (BbgGesBAG)

Nach kleineren Änderungen im Heilberufsgesetz im Jahre 2006 hat die Umsetzung der Richtlinie 2005/36/EG in einem Artikelgesetz über die Anerkennung von Berufsqualifikationen auf dem Gebiet der Gesundheitsberufe größere datenschutzrechtliche Relevanz. Es geht darum, Angehörigen anderer Mitgliedstaaten zu ermöglichen, ihren Beruf zumindest vorübergehend auch in Brandenburg auszuüben. Dies setzt voraus, dass eine Berufsanerkennung erfolgt und keine berufsrechtlich bedeutsamen Sachverhalte dagegen sprechen. Das Heilberufsgesetz soll deshalb ebenso wie das für nichtakademische Gesundheitsberufe geltende Gesundheitsberufeanerkennungsgesetz um Mitteilungspflichten und Datenverarbeitungsvorschriften ergänzt werden. In beiden Gesetzen gilt es, sowohl dem datenschutzrechtlichen Grundsatz der Datenerhebung beim Betroffenen und dem Verhältnismäßigkeitsprinzip als auch Aspekten der öffentlichen Sicherheit Rechnung zu tragen. Inwieweit

dieses gelingt, ist bei den noch im Entwurfstadium befindlichen Vorschriften, zu denen wir beratend Stellung nehmen, noch offen.

8.7.2 Krankenhausgesetz des Landes Brandenburg (LKGBbg)

Im Tätigkeitsbericht 1999 lautete die Überschrift der Ziffer A 8.3.1 „Krankenhäuser: Neue Bestimmungen zum Datenschutz in Sicht“. Aber erst Mitte 2006 signalisierte das Gesundheitsministerium, dass es, unserer Empfehlung folgend, ein laufendes Verfahren zur Novellierung des Landeskrankenhausgesetzes dazu nutzen werde, die Vorschriften zum Datenschutz statt wie bisher in einer Verordnung künftig im Gesetz selbst zu regeln. In die Erarbeitung des Gesetzesentwurfs wurden wir von Anfang an eingebunden. Noch sind die Diskussionen hierzu nicht abgeschlossen.

8.7.3 Brandenburgisches Gesundheitsdienstgesetz (BbgGDG)

Bei der Novellierung des Brandenburgischen Gesundheitsdienstgesetzes beschäftigten uns vor allem zwei Paragraphen. § 7 betrifft das Einladungs- und Rückmeldewesen für Früherkennungsuntersuchungen von Kindern (Näheres vgl. unter Ziffer 8.8), mit § 16 sollen zukünftig die Datenverarbeitungen im Öffentlichen Gesundheitsdienst speziell geregelt werden.

Bei der grundlegenden Neugestaltung der Vorschrift zur Verarbeitung personenbezogener Daten im Gesundheitsdienstgesetz konnten wir erreichen, dass Daten, die bei der freiwilligen Inanspruchnahme von Beratungsangeboten erhoben wurden, grundsätzlich nur mit Einwilligung des Betroffenen verarbeitet und von anderen Daten derselben Person getrennt werden. Ebenso wurde unserem Hinweis, dass im Gesundheitsamt neben „normalen“ personenbezogenen Daten auch solche einer besonderen Kategorie nach § 4a BbgDSG, wie z. B. Angaben über die Gesundheit oder die Sexualität, verarbeitet werden, in gewissem Umfang Rechnung getragen.

Dem Gesundheitsministerium war selbst daran gelegen, Übermittlungen des öffentlichen Gesundheitsdienstes an nicht öffentliche Personen/Stellen möglichst einzuschränken. Für die Übermittlung personenbezogener Daten an Dritte, die mit der Durchführung von Aufgaben des Öffentlichen Gesundheitsdienstes probeweise oder dauerhaft beauftragt werden können, wurde aber eine separate Befugnis geschaffen. Die Daten dürfen bei den privaten Auftragnehmern nur von medizinischem Personal genutzt werden. Nicht durchsetzen konnten wir uns hingegen mit dem Vorschlag, ausdrücklich festzuhalten, dass das Übertragen von Aufgaben an Private nur für den Fall zulässig sein soll, wenn daran ein überwiegendes Allgemeininteresse besteht. Das Gesundheitsministerium geht davon aus, dass ohne Not solche Maßnahmen

nicht ergriffen werden und hält das allgemeine Erfordernis seiner Zustimmung als Regulierungsinstrument für ausreichend.

8.7.4 Brandenburgisches Psychisch-Kranken-Gesetz (BbgPsychKG)

Im Jahr 2007 wurde uns ein Entwurf zur umfangreichen Novellierung des Brandenburgischen Psychisch-Kranken-Gesetz vorgelegt, welches Regelungen über Hilfen und Schutzmaßnahmen sowie den Vollzug gerichtlich angeordneter Unterbringung für psychisch Kranke vorsieht. Unsere Empfehlungen zielten im Wesentlichen darauf ab, das Erforderlichkeitsprinzip und das Gebot der Normenklarheit besser zu wahren. In diesem Zusammenhang baten wir auch um die Überprüfung der praktischen Relevanz einer erst 2001 eingefügten Regelung, die den Umgang mit Besucherdaten und insbesondere deren lange Speicherung von bis zu fünf Jahren, betrifft.

8.7.5 Brandenburgisches Rettungsdienstgesetz (BbgRettG)

Bei der Durchführung des Rettungsdienstes werden auch Daten über die Gesundheit, die besonders schützenswert sind, verarbeitet. Deshalb wiesen wir darauf hin, dass besondere Schweigepflichten für diejenigen, die im Rettungsdienst tätig sind, erforderlich sind. Diesen Hinweis griff das Ministerium umgehend auf. Auch sonst wurden etliche datenschutzrechtliche Verbesserungen aufgenommen.

Das Gesetz sieht sowohl bei der Durchführung des Rettungsdienstes als auch bei der Gebührenabrechnung eine Option für die Einbeziehung beauftragter Personen oder Stellen vor. Für Aufträge an nicht öffentliche Stellen forderten wir als zusätzliche Voraussetzung, die Notwendigkeit des Bestehens eines überwiegenden Allgemeininteresses und Maßnahmen, die den Schutz insbesondere von Gesundheitsdaten bei der Verarbeitung durch den Auftragnehmer sicherstellen. Problematisch erschienen uns auch Unterschiede bei Aufbewahrungsfristen und Vorlagepflichten, je nachdem, ob eine zuständige Stelle selbst tätig wird oder die Aufgabe überträgt. Ungeregelt sind bisher auch Datenverarbeitungen, die außerhalb der Leitstellen, etwa am Unfallort, stattfinden.

Die Überarbeitung wesentlicher Landesgesetze im Gesundheitsbereich bringt viele Chancen für datenschutzrechtliche Verbesserungen mit sich. Ob die Chance tatsächlich immer genutzt werden wird, lässt sich derzeit noch nicht beurteilen. Allerdings hat das Ministerium aus unseren ersten Stellungnahmen bereits viele Hinweise aufgegriffen.

8.8 Einladungen für Früherkennungsuntersuchungen von Kindern

In dem Bestreben, Kinder vor gesundheitlichen Defiziten, Vernachlässigungen oder Misshandlungen zu schützen, hat das Gesundheitsministerium im Laufe der Novellierung des Brandenburgischen Gesundheitsdienstgesetzes eine neue Vorschrift erarbeitet, um die Teilnahmequote an den Früherkennungsuntersuchungen für Kinder zu steigern.

Verantwortlich für Einladungen und verschiedene Datenabgleiche wird das Landesgesundheitsamt als zentrale Stelle sein. Für seine Aufgabenerfüllung erhält es zum einen von den Meldebehörden jährlich zum 1. Juni bestimmte Angaben über alle Kinder, die zwischen sieben und 58 Lebensmonaten alt sind. Zum anderen sollen Ärzte die Teilnahme an den Früherkennungsuntersuchungen (U 6, U 7 und U 8) der zentralen Stelle melden. Da die ärztliche Schweigepflicht bereits die Tatsache des Arztbesuches umfasst, musste eine Befugnis für deren Durchbrechung geschaffen werden. Den Abgleich der Meldedaten mit den Rückmeldungen der Ärzte regelt das Gesetz selbst trotz unserer Kritik nicht, er wird lediglich in der Gesetzesbegründung erwähnt. So bleiben z. B. Löschungsfristen für die abgeglichenen Daten offen.

Nach der Kinder-Richtlinie des Bundesausschusses der Ärzte und Krankenkassen gibt es für die Früherkennungsuntersuchungen Untersuchungsfristen und darüber hinausgehende Toleranzfristen. Eigentlich kann erst nach Ablauf der Toleranzfristen, die bei der U 6, U 7 und U 8 ein bis drei Monate betragen, für eine Untersuchung festgestellt werden, dass eine Rückmeldung von einem Arzt dazu nicht vorliegt. Die Krankenkassen übernehmen nach diesem Zeitpunkt nicht mehr die Kosten der Vorsorgeuntersuchung. Die Gesetzesbegründung geht daher davon aus, dass das Landesgesundheitsamt noch vor Ablauf der Untersuchungsfrist feststellt, für welche Kinder nicht bekannt ist, ob sie ärztlich untersucht wurden. Es müssen also auch Eltern, die einen Termin gegen Ende der Untersuchungsfristen oder noch innerhalb der Toleranzfristen vereinbart haben, damit rechnen, Erinnerungsschreiben zu erhalten. Für sie nimmt das Gesetz Datenverarbeitungen und einen weiteren Abgleich in Kauf, obwohl er völlig sinnlos ist.

Bei der U 9 wird auf eine Rückmeldung der Ärzte verzichtet, weil die Gesundheitsämter bei den Einschulungsuntersuchungen darauf hinwirken können, dass diese Früherkennungsuntersuchung durchgeführt wird. Damit ist bereits die Erforderlichkeit der Übermittlung der Meldedaten aller Kinder im Alter zwischen 48 und 58 Monaten fraglich.

Auf zusätzliche Einladungen verzichtet das Landesgesundheitsamt, wenn sich Kinder aufgrund einer schweren chronischen Erkrankung oder Behinde-

rung in kontinuierlicher ärztlicher Behandlung befinden. Im Gesetzgebungsverfahren wurde uns hierzu erläutert, dass beispielsweise der behandelnde Arzt auf Veranlassung der Eltern eine entsprechende Bescheinigung ausstellen könne. Die aktuelle Gesetzesbegründung scheint jedoch eher von einem einwilligungsunabhängigen Übermittlungsrecht auszugehen. Ein solches wäre jedoch im Gesetz normenklar zu regeln.

Bleiben die Einladungen zu den weiteren Untersuchungsterminen erfolglos, wird das zuständige Gesundheitsamt informiert und trifft – wie es im Gesetzesentwurf heißt – „geeignete und angemessene Maßnahmen, um auf eine erhöhte Teilnahmequote an den Früherkennungsuntersuchungen hinzuwirken“. Weitere Übermittlungsmöglichkeiten oder gar Wohnungsbetretungsrechte müssten als Grundrechtseingriffe eindeutig im Gesetzestext formuliert sein. Auch ist anzumerken, dass es keine ausdrückliche Pflicht zur Teilnahme an den angebotenen Untersuchungen gibt, mithin im Falle des Fernbleibens auch nicht gegen eine gesetzliche Pflicht verstoßen wird. Angesichts dieser Rechtslage bleibt als Maßnahme allenfalls eine Beratung oder das erneute Angebot einer Untersuchung durch das Gesundheitsamt.

Insgesamt wird ein aufwändiges und kostenintensives Verfahren mit Datenübermittlungen von verschiedenen Stellen, einer Durchbrechung der ärztlichen Schweigepflicht, mehreren Datenabgleichen und viel Papier (Erinnerungsschreiben) installiert, dessen Wirkung mehr als fraglich ist. Selbst bei der scheinbaren Erfolglosigkeit mehrerer Einladungen ist durch Rückfragen des Gesundheitsamtes bei den Betroffenen zunächst zu klären, ob nicht eine fehlende Rückmeldung durch den behandelnden Arzt oder ein anderer nachvollziehbarer Grund für die Nichtreaktion vorlag. Obwohl der Gesetzgeber insoweit selbst von einer „Unschuldsvermutung“ ausgeht, erfolgen die Rückfragen nicht durch die Zentrale Stelle, sondern diese informiert die zuständigen Gesundheitsämter, wodurch die betroffenen Familien dort bereits in ein ungünstiges Licht gerückt werden.

Datenabgleiche sind Eingriffe in das Recht auf informationelle Selbstbestimmung. Dies gilt besonders wenn dafür Meldepflichten von Ärzten für Angaben, die sonst unter die ärztliche Schweigepflicht fallen, geschaffen werden. Bevor ein solcher Datenabgleich eingeführt wird, müssen seine Eignung und Verhältnismäßigkeit im Hinblick auf das angestrebte Ziel genau geprüft werden.

9 Finanzen

9.1 Kontendatenabrufverfahren

9.1.1 Kontrolle des Abrufs zu Steuerzwecken

Mit der Änderung der Abgabenordnung (AO) durch das Gesetz zur Förderung der Steuerehrlichkeit sind neue Möglichkeiten des Zugriffs auf Bankdaten durch die Finanzbehörden geschaffen worden. Wir haben stichprobenartig zwei Finanzämter auf die Einhaltung der datenschutzrechtlichen Anforderungen bei der Durchführung von Kontenabrufersuchen überprüft.

In den von uns geprüften Fällen war der Kontenabruf jeweils zur Durchsetzung der Steuerpflicht bezüglich der Entrichtung von Umsatz- und/oder Einkommenssteuer erforderlich. Die Betroffenen schuldeten hohe Steuerbeträge. Kontenabfragen wurden durch die Finanzämter erst dann vorgenommen, als der begründete Verdacht bestand, dass neben den vom Betroffenen angegebenen Konten weitere Konten mit Vermögen vorhanden sind. Sämtliche bisher vorgenommenen Vollstreckungsmaßnahmen waren ergebnislos verlaufen. Zur Aufklärung der tatsächlichen Vermögensverhältnisse und insbesondere, um der Gefahr der Vermögensverschiebung zu begegnen, waren die Kontenabrufverfahren notwendig.

Die Entscheidung zur Durchführung der Kontenabfrage steht gemäß § 93 Abs. 7 AO im Ermessen der Finanzbehörde. Der Kontenabruf kann laut Anwendungserlass des Bundesministeriums der Finanzen nur anlassbezogen und zielgerichtet erfolgen und muss sich eindeutig auf eine bestimmte Person beziehen. Die Ermessenserwägungen des Finanzamtes wurden in den jeweiligen Aktenvermerken ausführlich dokumentiert und waren gut nachvollziehbar. Die Kontenabfragen erfolgten mittels der vom Bundeszentralamt für Steuern zur Verfügung gestellten Vordrucke, die gleichfalls zu den Akten genommen wurden. Unzureichend war allerdings teilweise die Dokumentation hinsichtlich der Gründe, weshalb die Auskunft nicht beim Steuerpflichtigen selbst eingeholt werden konnte.

Grundsätzlich soll vor einer Kontenabfrage gemäß § 93 Abs. 7 AO entsprechend dem Transparenzgebot die Finanzbehörde dem Steuerpflichtigen Gelegenheit geben, Auskunft über seine Konten und Depots zu erteilen. Ein Abruf bei den Kreditinstituten hat erst dann zu erfolgen, wenn ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziel geführt hat oder keinen Erfolg verspricht. Das ist dann der Fall, wenn durch das vorherige Auskunftsersuchen der Ermittlungszweck gefährdet würde. Die Informations-

pflicht entfällt dann jedoch nicht gänzlich, vielmehr ist der Beteiligte nachträglich über die Durchführung des Abrufs zu unterrichten.

In den meisten von uns geprüften Fällen wurden die Betroffen aus Rücksicht auf die Gefährdung des Ermittlungszweckes vorher nicht informiert. Es bestand wegen des bisherigen Verhaltens der Steuerpflichtigen die begründete Besorgnis der Vermögensverschiebung auf Dritte oder ins Ausland. Die Dokumentation enthielt dazu in zwei Fällen keine Angabe. Die Kontenabrufe führten zu positiven Ergebnissen. Festgestellt wurden jeweils mehrere existente, aber auch bereits aufgelöste Konten des Betroffenen selbst. Es wurde Auskunft erteilt über das Konto führende Institut, die Nummer des Kontos, den Kontoinhaber, das Datum der Einrichtung beziehungsweise das Löschungsdatum sowie über die Verfügungsberechtigten. Übermittelt wurden entsprechend der gesetzlichen Möglichkeit auch andere Konten, für die der Steuerpflichtige eine Verfügungsbefugnis besitzt.

Ist die vorhergehende Information des Betroffenen unterblieben, so ist der Steuerpflichtige nachträglich über die erfolgte Abfrage zu informieren. Dieser aus dem Transparenzgebot folgenden Pflicht kam lediglich ein Amt vollständig nach, z. T. war auf Grund der fehlenden Dokumentation nicht erkennbar, ob die Betroffenen informiert wurden.

Zur Dokumentation der erfolgten Kontenabrufe wurde jeweils ein Aktenvermerk angefertigt, der dem Steuervorgang beigefügt war. Dabei handelte es sich um einen Vermerk des Sachbearbeiters, der insbesondere die Ermessenserwägungen des Finanzamtes zur Durchführung des Abrufs darstellte. Häufig mangelte es jedoch an einer klaren Gliederung zu den einzelnen Erwägungen. Außerdem haben wir die teilweise unübersichtliche Aktenführung kritisiert, da sich Unterlagen nicht immer in einer Akte befanden.

Hinsichtlich der durchgeführten Kontenabfragen bestanden keine gravierenden datenschutzrechtlichen Mängel. Allerdings muss die Dokumentation der Entscheidung in den Akten verbessert sowie sichergestellt werden, dass die Betroffenen in jedem Fall zumindest nachträglich darüber informiert werden, dass ein Kontenabruf durchgeführt wurde.

9.1.2 Regelung zum Abruf von Kontostammdaten für Leistungsbehörden verfassungswidrig

Das Bundesverfassungsgericht hat im Juni 2007 über die Zulässigkeit der automatisierten Abfrage von Kontostammdaten der Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern und Depots durch die Finanz- und andere Behörden sowie die Gerichte

entschieden.[65] § 93 Abs. 8 Abgabenordnung (AO) verstößt danach gegen den verfassungsrechtlichen Bestimmtheitsgrundsatz und damit gegen das Grundrecht auf informationelle Selbstbestimmung. Es muss konkret festgelegt werden, welche Sozialleistungsbehörden zu welchem Zweck zum Abruf von Kontostammdaten berechtigt sind.

Eine Konkretisierung des § 93 Abs. 8 AO erfolgte bereits mit In-Kraft-Treten des Unternehmenssteuerreformgesetzes 2008.[66] Danach dürfen die für die Grundsicherung für Arbeitsuchende, die Sozialhilfe, die Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz, die Aufstiegsfortbildungsförderung und das Wohngeld zuständigen Behörden die Abfrage der Kontostammdaten durchführen.

Voraussetzung ist, dass ein vorheriges Auskunftsersuchen an den Betroffenen nicht zum Ziel geführt hat oder keinen Erfolg verspricht. Vor einem Abrufersuchen ist der Betroffene auf die Möglichkeit eines Kontoabrufs hinzuweisen, was in amtlichen Vordrucken und Merkblättern geschehen kann. In der Regel muss der Betroffene nach Durchführung des Kontoabrufs von der abrufenden Behörde benachrichtigt werden. Die jeweilige Sozialleistungsbehörde hat das Kontenabrufersuchen unmittelbar an das Bundeszentralamt für Steuern zu richten.

§ 93 Abs. 7 AO und § 24c Abs. 3 S. 1 Nr. 2 Kreditwesengesetz sind dagegen mit dem Grundgesetz vereinbar.

9.2 Deutschland wird durchnummeriert – Einführung einer einheitlichen Steueridentifikationsnummer

Nach der einheitlichen, lebenslang gültigen neuen Krankenversicherungsnummer wird mit dem bundeseinheitlichen Identifikationsmerkmal für Besteuerungsverfahren von Personen und Wirtschaftsunternehmen eine weitere große Datenbank aufgebaut. Im Juli 2007 wurde mit der Vergabe der eindeutigen Identifikationsnummer an jeden Bürger begonnen.

Die Steuer-Identifikationsnummer (Steuer-ID) gilt für alle Bürger von der Geburt bis über den Tod hinaus. Sie ersetzt für natürliche Personen die bisherige Steuernummer und besteht aus zehn Ziffern und einer zusätzlichen Prüfziffer. Die Steuer-ID darf nicht aus anderen Daten über den Steuerpflichtigen gebildet oder abgeleitet werden, aus ihr selbst sollen keine Rückschlüs-

[65] Beschluss des Bundesverfassungsgerichts vom 13. Juni 2007 (1 BvR 1550/03; 1 BvR 2357/04 und 1 BvR 603/05)

[66] Unternehmenssteuerreformgesetz 2008 vom 14. August 2007 (BGBl. I S. 1912)

se auf die dahinter stehende Person möglich sein. Zu der Identifikationsnummer werden Familiennamen, frühere Namen, Vornamen, Doktorgrad, Ordensnamen/Künstlernamen, Tag und Ort der Geburt und Geschlecht, aktuelle und frühere Anschrift, sowie das zuständige Finanzamt gespeichert. § 139b Abgabenordnung (AO) ist hierfür die gesetzliche Grundlage.

Um die Steuer-ID zu erstellen und dem Bürger bekannt geben zu können, übermittelten alle Meldebehörden in der Bundesrepublik Deutschland bis zum 30. Juni 2007 dem Bundeszentralamt für Steuern die in ihrem Zuständigkeitsbereich im Melderegister registrierten Einwohner. Anhand der gemeldeten Daten vergibt das Zentralamt für jede gemeldete Person ein vorläufiges Bearbeitungsmerkmal. Um Dubletten, d. h. einen mehrfach mit leicht abweichender Schreibweise existierenden Datensatz herauszufiltern, wird anschließend ein Datenabgleich durchgeführt. Die Dubletten werden sodann gelöscht und die vergebene Steuer-ID der zuständigen Meldebehörde und dem Bürger mitgeteilt.

Bürger, die wirtschaftlich tätig sind, wie beispielsweise Handwerker und Freiberufler erhalten zusätzlich eine Wirtschafts-Identifikationsnummer. An juristische Personen und Personenvereinigungen wird diese gleichfalls vergeben.

Mit Einführung der Identifikationsnummer erfolgt demnach auch ein indirekter Abgleich der Daten bei den Melderegistern. 82 Millionen Personendaten werden geprüft. Vor allem aus diesem Grund wird neben weiterer grundsätzlicher verfassungsrechtlicher Bedenken die Verfassungskonformität der Steuer-Identifikationsnummer derzeit kontrovers diskutiert. Bereits im Jahr 2003, als die Abgabenordnung geändert und die Steuernummer gesetzlich geregelt wurde, äußerten die Datenschutzbeauftragten des Bundes und der Länder ihre Zweifel. Zwar ist in § 139b Abs. 5 i. V. m. Abs. 4 AO festgelegt, inwieweit die Steuer-ID verwendet werden darf. Die Zwecke sind jedoch nicht abschließend aufgeführt, sondern enthalten eine Öffnungsklausel, nach der die Datenspeicherung erlaubt ist, um: „den Finanzbehörden die Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen Aufgaben zu ermöglichen“. Sobald also die Aufgaben erweitert werden, erhält auch die Steuer-ID eine neue Bedeutung und Dimension.

Davon ausgehend, dass das Bundesverfassungsgericht in seiner ständigen Rechtsprechung eine unbeschränkte Verknüpfungsmöglichkeit durch ein einheitliches Personenkennzeichen als unzulässig angesehen hat, muss die Vergabe einer zentralen Nummer zumindest an einen engen, gesetzlich klar definierten Zweck gebunden sein. Dies ist durch die bestehende Öffnungsklausel zweifelhaft. Bereits jetzt ist absehbar, dass die Verwendung der Steuer-ID nicht auf den Zweck der Steueridentifikation beschränkt bleiben

wird. Durch die Vergabe über die Kommunen und den Abgleich mit den Melderegisterdaten wurde die Möglichkeit eröffnet, dass die Daten auch in diesen Bereichen genutzt werden. Die Vergangenheit hat gezeigt, dass derartige Befürchtungen schnell Realität werden können. Als Beispiel sei die Verfahrensweise für die so genannten Freistellungsaufträge genannt. Diese zunächst nur für steuerliche Zwecke erhobenen Daten, können nun auch für den Abgleich der beim Bundeszentralamt für Steuern gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen verwendet werden.

Des Weiteren plante die Bundesregierung mit dem Jahressteuergesetz 2008 die zentrale Steuerdatei um zusätzliche Daten zu ergänzen, etwa um die Religionszugehörigkeit, den Ehepartner, die Kinder und deren Steuer-ID sowie Angaben zu den Steuerklassen. Der Gesetzentwurf sah die Einführung eines optionalen Anteilsverfahrens für berufstätige Ehepaare als Alternative zur Wahl der mit einem hohen Lohnsteuerabzug verbundenen Steuerklasse V vor. Die Folge davon wäre gewesen, dass der Arbeitgeber bei Anwendung dieses freiwilligen Verfahrens genauere Rückschlüsse auf das Einkommen des jeweils anderen Ehegatten hätte ziehen können als bisher.

Zwar wurde auch auf Grund der Intervention der Datenschutzbeauftragten das Anteilsverfahren komplett aus dem Regierungsentwurf herausgenommen, doch bleiben Fragen offen: Ungewiss ist, ob das vorgesehene Authentifizierungsverfahren für den Arbeitgeber den Schutz vor Zugriffen unberechtigter Dritter bietet. Die Daten aus der Zentraldatei sollten nur unter Mitwirkung des betroffenen Bürgers abgerufen werden können.

Die Steueridentifikationsnummer bringt für den Bürger Erleichterungen im elektronischen Datenübermittlungsverfahren und für die Finanzbehörden neue Kontrollmöglichkeiten. Keinesfalls darf diese Identifikationsnummer zu einem verfassungsrechtlich unzulässigen Personenkennzeichen werden.

9.3 Neues Finanzmanagement in der Landesverwaltung

Eines der wichtigsten aktuellen IT-Projekte der Landesregierung ist die Einführung des Neuen Finanzmanagements (NFM) zur Anwendung betriebswirtschaftlicher Steuerungselemente in der Landesverwaltung. Wesentliches Element hierbei ist die Nutzung der Kosten- und Leistungsrechnung (KLR) zur Effizienz- und Kostenkontrolle bei der Erbringung von Verwaltungsdienstleistungen. Über die entsprechenden Pilotprojekte hatten wir bereits in unseren vergangenen Tätigkeitsberichten[67] informiert.

[67] vgl. zuletzt Tätigkeitsbericht 2004/2005, A 1.3

Auf Grund der positiven Erfahrungen in den beiden ersten Projektwellen, in denen die KLR bzw. das NFM in insgesamt acht ausgewählten Pilotbehörden der Landesverwaltung erprobt wurde, hat die Landesregierung im Dezember 2005 deren landesweite Einführung beschlossen. Die Entscheidung soll dazu dienen, die Grundlagen für eine transparentere und wirkungsvollere Haushaltsplanung und Haushaltswirtschaft zu legen. Ziel ist es auch, die Voraussetzungen für die Aufstellung eines so genannten „Produkthaushalts“ zu schaffen, in dem die bei der Erstellung von „Verwaltungsprodukten“ eingesetzten Mittel der erbrachten Leistung gegenüber gestellt werden.

Parallel zur landesweiten Einführung des Neuen Finanzmanagements wurde von der Landesregierung die Modernisierung und Erweiterung des bisherigen Verfahrens zum Haushalts-, Kassen- und Rechnungswesen (HKR) beschlossen. Realisiert werden soll ein flächendeckendes, integriertes und inhaltlich ausbaufähiges System, welches das bestehende Verfahren ProFiskal ablöst. Der Beschluss spiegelt auch die Festlegung in der IT-Strategie des Landes wider, mittelfristig ein einheitliches integriertes ERP-System (Enterprise Resource Planning) einzuführen. Die zentrale Projektverantwortung trägt das Ministerium der Finanzen.

Technische Basis der beschlossenen Erneuerung des HKR-Verfahrens sowie der landesweiten Einführung des NFM ist vor dem Hintergrund der Vorarbeiten in den ersten beiden Projektwellen ein SAP-R/3-System. Zum Einsatz kommen die jeweils fachspezifischen SAP-Module wie z. B. PSM für die Mittelbewirtschaftung, FI zur Finanzbuchhaltung, CO zum Controlling oder CATS zur mitarbeiterbezogenen Erfassung der Arbeitszeiten pro Verwaltungsprodukt. Die zentralen Systemkomponenten (SAP-Applikationsserver und Datenbankserver) werden bei einem Dienstleister gemeinsam für die gesamte Landesverwaltung betrieben. Wegen aktueller Entwicklungen ist dies jedoch nicht mehr der Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben, sondern mit der Firma T-Systems ein externer, privater Dienstleister. Die daraus entstehenden Konsequenzen erörtern wir an anderer Stelle in diesem Bericht.[68]

Aus Sicht des Datenschutzes und der IT-Sicherheit verlangen die Erneuerung des HKR-Verfahrens und die landesweite Einführung des NFM eine Fortschreibung und Anpassung der jeweiligen Sicherheitskonzepte unter Berücksichtigung der projektspezifischen Besonderheiten und der Weiterentwicklung des Standes der Technik. Bereits im Jahr 2002 wurde bei der Risikoanalyse für das existierende HKR-Verfahren ProFiskal festgestellt, dass der Schutzbedarf der verarbeiteten Daten bzgl. des Schutzziels Integrität als hoch einzuschätzen ist. Ähnliche Ergebnisse liefern Vorarbeiten für ein HKR-

[68] vgl. A 9.4 und A 5.3.1

Sicherheitskonzept, welche durch das Ministerium der Finanzen während der zweiten NFM-Projektwelle beauftragt wurden. Konsequenz dieser Einschätzung ist, dass im Rahmen der Erneuerung des HKR-Verfahrens für die SAP-basierte Lösung besondere Sicherheitsmaßnahmen umgesetzt werden müssen, die dem hohen Schutzbedarf der Daten gerecht werden. Solche Maßnahmen könnten z. B. sein:

- Ende-zu-Ende-Verschlüsselung bei der Übertragung von Daten über Netzwerke,
- Nutzung digitaler Signaturen zur Sicherung von Integrität und Authentizität,
- Verwendung von Chipkarten zur sicheren Verwaltung von Schlüsseln für die Authentifizierung der Nutzer und digitale Signierung von Daten,
- Einsatz starker kryptografischer Verfahren gemäß Empfehlung der Bundesnetzagentur,
- Protokollierung von Zugriffen, Sicherung der Nichtmanipulierbarkeit von Protokollen.

Aus unterschiedlichen Gründen kam es bei der Umsetzung des Kabinettbeschlusses zu Projektverzögerungen. Insbesondere wurde die landesweite Einführung des NFM auf einen späteren Zeitpunkt verschoben, um drohende Fehlinvestitionen wegen einer Standardisierung von Produkthaushalten auf Bundesebene zu vermeiden. Intensiv wird dagegen seit November 2007 an der Ablösung des bestehenden HKR-Verfahrens ProFiskal durch eine SAP-basierte Lösung gearbeitet. Die Produktivsetzung erfolgt schrittweise und ist für die ersten Landesbehörden im 2. Quartal 2008 geplant. Wir werden diesen Prozess beratend begleiten.

Die landesweite Einführung des modernisierten Verfahrens zum Haushalts-, Kassen- und Rechnungswesen sowie des Neuen Finanzmanagements erfordern die Fortschreibung und Anpassung der jeweiligen Sicherheitskonzepte sowie die rechtzeitige Umsetzung adäquater Sicherheitsmaßnahmen. Dabei ist der hohe Schutzbedarf der in Teilverfahren bearbeiteten Daten zu berücksichtigen.

9.4 Outsourcing des SAP-Systembetriebs im Neuen Finanzmanagement

Seit Mitte 2006 bearbeitete das Ministerium der Finanzen das Projekt SAP-Outsourcing. Ziel dieses Projekts war es, aus wirtschaftlichen Erwägungen den Systembetrieb der zentralen Komponenten des DV-

Verfahrens zum Neuen Finanzmanagement (NFM)[69] vom zentralen IT-Dienstleister des Landes, dem Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben (LDS), zu einem externen Dienstleister zu verlagern. Fragen der Gewährleistung der IT-Sicherheit wurden dabei jedoch nur nachrangig betrachtet.

Von der Auslagerung des Systembetriebs der zentralen SAP-Komponenten waren zunächst insgesamt sieben der acht Pilotbehörden der zweiten Welle des NFM-Projekts betroffen. Eine Ausnahme bildet der Polizeibereich, für den der Zentraldienst der Polizei ein separates SAP-System betreibt. Auf Grund des Beschlusses der Landesregierung zur flächendeckenden Einführung des Neuen Finanzmanagements und zur Erneuerung des Haushalts-, Kassen- und Rechnungswesens werden künftig alle Behörden der Landesverwaltung betroffen sein.

Im Dezember 2006 wurden wir erstmalig detailliert über Einzelheiten der Auslagerung des SAP-Systembetriebs informiert. Auf einer Beratung mit Vertretern des Ministeriums der Finanzen, des zukünftigen Dienstleisters T-Systems und der Firma SAP wurden insbesondere Fragen zur Gewährleistung des Datenschutzes und der IT-Sicherheit sowie zur rechtskonformen Umsetzung des Outsourcings als Datenverarbeitung im Auftrag diskutiert. Schnell wurde deutlich, dass noch erhebliche Defizite und Unklarheiten sowohl im inhaltlich-konzeptionellen Bereich als auch bei der praktischen Umsetzung der Sicherheitskonzepte bestanden. Der ursprüngliche Zeitplan, die Migration des SAP-Produktivsystems zum 1. Februar 2007 abzuschließen, erwies sich als zu knapp.

Zu den wesentlichen Punkten, die vor der Inbetriebnahme des Verfahrens bei T-Systems zu klären waren, gehörte einerseits eine Fortschreibung des existierenden Sicherheitskonzepts für das NFM-Projekt. Hierbei sollten die spezifischen Sicherheitsmaßnahmen im Rechenzentrum des neuen Dienstleisters unter Berücksichtigung des Outsourcings definiert und deren Umsetzung vor Ort geprüft werden. Andererseits war aus unserer Sicht eine Anpassung des Sicherheitskonzepts für das Landesverwaltungsnetz (LVN) erforderlich. Hintergrund ist, dass sich das Rechenzentrum der Firma T-Systems für die Abwicklung des SAP-Systembetriebs in Frankfurt/Main befindet und somit das LVN zum Dienstleister hin geöffnet werden muss. Die neue Rolle des LDS nach dem Outsourcing beschränkt sich darauf, einen zentralen Übergabepunkt für die Weiterleitung der NFM-Daten zu T-Systems bereitzustellen. Den durch die Öffnung des LVN entstehenden potentiellen Risiken auch für andere im LVN betriebene Verfahren ist durch geeignete Sicherheitsmaßnahmen zu begegnen.

---

[69] vgl. A 9.3

Mehrfach wiesen wir die Projektverantwortlichen auf diese Forderungen hin. Leider wurden sie nur zum Teil erfüllt. Insbesondere beauftragte das Ministerium der Finanzen eine externe Firma mit der Fortschreibung des NFM-Sicherheitskonzepts. Darin sind zwar die Maßnahmen, welche im Rechenzentrum von T-Systems realisiert werden müssen, aufgezählt, eine Prüfung auf deren tatsächliche Umsetzung fand jedoch nicht statt. Zum Problem der Absicherung der Schnittstelle im LVN und der Öffnung des LVN zu T-Systems machte das Ministerium der Finanzen keine Ausführungen.[70]

Trotz unserer Bedenken erteilte das Ministerium der Finanzen am 28. Februar 2007 die Freigabe für das Outsourcing und vollzog die Migration der zentralen SAP-Verfahrenskomponenten in das Rechenzentrum zu T-Systems. Der Produktivbetrieb dort läuft seit dem 1. März 2007. Diese Entscheidung war für uns Anlass, kurzfristig alle laut Brandenburgischem Datenschutzgesetz erforderlichen Unterlagen zur Auslagerung des Verfahrens anzufordern. Die Prüfung der Dokumente offenbarte eine Reihe von Mängeln und Lücken:

- fehlender Nachweis der Umsetzung und der Wirksamkeit der Sicherheitsmaßnahmen bei T-Systems vor der Erteilung der Freigabe für die Auslagerung des Verfahrens,

- fehlende Berücksichtigung der Risiken, die durch die Öffnung des LVN zu T-Systems entstehen können,

- unvollständiges und z. T. fehlerhaftes Verfahrens- und Anlagenverzeichnis,

- fehlende Anlagen zum Vertrag über die Datenverarbeitung im Auftrag, fehlende angepasste Servicevereinbarung mit dem LDS,

- fehlender Nachweis der Einhaltung der gesetzlichen Unterrichtungspflichten über die Datenverarbeitung im Auftrag,

- fehlende Beteiligung des behördlichen Datenschutzbeauftragten des Ministeriums der Finanzen im Outsourcing-Projekt,

- fehlende Beteiligung der Personalräte der einzelnen Pilotbehörden trotz wesentlicher Änderung des Verfahrens.

Wegen der aufgezählten Verstöße gegen das Brandenburgische Datenschutzgesetz wurde die Auslagerung des SAP-Systembetriebs gegenüber dem Ministerium der Finanzen formal beanstandet. Mit seiner Antwort auf diese Beanstandung übersandte uns der Minister eine Reihe von Unterlagen,

[70] zu diesem speziellen Problem vgl. A 5.3.1

aus denen die Nacharbeiten zur Beseitigung der festgestellten Mängel ersichtlich waren. Insbesondere wurden die formalen Erfordernisse (Verfahrens- und Anlagenverzeichnis, Vertragsunterlagen, Unterrichtungspflichten) von Seiten der Projektverantwortlichen erfüllt.

Durch eine externe Beratungsfirma fand außerdem eine Prüfung der Umsetzung der Sicherheitsmaßnahmen im LDS und im LVN statt. Diese Prüfung führte zu dem Ergebnis, dass in diesen Bereichen fast alle erforderlichen Sicherheitsmaßnahmen umgesetzt sind. Wir gehen davon aus, dass zügig an der Realisierung der noch fehlenden Maßnahmen gearbeitet wird. Ausdrücklich von dem Prüfauftrag ausgenommen waren die Schnittstelle zwischen dem LVN und dem Weitverkehrsnetz zu T-Systems sowie das Rechenzentrum von T-Systems selbst. Mit der Klärung der ersten Frage befasst sich inzwischen eine Arbeitsgruppe unter Leitung des Ministeriums des Innern. Zum Nachweis, dass alle laut Sicherheitskonzept erforderlichen Maßnahmen bei T-Systems umgesetzt sind, liegt den Unterlagen ein entsprechendes Schreiben des Dienstleisters bei. Fraglich ist, inwieweit das Ministerium der Finanzen damit seiner Kontrollverantwortung als Auftraggeber bei der mit dem Outsourcing verbundenen Datenverarbeitung im Auftrag nachkommt. Wir behalten uns eine entsprechende eigene Prüfung vor.

Beauftragt eine öffentliche Stelle einen Dienstleister mit der Abwicklung des IT-Systembetriebs für ein DV-Verfahren, sind vor der Produktivsetzung alle erforderlichen Maßnahmen für die Gewährleistung von Datenschutz und IT-Sicherheit zu realisieren. Dies gilt auch bei einem Wechsel des Dienstleisters.

Teil B

Akteneinsicht und Informationszugang

1 Strafgebühr wegen einer Beschwerde bei der Landesbeauftragten?

Den Schriftwechsel zwischen dem Wirtschaftsministerium und einem Innungsverband durfte der Antragsteller zwar ohne Einschränkungen einsehen, eine Fotokopie wurde ihm jedoch mit der Begründung verweigert, das Akteneinsichts- und Informationszugangsgesetz sehe lediglich die Gewährung der Einsicht in die Originale vor.

In der Korrespondenz zwischen der Behörde und dem Verband ging es um die Gebührenkalkulation für das Schornsteinfegerhandwerk. Zunächst sagte das Ministerium dem Antragsteller zu, ihm gegen Auslagenerstattung Fotokopien fertigen zu wollen, überlegte es sich später aber anders. Die Vervielfältigung von Akten entspreche nicht dem Anliegen des Akteneinsichtsrechts, begründete das Ministerium seine schriftliche Ablehnung. Die Akteneinsicht selbst wurde dem Antragsteller aufgrund dieses Meinungswandels ausdrücklich nicht in Rechnung gestellt.

Darüber hinaus argumentierte das Ministerium mit einem vermeintlich zu erwartenden Rechtsmissbrauch durch den Antragsteller. Als Beleg hierfür wurde der Landesbeauftragten das Ergebnis einer Internet-Recherche über die politischen Absichten des Antragstellers präsentiert.

Richtig ist, dass das Akteneinsichts- und Informationszugangsgesetz keine Regelung trifft, ob Fotokopien eingesehener Dokumente herauszugeben sind. Dies bedeutet jedoch nicht, dass die Herausgabe nicht vorgesehen ist, sondern lediglich, dass die Akten führende Stelle nach pflichtgemäßem Ermessen über ein entsprechendes Begehren zu entscheiden hat. Das Informationszugangsrecht ist nur erfüllt, wenn der Antragsteller die Informationen vollständig erhält und dauerhaft über sie verfügen kann. Wenn die Offenlegung außer Frage steht, die technischen Möglichkeiten vorhanden sind und der Aufwand für das Kopieren nicht unangemessen hoch ist, reduziert sich dieses Ermessen jedoch regelmäßig gegen null. Die Ablehnung der Herausgabe von Fotokopien mit der alleinigen Begründung, das Gesetz sehe dies nicht vor, stellt eine Nichtausübung des Ermessens und somit eine unzulässige Verweigerung des Informationszugangsanspruchs dar.

Durch den Verweis auf die politischen Aktivitäten des Antragstellers verwendete das Ministerium eines der ausdrücklich angestrebten Ziele des Akteneinsichts- und Informationszugangsgesetzes – nämlich die Stärkung der Möglichkeiten zur politischen Mitgestaltung – als Argument gegen einen vollständigen Informationszugang, indem es die politische Mitgestaltung als Rechtsmissbrauch einstufte. Hinzu kommt, dass das Recht auf Akteneinsicht ohne Voraussetzung gilt. Weder bedarf es eines berechtigten Interesses an der Einsichtnahme, noch darf die Verwaltung den Antragsteller nach seinen Absichten fragen, geschweige denn ohne sein Wissen im Internet entsprechende Recherchen anstellen. Dadurch verstieß die Behörde sowohl gegen den Grundsatz der Voraussetzungslosigkeit des Akteneinsichtsrechts als auch gegen das datenschutzrechtliche Erfordernis einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Nachdem das Ministerium die im weiteren Verlauf mehrfach ergangenen Hinweise und Vermittlungsangebote der Landesbeauftragten unbeantwortet ließ, sprach diese eine Beanstandung aus und forderte es auf, ihr mitzuteilen, wie das Informationszugangsrecht des Antragstellers gewährleistet und vergleichbare Vorfälle künftig vermieden werden sollen.

In Reaktion auf die Beanstandung erließ das Ministerium einen Änderungsbescheid an den Antragsteller. Darin hielt es an der Verweigerung der Herausgabe der Fotokopien fest. Es erklärte die Auskundschaftung der politischen Aktivitäten des Antragstellers sogar für entscheidungsrelevant und begründete sie mit der Pflicht zur umfassenden Aufklärung und Beweiserhebung. Während dem Antragsteller im ursprünglichen Ablehnungsbescheid noch die Kostenfreiheit für die Akteneinsicht zugesichert wurde, erklärte die Behörde in ihrem Änderungsbescheid, dies habe sich lediglich auf die Erstattung der – nicht angefallenen – Auslagen bezogen, nicht auf die Gebühr für die Einsichtnahme. Obwohl sich in der Sache keine Änderung ergeben hatte, erhob das Ministerium nunmehr eine Gebühr in Höhe von 51 Euro. Ein gegebenenfalls vorhandenes Vertrauen in die Gebührenfreiheit sei nicht schutzwürdig. Für den Antragsteller bedeutete dies, dass ihm im Ergebnis seiner Beschwerde bei der Landesbeauftragten Kosten entstanden sind, deren Erhebung als unzulässige Abschreckungsmaßnahme einzustufen, nahe liegt.

Mit der formalen Beanstandung waren die gesetzlichen Kompetenzen der Landesbeauftragten erschöpft; eine weitere Vermittlung zwischen dem Ministerium und dem Antragsteller hätte keine Erfolgsaussichten gehabt. Dem Petenten blieb nur noch die Klage vor dem Verwaltungsgericht. Der Gesetzgeber bleibt indessen aufgefordert, das Akteneinsichts- und Informationszugangsgesetz um ein ausdrückliches Recht auf Fotokopien zu ergänzen. Dies würde dazu beitragen, in der täglichen Anwendung des Gesetzes aufwändige Diskussionen um eine Selbstverständlichkeit zu vermeiden. Sowohl die In-

formationsfreiheitsgesetze anderer Länder und des Bundes als auch das Umweltinformationsgesetz des Landes Brandenburg sehen längst einen solchen Anspruch vor.

Ist ein Antragsteller der Auffassung, dass ihm Informationen zu Unrecht vorenthalten werden, kann er sich jederzeit mit einer Beschwerde an die Landesbeauftragte wenden. Für die Inanspruchnahme dieses Rechts darf er von der Behörde, gegen die sich seine Beschwerde richtet, in keiner Weise benachteiligt werden.

2 Kommerzielle Weiterverwendung öffentlicher Informationen – gleiches Recht für alle

Die öffentliche Hand verpflichtet sich zuweilen durch Lizenzvereinbarungen, privaten Unternehmen exklusiv und regelmäßig Informationen zur Verfügung zu stellen. Diese bereiten die Daten auf und verkaufen sie in Form höherwertiger Produkte auf dem Markt. Können Konkurrenten auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes verlangen, dass auch ihnen die Informationen in der gleichen Weise übermittelt werden? Diese Frage wurde im Zusammenhang mit den Bekanntmachungen für Ausschreibungstexte des Landes im Internet an uns herangetragen.

Das Akteneinsichts- und Informationszugangsgesetz geht davon aus, dass ein Antragsteller einzelfallbezogen den Zugang zu bestimmten Informationen beantragt. Ein solcher Antrag löst ein klassisches Verwaltungsverfahren aus und endet mit einem Bescheid sowie ggf. einer Gebührenerhebung. Eine regelmäßige Übermittlung stets neu verfügbarer Informationen sieht das Akteneinsichts- und Informationszugangsgesetz (AIG) nicht ausdrücklich vor, schließt es jedoch auch nicht aus. Entscheidet sich die Behörde, nach Ausüben ihres pflichtgemäßen Ermessens, so vorzugehen, muss sie alle Interessenten in der gleichen Weise behandeln.

Das Antragsverfahren bleibt dennoch Kernbestandteil des Akteneinsichts- und Informationszugangsgesetzes. Es soll sicherstellen, dass nur solche Informationen herausgegeben werden, die auf der Grundlage des Gesetzes öffentlich gemacht werden dürfen. Im Falle der Ausschreibungsblätter ging es jedoch nicht um die Prüfung der Offenlegung – schließlich hat die öffentliche Stelle die Informationen ja ausschließlich zum Zweck ihrer Veröffentlichung erstellt. Zu klären war vielmehr, ob und in welchem Umfang die öffentliche Verwaltung das Recht hat, in Lizenzverträgen eine Exklusivität mit einzelnen Vertragspartnern zu vereinbaren.

Der Lizenzvertrag zu den Ausschreibungstexten sah vor, dass der Lizenznehmer die unbearbeiteten Texte vom Land erhält, aufbereitet, in gedruckter Form herausgibt und (kostenpflichtig) vertreibt. Auch hatte er sie im Internet entsprechend zu publizieren. Der Lizenznehmer wurde verpflichtet, Mitbewerbern die ihm vom Land zur Verfügung gestellten, noch unbearbeiteten Informationen gegen eine angemessene Gebühr für den Aufwand der Übermittlung weiterzuleiten, damit diese sie ebenfalls im Internet in einer eigenen Version anbieten können. Dadurch sollen Mitbewerber einerseits nicht von Informationen ausgeschlossen werden, sich andererseits aber auch keinen ungerechtfertigten Kostenvorteil sichern können.

Alle Unternehmen müssen die Informationen zu den gleichen Bedingungen, d. h. auch zu den gleichen Kosten beziehen können. Eine Befreiung des Lizenznehmers von diesen Kosten ist zulässig, wenn eine entsprechende Gegenleistung vereinbart wird. Im vorliegenden Fall verpflichtete sich der Lizenznehmer zum Druck und Vertrieb der Ausschreibungsblätter. Hierfür wären dem Land ohne einen Lizenzvertrag, d. h. wenn es selbst für die Herausgabe hätte sorgen müssen, Kosten angefallen. Die Tatsache, dass die Kosten des Lizenznehmers über den Markt refinanziert werden, spielt dabei keine Rolle.

Zwar konnte über die zunächst strittige Höhe der Kosten für die Weiterleitung der Ausschreibungstexte durch den Lizenznehmer an dessen Mitbewerber schließlich Einvernehmen erzielt werden. Jedoch sollte grundsätzlich nicht das lizenzierte Unternehmen für die Gleichbehandlung der Mitbewerber in die Verantwortung genommen werden, sondern das Land selbst als Lizenzgeber zuständig sein.

Die entscheidende Rechtsgrundlage für diesen Fall war nicht das Akteneinsichts- und Informationszugangsgesetz, sondern die Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors. Sie beinhaltet unter anderem ein grundsätzliches Verbot von Ausschließlichkeitsvereinbarungen. Bereits bestehende Vereinbarungen, die eine solche Exklusivität beinhalten, werden bei Vertragsablauf, spätestens jedoch am 31. Dezember 2008 beendet. Lizenzen dürfen also den freien Wettbewerb nicht behindern. Mit der Richtlinie bestehen innerhalb der Europäischen Union erstmals einheitliche Konditionen für die Vermarktung von Informationen des öffentlichen Sektors durch private Unternehmen.

Die Richtlinie wurde mit dem Informationsweiterverwendungsgesetz vom 13. Dezember 2006[71] in deutsches Recht gefasst. Das Gesetz gilt auch für

[71] Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen vom 13. Dezember 2006 (BGBl. I S. 2913)

die öffentlichen Stellen in Brandenburg. Es regelt nicht den Zugang zu, sondern lediglich die kommerzielle Weiterverarbeitung von Informationen, die auf der Grundlage bereits bestehender Zugangsregelungen – also beispielsweise des Akteneinsichts- und Informationszugangsgesetzes – offen zu legen sind.

Das Informationsweiterverwendungsgesetz schreibt für die Vermarktung von Informationen des öffentlichen Sektors durch private Unternehmen einheitliche Konditionen vor. Der freie Wettbewerb in der Informationswirtschaft soll unter anderem durch das grundsätzliche Verbot von Ausschließlichkeitsvereinbarungen gestärkt werden. Die Regelungen des Akteneinsichts- und Informationszugangsgesetzes bleiben davon unberührt.

3 Anonyme Prüfungsstatistiken sind keine Geheimnisse

Eine als Zweckverband organisierte kommunale Ausbildungseinrichtung wurde gebeten, statistische Informationen zur Situation der Auszubildenden herauszugeben, reagierte auf diesen Antrag jedoch nicht. Zunächst schien es sich lediglich um ein leicht auszuräumendes Fristversäumnis der Verwaltung zu handeln …

... tatsächlich zeigte sich aber, dass der Zweckverband absichtsvoll in Untätigkeit verharrte. Unsere Bitte um eine Stellungnahme zum Sachverhalt, die wir stets einholen, um zu einer objektiven Beurteilung der Angelegenheit zu gelangen, wurde zunächst ignoriert, aufgeschoben und später nur unvollständig beantwortet. Die Antragstellerin interessierte sich für die Auswertung der Abschlussprüfungen aus den Jahren 2003 bis 2005, erhielt allerdings lediglich vorläufige Informationen über die Abschlussprüfungen des Einstellungsjahrgangs 2003, also des Jahrgangs, der erst im Jahre 2006 die Prüfung ablegte. Sie bestand auf einer vollständigen Information aus den von ihr angegebenen Jahren. Daraufhin lehnte der Verband ihren Antrag mit der Begründung ab, es lägen keine weiteren Auswertungen vor, da die genannten Ausbildungsjahrgänge erst nach einer dreijährigen Ausbildung ihre Abschlussprüfung ablegten und diese naturgemäß erst nach erfolgter Prüfung ausgewertet werden könnten. Personenbezogene Daten und eine „grundsätzliche Erörterung“ durch die Gremien des Zweckverbandes stünden darüber hinaus einer Herausgabe entgegen. Weshalb der bereits erfolgten Offenlegung der Daten zum Einstellungsjahrgang 2003 diese Gründe nicht entgegenstanden haben sollen, erklärte der Verband nicht.

Dass der Schutz personenbezogener Daten der Herausgabe einer anonymen Statistik nicht entgegensteht, ist ebenso offensichtlich wie die Tatsache, dass eine Erörterung in den Verbandsgremien den Anspruch, den das Akteneinsichts- und Informationszugangsgesetz jedem einzelnen gibt, nicht zu erset-

zen vermag. Ausreichend deutlich schien uns auch der Informationswunsch der Antragstellerin gewesen zu sein, die Auswertungen der in den Jahren 2003 bis 2005 durchgeführten Prüfungen zu erhalten und nicht die in der Zukunft liegenden Abschlüsse der in diesen Jahren begonnenen Ausbildungen. Die weit nach Verstreichen der einmonatigen Regelbearbeitungsfrist erfolgte Ablehnung enthielt daher keine auf die Ausnahmetatbestände des Gesetzes bezogene Begründung. Außerdem kam der Zweckverband seiner Pflicht, die Landesbeauftragte zu unterstützen, nur zögerlich und unvollständig nach. Die Landesbeauftragte beanstandete diese Verstöße gegen das Akteneinsichts- und Informationszugangsgesetz.

In seiner Stellungnahme zu dieser Beanstandung erläuterte der Zweckverband – elf Monate nach Antragstellung – erstmals seine rechtliche Auffassung: Danach sei er als Prüfungseinrichtung im Bereich von Unterricht und Prüfung tätig. Aufgrund des Bezugs der beantragten Informationen zu diesen Aufgaben käme das Akteneinsichts- und Informationszugangsgesetz nicht zur Anwendung. Trotz eindeutiger Erläuterung unsererseits, auf welchen Prüfungszeitraum sich das Einsichtsbegehren der Antragstellerin bezieht, wiederholte der Verband, dass Informationen der genannten Einstellungsjahrgänge noch nicht vorlägen. Er ließ allerdings erkennen, dass für die von der Antragstellerin bezeichneten Jahrgänge ohnehin keine Statistiken vorlägen. Es müsste also auf die personenbezogenen Prüfungsunterlagen der einzelnen Auszubildenden zurückgegriffen werden, die aus Datenschutzgründen nicht offenbart werden könnten.

Der Verband ging zu Recht davon aus, dass er nicht verpflichtet ist, Auswertungen, die nicht existieren, für die Antragstellerin zu erstellen. Auch kommt die Einsicht in die persönlichen Prüfungsunterlagen der Auszubildenden nicht in Frage. Um diese Selbstverständlichkeiten klarzustellen, hätte es allerdings keiner elf Monate bedurft. Für nicht zutreffend halten wir hingegen die Aussagen des Zweckverbands zum Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes, das Prüfungseinrichtungen vom Informationszugang ausnimmt, soweit sie im Bereich von Prüfungen tätig werden. Diese Bestimmung bezweckt lediglich, zu verhindern, dass die Inhalte beabsichtigter Prüfungen bekannt werden. Eine Übersicht über die Ergebnisse bereits stattgefundener Klausuren hat keinerlei Bezug zu deren Inhalt und ist von dieser Regelung nicht umfasst. Ihre Erstellung ist eine Verwaltungsaufgabe, die dem Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes unterliegt.

Ein Antrag auf Informationszugang ist in der Regel spätestens nach einem Monat zu bescheiden; wird er abgelehnt, muss dies unter Bezugnahme auf die gesetzlichen Ausnahmetatbestände schriftlich begründet werden. Der Herausgabe anonymer Statistiken über die Ergebnisse bereits erfolgter Prüfungen steht das Akteneinsichts- und Informationszugangsgesetz nicht entgegen.

4 Wenn die Verwaltung nichts tut, entstehen keine Akten

Nachdem die Stadtverordneten beschlossen hatten, es mögen Gedenktafeln für die Opfer des Stalinismus aufgestellt werden, interessierte sich ein Antragsteller dafür, was die Verwaltung getan hat, um diesen Beschluss umzusetzen.

An bestimmten Schulen sollten Gedenktafeln angebracht werden, die an die in der Zeit des Stalinismus ermordeten Schüler erinnern. Der Antragsteller nahm an, dass zur Umsetzung dieses Beschlusses zumindest ein Schriftverkehr zwischen der Stadtverwaltung und den betroffenen Schulen vorliegen müsste und beantragte, diesen einzusehen. Sein Antrag wurde jedoch mit der Begründung abgelehnt, dass verwaltungsinterne Unterlagen nicht übersandt werden könnten. Sein fortgesetztes Bemühen um den Informationszugang wurde von der Stadtverwaltung in den folgenden dreieinhalb Monaten mit Zwischenbescheiden, Urlaubsankündigungen und Zuständigkeitsverweisen beantwortet. Schließlich beschwerte sich der Antragsteller bei uns.

Die maximale Bearbeitungsfrist für Anträge auf Akteneinsicht beträgt einen Monat. Zudem muss für die Geheimhaltung von Informationen ein gesetzlicher Ausnahmetatbestand vorliegen. Die Begründung, Unterlagen seien „verwaltungsintern“, reicht hierfür nicht aus. Schließlich ist es gerade Ziel des Akteneinsichts- und Informationszugangsgesetzes, dass Verwaltungsinterna, denen kein besonderer Schutzbedarf zukommt, öffentlich bekannt werden. Nachdem wir die Stadt hierauf hingewiesen und um eine umgehende Bearbeitung gebeten haben, erneuerte sie im Ergebnis zwar die Ablehnung des Antrags, teilte dem Antragsteller aber in einer geänderten Begründung mit, dass sie gar nicht über Unterlagen verfüge, aus denen die gewünschten Informationen hervorgehen. Die Frage, was die Verwaltung getan hat, um den Beschluss der Stadtverordneten umzusetzen, hat sich für den Antragsteller somit beantwortet.

Bereits die Tatsache, dass zur Einsicht beantragte Akten gar nicht existieren, kann für den Antragsteller eine wertvolle Information sein. Auch wenn in einem solchen Fall eine Einsicht naturgemäß tatsächlich unmöglich ist, kann der Antrag nicht einfach abgelehnt werden, vielmehr muss eine Mitteilung darüber erfolgen, dass die begehrten Unterlagen nicht vorliegen.

5 Agrarsubventionen der EU: Wer bekommt wie viel?

Wie hoch sind die einzelnen Subventionen aus den europäischen Fördermitteln, die das Land Brandenburg an landwirtschaftliche Betriebe auszahlt? Und vor allem: Wer bekommt sie? Längst haben andere Mitgliedsstaaten und auch ein deutsches Bundesland Ross und Reiter genannt. Großbritannien wunderte sich darüber, dass ausgerechnet die königliche Familie den größten Anteil der Fördermittel erhält; in Nordrhein-Westfalen stellte sich heraus, dass vor allem Großkonzerne − sogar Energieunternehmen − nicht unerhebliche Agrarförderungen erhalten. In Brandenburg wurde hingegen die Herausgabe entsprechender Informationen vom Land teilweise abgelehnt.

Fördermittel, die an Ein-Personen-Betriebe ausgezahlt werden, stellen personenbezogene Daten dar, die, soweit keine Zustimmung der Betroffenen vorliegt, nach dem Akteneinsichts- und Informationszugangsgesetz in der Regel nicht offenbart werden dürfen. Der größte Teil der Fördermittel wird jedoch an größere landwirtschaftliche Unternehmen ausgezahlt, sodass der Datenschutz ihrer Offenlegung nicht entgegensteht. Allerdings schützt das Gesetz auch Unternehmensdaten sehr weit gehend. Diese Bestimmung führte dazu, dass eine Initiative den Zugang zu den von brandenburgischen Behörden ausgezahlten Agrarförderungen nur erhalten hat, soweit die jeweiligen Unternehmen damit einverstanden waren. Für die Antragsteller waren diese Informationen zu lückenhaft, um sich ein vollständiges Bild von den Auswirkungen der Fördermittelvergabe auf die Landwirtschaft zu machen.

Informationsfreiheitsgesetze anderer Bundesländer schützen – anders als das brandenburgische Akteneinsichts- und Informationszugangsgesetz – keine Daten, bloß weil sie einen Bezug zu einem Unternehmen aufweisen. Sie nehmen lediglich Betriebs- und Geschäftsgeheimnisse von dem Recht auf Informationszugang aus. Damit ist nur jener wettbewerbsrechtlich relevante Kern von Unternehmensdaten geschützt, mit Hilfe dessen sich Konkurrenten auf dem Markt einen unzulässigen Vorteil verschaffen könnten. Subventionen gehören nicht zu den Betriebs- und Geschäftsgeheimnissen. Ob sie gezahlt werden, entscheidet sich nicht auf dem freien Markt, sondern ist abhängig von den für alle Betriebe gleichermaßen geltenden Förderkriterien. Ihre Offenlegung ist nicht geeignet, dem Unternehmen zu schaden.

Betrachtet man Informationen über Agrarförderungen als Umweltinformationen, käme nicht das Akteneinsichts- und Informationszugangsgesetz, sondern das Umweltinformationsgesetz vorrangig zur Anwendung. Im Hinblick auf die Daten von Unternehmen sieht es – wie die Informationsfreiheitsgesetze anderer Länder auch – nur den Schutz von Betriebs- und Geschäftsgeheimnissen vor. Auf seiner Grundlage könnten die Fördermittelempfänger und die Höhe der Gelder auch für Brandenburg offen gelegt werden. Nach der gesetzlichen Begriffsbestimmung gelten als Umweltinformationen Maßnahmen oder Tätigkeiten, die sich auf die Umweltbestandteile wie Luft, Wasser, Boden, Landschaft und natürliche Lebensräume etc. auswirken oder wahrscheinlich auswirken. Agrarförderungen der Landwirtschaft werden für Investitionen genutzt, die unmittelbare Umweltauswirkungen haben, sei es für die Düngung von Nutzflächen, die mit Emissionen verbundene Tierhaltung oder die Veränderung der Gewässerstruktur. Zahlreiche Förderungen werden sogar explizit mit dem Ziel begründet, den Zustand der Umwelt zu verbessern. Dennoch urteilte ein nordrhein-westfälisches Verwaltungsgericht in derselben Angelegenheit, dass der Zweck der Fördermaßnahmen bei der Beurteilung, ob es sich um eine Umweltinformation handelt, im Vordergrund stehe. Da es vor allem um Zahlungen im Rahmen der Verbesserung der Wettbewerbsfähigkeit der Erzeuger gehe, komme das Umweltinformationsgesetz als Rechtsgrundlage für die Bearbeitung des Antrags deshalb nicht in Betracht, weil es sich gar nicht um Umweltinformationen handele. Obwohl es sich um die Rechtsprechung aus einem anderen Bundesland handelt, richtet sich das Land Brandenburg nach diesem Urteil und wendet ausschließlich das Akteneinsichts- und Informationszugangsgesetz an.

Während der Informationszugang in Brandenburg noch an restriktiven Bestimmungen des Landesrechts scheitert, hat die Europäische Kommission sich selbst zu vollständiger Transparenz im Hinblick auf die Fördermittel aus dem EU-Haushalt verpflichtet. Künftig wird es eine jährliche Aufstellung der Fördermittelempfänger geben – ab 2008 für die Subventionen aus dem Strukturfonds und ab 2009 auch für die Mittel aus der Gemeinsamen Agrarpolitik. Die Änderungen in den einschlägigen Verordnungen der Europäischen Gemeinschaften gelten auch in Brandenburg unmittelbar; die Veröffentlichung ist voraussichtlich vom Land vorzunehmen. Für die bisher in der Vergangenheit ausgezahlten Fördergelder gilt dies jedoch nicht; die Antragsteller müssen daher auf plausible Daten aus Brandenburg vorerst verzichten.

Dies zeigt deutlich, dass die Vorschriften des brandenburgischen Akteneinsichts- und Informationszugangsgesetzes im Hinblick auf den restriktiven Schutz von Unternehmensdaten den Transparenzzielen des Gesetzes entgegenstehen. Die Landesbeauftragte hält daher eine Änderung dieser Vorschrift für sinnvoll: Lediglich Betriebs- und Geschäftsgeheimnisse sollten

geschützt werden, soweit sie das Interesse der Öffentlichkeit an einer Offenlegung überwiegen.

Während das Akteneinsichts- und Informationszugangsgesetz eine vollständige Transparenz auf dem Gebiet der Agrarförderung verhindert, ermöglicht in Zukunft die Transparenzinitiative der Europäischen Kommission, zu erfahren, welche Betriebe in welcher Höhe gefördert wurden.

6 Kampfmittelbelastung als Umweltinformation?

Um sich über die Belastung eines Geländes zu informieren, auf dem eine Müllverbrennungsanlage geplant war, beantragte ein in einem anderen Bundesland ansässiger Bürger die Herausgabe einer Fotokopie der Bescheinigung über die Kampfmittelfreiheit des entsprechenden Flurstücks. Die Behörde war zwar bereit, ihm die Einsicht in die Originalakten zu gewähren, verweigerte aber die Herausgabe von Fotokopien.

Angaben zur Kampfmittelbelastung und zu deren Beräumung stellen sowohl Informationen zum Zustand der Umweltbelastung (Bodenbelastung) als auch zu umweltrelevanten Maßnahmen und Tätigkeiten (Kampfmittelberäumung) dar. Auch enthalten sie Angaben über mögliche Gefährdungen der menschlichen Sicherheit (Explosionsgefahr). Nach den Begriffsbestimmungen des Umweltinformationsgesetzes handelt es sich bei der Kampfmittelfreiheitsbescheinigung somit eindeutig um Umweltinformationen. Dieser Begriff beschränkt sich keineswegs auf die Aufgaben der Umweltbehörden, sondern bezieht sich auf alle öffentlichen Aufgaben, soweit diese eine Umweltrelevanz aufweisen.

Wird der Zugang zu Umweltinformationen beantragt, ist das Umweltinformationsgesetz des Landes Brandenburg gegenüber dem Akteneinsichts- und Informationszugangsgesetz vorrangig anzuwenden. Es setzt die europäische Umweltinformationsrichtlinie (Richtlinie 2003/4/EG) in Landesrecht um[72] und verweist inhaltlich weit gehend auf das Umweltinformationsgesetz des Bundes. Darin wird dem Antragsteller ein Wahlrecht hinsichtlich der Art des Informationszugangs eingeräumt, von dem nur aus gewichtigen Gründen abgewichen werden darf. Diese Gründe müssen dem Antragsteller mitgeteilt werden. Eine Einschränkung des Wahlrechts stellt eine teilweise Ablehnung des Informationszugangs dar, gegen die der Antragsteller Rechtsmittel einlegen kann.

[72] Umweltinformationsgesetz des Landes Brandenburg (BbgUIG) vom 26. März 2007 (GVBl. I S. 74)

Dass die Weigerung, Fotokopien herauszugeben, für den Antragsteller ein unangemessenes Hindernis bei der Wahrnehmung seiner Rechte darstellen kann, wird an diesem Fall besonders deutlich: Für die Einsichtnahme in ein Dokument, das lediglich drei DIN A4 Seiten umfasst, hätte er eine Tagesreise nach Brandenburg antreten und finanzieren müssen.

Die zuständige Landesbehörde war zunächst der Auffassung, mit dem Angebot, die Originalakten vorzulegen, den Erfordernissen der Informationsfreiheit Genüge getan zu haben. Sie ließ sich jedoch durch unsere Beratung davon überzeugen, dass die Vorschriften des Umweltinformationsgesetzes auch auf den Kampfmittelbeseitigungsdienst anzuwenden sind und übersandte dem Antragsteller die gewünschten Fotokopien.

Das Umweltinformationsgesetz des Landes Brandenburg geht dem Akteneinsichts- und Informationszugangsgesetz vor, soweit Umweltinformationen beantragt werden. Unter diesen Begriff fallen auch solche Daten, die ihre Umweltrelevanz erst auf den zweiten Blick offenbaren.

7 Zweckverbände sind kein rechtsfreier Raum

Eine Bürgerin beantragte bei einem Zweckverband Einsicht in die zu einem Grundstück geführte Akte über den Anschluss an die Abwasserentsorgungsanlage. Die Antragstellerin ist Mitglied einer Erbengemeinschaft und damit Miteigentümerin des Grundstücks. Der Zweckverband verweigerte die Akteneinsicht mit immer neuen Argumenten.

In Bezug auf ihre Eigenschaft als Miteigentümerin des Grundstücks handelt es sich auch um die personenbezogenen Daten der Antragstellerin, sodass sie einen Anspruch auf Akteneinsicht aufgrund des Brandenburgischen Datenschutzgesetzes hat. Da in den Akten auch personenbezogene Daten Dritter (insbesondere der Miterben) enthalten sind, ist eine Abwägung mit deren schutzwürdigen Interessen vorzunehmen. Im vorliegenden Fall sahen wir keinen Grund, die Akteneinsicht zu verweigern.

Der anwaltlich vertretene Zweckverband ignorierte allerdings unsere Argumentation zum datenschutzrechtlichen Anspruch auf Akteneinsicht und stützte seine Ablehnung auf das Akteneinsichts- und Informationszugangsgesetz.

Zunächst behauptete der Zweckverband, das Akteneinsichts- und Informationszugangsgesetz sei für Zweckverbände nicht anwendbar. Es gelte nur für Gemeindeverbände und ein Zweckverband sei kein Gemeindeverband. Es ist zwar korrekt, dass der Zweckverband kein Gemeindeverband ist. Allerdings sind nach dem Gesetz über die kommunale Gemeinschaftsarbeit die für Gemeindeverbände geltenden Vorschriften auch für Zweckverbände anzu-

wenden, sofern gesetzlich nichts anderes bestimmt ist. Da dies nicht der Fall ist, kann kein Zweifel daran bestehen, dass das Akteneinsichts- und Informationszugangsgesetz auch für Zweckverbände gilt.

Darüber hinaus argumentierte der Zweckverband, dass der datenschutzrechtliche Auskunfts- und Akteneinsichtsanspruch von den Regelungen des Akteneinsichts- und Informationszugangsgesetzes verdrängt werde. Auch diese Ansicht ist unzutreffend. Beide Ansprüche wurden zur Durchsetzung unterschiedlicher Grundrechte geschaffen. Geht es im Datenschutzrecht darum zu wissen, wer was bei welcher Gelegenheit über den Antragsteller gespeichert hat, hat das Akteneinsichts- und Informationszugangsgesetz einen völlig anderen Hintergrund. Letzteres soll durch die Transparenz behördlicher Entscheidungen die Wahrnehmung der demokratischen Mitgestaltungsrechte erleichtern. Beide Ansprüche können daher durchaus parallel gelten, wobei hervorzuheben ist, dass der datenschutzrechtliche Anspruch zudem unentgeltlich ist.

Trotz der eindeutigen Rechtslage weigerte sich der Zweckverband weiterhin, Akteneinsicht auf der Grundlage des Brandenburgischen Datenschutzgesetzes zu gewähren und trieb die Antragstellerin in ein möglicherweise Jahre dauerndes verwaltungsgerichtliches Verfahren, um ihre Grundrechte durchzusetzen. Das gesamte Verhalten des Zweckverbandes und seines Anwaltes war offensichtlich darauf angelegt, eine Akteneinsicht unter allen Umständen zu verweigern.

Wir haben das Verhalten des Zweckverbandes deshalb förmlich beanstandet und die Kommunalaufsicht gebeten, die Gewährung der Akteneinsicht im öffentlichen Interesse anzuordnen. Die Kommunalaufsicht teilt zwar unsere Auffassung, sieht sich wegen des laufenden Gerichtsverfahrens aber gehindert, tätig zu werden.

Das Akteneinsichts- und Informationszugangsgesetz gilt auch für Zweckverbände. Begehrt ein Mitglied einer Erbengemeinschaft Einsicht in Akten, die ein zur Erbmasse gehörendes Grundstück betreffen, handelt es sich dabei um seine eigenen personenbezogenen Daten. Der Anspruch richtet sich deshalb in erster Linie nach dem Brandenburgischen Datenschutzgesetz. Gegebenenfalls muss eine Abwägung mit den schutzwürdigen Interessen der übrigen Miterben vorgenommen werden.

8 Akteneinsicht bei Kommunalabgaben

Eine Amtsverwaltung war der Meinung, dass das Akteneinsichts- und Informationszugangsgesetz nicht für solche Informationen gelte, die aus Verfahren nach dem Kommunalabgabengesetz stammen. Sie bat uns zu dieser Frage um unsere Einschätzung.

Die Amtsverwaltung führte mehrere Gründe an, aus denen eine Anwendung des Akteneinsichts- und Informationszugangsgesetzes nach ihrer Auffassung ausgeschlossen sei. Das Kommunalabgabengesetz für das Land Brandenburg verweise auf die Verfahrensvorschriften eines Bundesgesetzes, nämlich der Abgabenordnung. In der Abgabenordnung habe der Gesetzgeber bewusst keine Akteneinsichtsrechte vorgesehen. Da die Abgabenordnung ein Bundesgesetz sei, verdränge sie das Landesrecht, also hier das Akteneinsichts- und Informationszugangsgesetz. Außerdem sei die Abgabenordnung das speziellere Gesetz und verdränge deshalb das allgemeine Informationszugangsrecht.

Die Rechtsauffassung der Amtsverwaltung halten wir für unzutreffend. An der grundsätzlichen Anwendbarkeit des Akteneinsichts- und Informationszugangsgesetzes auch bei kommunalabgabenrechtlichen Angelegenheiten besteht kein Zweifel. Das Kommunalabgabengesetz enthält keine eigenen Verfahrensvorschriften, sondern erklärt eine Reihe von Vorschriften der Abgabenordnung für anwendbar. Der Landesgesetzgeber hat sich also entschieden nur bestimmte, bereits bestehende bundesrechtliche Regelungen in sein Landesgesetz einzubeziehen. Durch diese Einbeziehung werden die bundesrechtlichen Vorschriften der Abgabenordnung zu Landesrecht und können nicht als Bundesrecht vorgehen.

Auch inhaltlich schließt die Geltung einiger Vorschriften der Abgabenordnung die Anwendung des Akteneinsichts- und Informationszugangsgesetzes nicht aus. Das Akteneinsichtsrecht besteht u. a. gegenüber Gemeinden und Gemeindeverbänden, ohne dass eine Einschränkung auf bestimmte Verfahren vorgenommen wird. Wegen des Grundrechtscharakters des Rechts auf Informationszugang können spezielle Gesetze die Geltung des Akteneinsichts- und Informationszugangsgesetzes nur dann einschränken, wenn diese Gesetze diese Einschränkung ganz ausdrücklich vorsehen. Dies ist weder im Kommunalabgabengesetz noch bei der Abgabenordnung der Fall.

Es ist zwar richtig, dass der Gesetzgeber der Abgabenordnung im Jahre 1977 ausdrücklich kein Recht auf Akteneinsicht vorgesehen hat. Dies bezieht sich aber nur auf die Rechte der Verfahrensbeteiligten, jedoch nicht auf das Akteneinsichts- und Informationszugangsgesetz, das der Wahrnehmung eines völlig anderen Rechtes als des der Verfahrensbeteiligten dient.

Das Akteneinsichts- und Informationszugangsgesetz sieht vor, dass die Akteneinsicht erst nach Abschluss des kommunalabgabenrechtlichen Verfahrens gewährt wird, allerdings gegebenenfalls wegen entgegenstehender überwiegender öffentlicher oder privater Interessen eingeschränkt werden kann. Da in den Akten aus abgabenrechtlichen Verfahren in der Regel entweder personenbezogene Daten oder Unternehmensdaten enthalten sein dürften, ist eine Akteneinsicht ohne Einwilligung der Betroffenen nur in Ausnahmefällen möglich. Zudem stellt das Akteneinsichts- und Informationszugangsgesetz klar, dass gesetzliche Geheimhaltungspflichten, wie z. B. das bei kommunalen Steuern geltende Steuergeheimnis, unberührt bleiben.

Das Akteneinsichts- und Informationszugangsgesetz ist grundsätzlich für Informationen aus kommunalabgabenrechtlichen Verfahren anwendbar. Seine Ausnahmetatbestände gewährleisten auch in diesen Fällen einen angemessenen Ausgleich zwischen dem Grundrecht auf Informationszugang und überwiegenden öffentlichen und privaten Geheimhaltungsinteressen.

Teil C

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Zwei arbeitsreiche Jahre liegen hinter den Mitarbeiterinnen und Mitarbeitern der Dienststelle. Erwartungsgemäß hat der Bedarf an Beratung und Kontrolle im Bereich der IT-Sicherheit im Land Brandenburg weiter stark zugenommen. Zahlreiche Verfahrenseinführungen wurden von den Mitarbeitern meines Hauses begleitet. Dabei handelte es sich überwiegend um IT-Verfahren der Landesregierung.

Für die Beratung und Kontrolle der Kommunen blieb dadurch weniger Zeit. Da es sich nicht um einen kurzzeitigen Engpass handelt, sondern vor allem um ein Problem der ordnungsgemäßen Aufgabenerfüllung für die Zukunft, hatte ich mich entschlossen, trotz eines allgemeinen Personalabbaus im Land Brandenburg eine neue Informatikerstelle zur Verstärkung des Bereiches Technik und Organisation zu beantragen. So wie die Dimensionen der IT-Vorhaben stetig wachsen, wachsen auch die Anforderungen an ihre Kontrolle und steigt der Beratungsbedarf im Vorfeld. In seiner letzten Sitzung im Dezember 2007 hat der Landtag des Landes Brandenburg die zusätzliche Stelle eines Informatikers verabschiedet. Ich freue mich, diese im Jahr 2008 besetzen zu können und möchte mit diesem Kompetenzzuwachs insbesondere die Beratungsangebote an die Kommunen zur Datensicherheit stärken.

Im Bereich Recht nimmt auch weiterhin die Umsetzung des Hartz-IV-Gesetzes einen breiten Raum ein. Die Zahl der Eingaben ist hoch und die Fälle sind vielfältiger und auch komplizierter geworden. Von einer eingetretenen Routine kann keine Rede sein.

Insbesondere zu den Themen Gesundheit und Kinderschutz waren zahlreiche Gesetzgebungsvorhaben des Ministeriums für Arbeit, Soziales, Gesundheit und Familie zu begleiten. Dies war nicht immer einfach, da die Aufsicht über die für solche Vorhaben relevanten Kliniken fast vollständig dem Innenministerium obliegt. Zahlreiche Innovationen, wie die Einführung von Telemedizin oder anderer Organisationsformen in der Krankenversicherung gestalten die datenschutzrechtlichen Aufgaben in diesem Bereich weiterhin vielfältig.

Der Bereich Öffentlichkeitsarbeit hat in den letzten beiden Jahren eine zunehmende Zahl von Veranstaltungen vorbereitet. Regelmäßige Bürgerberatungen, die Teilnahme an dem Brandenburg-Tag oder Tagen der offenen Tür des Landtages und des Berliner Abgeordnetenhauses waren zu organisieren sowie Broschüren zu erstellen oder neu aufzulegen. Im März 2007 hat unsere Mitarbeiterin aus der Öffentlichkeitsarbeit Frau Regine Perthes unsere Behörde verlassen, um nun das Sekretariat des Landtagspräsidenten zu leiten. Obwohl wir ihren Weggang sehr bedauern, haben wir uns mit ihr über diese Herausforderung gefreut. In einem Auswahlverfahren konnte die Stelle zügig mit Frau Sille Abel neu besetzt werden. Sie setzt die Arbeit von Frau Perthes mit viel Engagement fort.

2 Zusammenarbeit mit dem Landtag

Im September 2006 wurde der 13. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht auf der Grundlage der Stellungnahmen der Landesregierung im Innenausschuss des Landtages beraten. Themen waren die Bedeutung der möglichst frühzeitigen Einbindung der Landesbeauftragten bei der Einführung neuer IT-Verfahren im Hinblick auf erforderliche technisch-organisatorische Maßnahmen sowie die Zusammenlegung der beiden Datenschutzaufsichtsbehörden für den privaten und öffentlichen Bereich. Hierzu hat der Innenausschuss dem Landtag empfohlen, die Landesregierung aufzufordern, bis zum 30. Juni 2008 zu prüfen, ob eine Zusammenführung der Aufsicht über den Datenschutz im öffentlichen und nicht öffentlichen Bereich bei der für den nicht öffentlichen Bereich zuständigen Stelle finanzielle Einsparpotentiale bringen würde und ob diese daher sinnvoll wäre. Das Parlament hat diese Empfehlung in seiner Sitzung am 22. November 2006 aufgenommen.

Im Juni 2007 hat der vom Parlament eingesetzte Sonderausschuss „Normen und Standards“ seinen Abschlussbericht zu Verwaltungsmodernisierung und Bürokratieabbau in Brandenburg vorgelegt. Der Sonderausschuss empfahl dem Ministerium des Innern, die Zuständigkeit für den Datenschutz im privaten Bereich der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu übertragen. In seiner Sitzung im Juli 2007 hat das Parlament den Bericht des Sonderausschusses zur Kenntnis genommen. Nur vier Monate später hat die Mehrheit des Parlaments einen Beschlussantrag zur Zusammenlegung der Datenschutzaufsicht bei der Landesbeauftragten im Zusammenhang mit der Änderung des Brandenburgischen Datenschutzgesetzes leider abgelehnt. Dies ist umso bedauerlicher, als der von der Landesregierung eingebrachte Entwurf des Datenschutzgesetzes ausdrücklich das Ziel des Bürokratieabbaus verfolgt hat.

3 Kooperation mit den behördlichen Datenschutzbeauftragten

Im Berichtszeitraum haben wir die Tradition fortgesetzt, einmal jährlich eine Beratung mit den behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden in unserer Dienststelle durchzuführen.

Die Beratungen werden unverändert gut angenommen. Die behördlichen Datenschutzbeauftragten bringen Themen aus ihrer eigenen Praxis vor Ort in die Diskussion ein. Dabei stellt sich immer wieder heraus, dass selbst in größeren Verwaltungen dem Datenschutz und der organisatorischen Einbindung des behördlichen Datenschutzbeauftragten in die Entscheidungsabläufe immer noch eine nur geringe Bedeutung zugemessen wird. Dies zeigt sich schon daran, dass die behördlichen Datenschutzbeauftragten in vielen Fällen sowohl im Hinblick auf die zur Verfügung stehende Arbeitszeit als auch in Bezug auf ihre Arbeitsbedingungen unzureichend ausgestattet sind.

Inhaltliche Schwerpunkte der Beratungen waren technische und organisatorische Fragen des Datenschutzes (z. B. zu Risikoanalyse, Sicherheitskonzept oder zur Datenverarbeitung im Auftrag), datenschutzrechtliche Aspekte der Kommunalverfassung, der Verarbeitung von Geodaten, des Personaldatenschutzes sowie Fragen zu Akteneinsicht und Informationszugang.

4 Zusammenarbeit auf nationaler Ebene

4.1 Datenschutzbehörden

Im Berichtszeitraum fanden wieder regelmäßige Kooperationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich, dem Ministerium des Innern, statt. Insbesondere die Schnittstellen zwischen öffentlichem und privatem Bereich sind hier von Bedeutung. So kommt es inzwischen durchaus zu gleichartigen Themenbefassungen, wie beispielsweise bei den Netzwerken für gesunde Kinder. Ein Austausch zwischen den Datenschutzaufsichtsbehörden ist in diesen Fällen besonders wichtig, um möglichst gleiche datenschutzrechtliche Anforderungen an die Netzwerke zu stellen. Im Berichtszeitraum haben die Aufsichtsbehörden auch bei der Erstellung eines Lehrangebots zum Thema „Datenschutz für Schüler“ zusammengearbeitet. Das Ministerium des Innern hat das von uns initiierte Projekt im Bereich privaten Datenschutzes mit inhaltlichen Beiträgen unterstützt.

Auch die traditionell gute Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde fortgesetzt. Im Berichtszeitraum

haben wir mit den Berliner Kolleginnen und Kollegen zwei Kurzratgeber zu technischen Themen „RFID-Technologie: Funkchips im Alltag“ und vom „Fingerabdruck bis zur DNA-Analyse – Datenschutz beim Einsatz biometrischer Verfahren“ sowie einen Ratgeber zu Hartz IV erarbeitet und herausgegeben. Der Hartz-IV-Ratgeber ist in beiden Ländern und auch weit darüber hinaus ein so großer Erfolg geworden, dass wir uns freuen, ihn demnächst in einer überarbeiteten Fassung neu auflegen zu können. Dies werden sicher nicht die letzten gemeinsamen Projekte sein, zumal die Zahl der gemeinsamen Behörden beider Bundesländer zunimmt und damit auch die Datenschutzaufsicht stärker abgestimmt werden muss.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Jahre 2006 im Frühjahr und Herbst unter dem Vorsitz des Landesbeauftragten für den Datenschutz Sachsen-Anhalt Herrn Dr. von Bose. Ein Jahr später übernahm der Thüringer Datenschutzbeauftragte, Herr Stauch, den Vorsitz. Wie immer wurden zahlreiche Entschließungen zu aktuellen politischen Themen verabschiedet.[73] Auch hier kristallisierten sich als Schwerpunkte die wachsende Zahl von Zentraldateien und Fragen der Sicherheit heraus. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat außer Entschließungen auch Orientierungshilfen verabschiedet, die die zuständigen Arbeitskreise erarbeitet hatten.[74]

Die Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten haben wieder in zahlreichen Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder mitgewirkt.

4.2 Sitzungen des Arbeitskreises Medien unter Vorsitz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

In den Jahren 2006 und 2007 fanden unter dem Vorsitz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht vier turnusmäßige Sitzungen des Arbeitskreises Medien in Babelsberg, Kleinmachnow, Potsdam und Bonn statt.

Im Arbeitskreis Medien diskutieren die Datenschutzbeauftragten von Bund und Ländern aktuelle und strategische Fragen des Datenschutzes aus den Bereichen Telekommunikations-, Multimedia- und Rundfunkrecht. An einem Teil der Sitzungen des Arbeitskreises nimmt zudem regelmäßig ein Vertreter des Arbeitskreises der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten teil.

---

[73] siehe Anlage 3

[74] siehe Anlage 5

Der Arbeitskreis Medien hat für die Konferenz der Datenschutzbeauftragten Entschließungen gegen die Aushöhlung des Fernmeldegeheimnisses zu Gunsten privater Zwecke im Urheberrecht[75] und zur anonymen Nutzung des digitalen Fernsehens[76] sowie gegen die Einführung der Vorratsdatenspeicherung vorbereitet.[77]

Darüber hinaus aktualisierte der Arbeitskreis die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und Internet am Arbeitsplatz[78] sowie die Orientierungshilfe zu Fragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet.[79]

4.3 Informationsfreiheitsbeauftragte

In den Jahren 2006 und 2007 haben sich die Informationsfreiheitsbeauftragten insgesamt viermal zu gemeinsamen Sitzungen getroffen. Im Jahr 2006 fanden die Sitzungen erstmals unter Leitung des Bundesbeauftragten für den Datenschutz und Informationsfreiheit, Peter Schaar, statt, der durch Inkrafttreten des Bundesinformationsfreiheitsgesetzes auch zum Beauftragten für Informationsfreiheit geworden war. Auch erweiterte sich der Kreis der bisher vier Informationsfreiheitsbeauftragten auf insgesamt acht Beauftragte. Hinzu kamen die Bundesländer Bremen, Mecklenburg-Vorpommern und das Saarland. Die Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland (AGID) wurde in der Sitzung am 26. Juni 2006 in Konferenz der Informationsfreiheitsbeauftragten, kurz IFK umbenannt.

In ihrer Sitzung am 26. Juni 2006 verabschiedete die Konferenz die Entschließung „Verbraucherinformationsgesetze nachbessern“. In der Dezembersitzung 2006, nach dem Scheitern des ersten Gesetzesentwurfs, befasste sie sich in der Entschließung „Verbraucherinformation unverzüglich regeln“[80] erneut mit diesem Thema. Eine weitere Entschließung „Transparenz der Verwaltung im Internet: Eigeninitiative gefragt!“[81] wurde ebenfalls im Dezember 2006 verabschiedet.

Im ersten Halbjahr 2007 übernahm Herr Thilo Weichert für das Land Schleswig-Holstein den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten.

---

[75] Entschließung „Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht“, siehe Anlage 3.6.4

[76] Entschließung „Anonyme Nutzung des Fernsehens erhalten!“, siehe Anlage 3.3.4

[77] vgl. A 1.3.1

[78] siehe Anlage 5 und vgl. A 5.4.4

[79] siehe Anlage 5

[80] siehe Anlage 4.2.2

[81] siehe Anlage 4.2.1

Sie verabschiedete in ihrer Sitzung im Juni 2007 eine Entschließung zu dem Dauerbrenner-Thema Betriebs- und Geschäftsgeheimnis bei Akteneinsicht mit dem Titel „Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken!“.[82] Die zweite Sitzung im Jahr 2007 fand im Dezember unter dem Vorsitz des Landesbeauftragten für Informationsfreiheit der Freien Hansestadt Bremen, Herrn Holst, statt. Ein wichtiges Thema dieser Sitzung war der sehr konstruktive Austausch mit Archivaren zum Thema „Abgrenzung von Archiv- und Informationsfreiheitsrecht“.

5 Öffentlichkeitsarbeit

5.1 Internationales Symposium Informationsweiterverwendung

Zum nunmehr fünften Mal veranstaltete die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht am 4. und 5. Juni 2007 ein Internationales Symposium in Potsdam. Thematisch stehen Fragen der Informationsfreiheit im Vordergrund dieser in zweijährigem Rhythmus stattfindenden Veranstaltungsreihe. Das Symposium beschäftigte sich mit Vermarktung von Informationen des öffentlichen Sektors durch private Unternehmen auf der Grundlage der Weiterverwendungsrichtlinie der Europäischen Gemeinschaften. Diese wird in der Bundesrepublik Deutschland durch das auch für Brandenburg geltende Informationsweiterverwendungsgesetz vom 13. Dezember 2006 umgesetzt.

Neben Referenten aus Brandenburg und der Bundesrepublik nutzten zahlreiche Experten aus der Europäischen Union und den mittel- und osteuropäischen Staaten sowie den USA das Internationale Symposium, um über ihre Erfahrungen mit der Weiterverarbeitung öffentlicher Informationen zu berichten und Einblicke in bereits realisierte Projekte zu geben: Bedarf es überhaupt einer Regelung, um Informationen des öffentlichen Sektors nutzbar zu machen und falls ja, erfüllt das Informationsweiterverwendungsgesetz diesen Zweck? Benötigen wir einen institutionellen Rahmen für seine Umsetzung? Wie groß ist das ökonomische Potenzial und somit der Marktwert von Informationen des öffentlichen Sektors wirklich? Soll der Staat für die Bereitstellung Gebühren verlangen und wenn ja, welche Kosten sind angemessen? In welchem Verhältnis stehen die Regelungen zu den Informationsfreiheitsgesetzen?

Die Präsentationen sowie die rege geführten Aussprachen verdeutlichten, aus welch unterschiedlichen Perspektiven das Thema betrachtet wird. Juristen, Sozialwissenschaftler, Verwaltungspraktiker und Wirtschaftsexperten

[82] siehe Anlage 4.1

beurteilten die Herausforderungen höchst unterschiedlich. Vor allem zeigte sich, dass der Ansatz von Land zu Land unterschiedlich ist und die allen gemeinsame Aufgabe entsprechend vielfältig wahrgenommen wird. Während in Brandenburg zwar bereits langjährige Erfahrungen mit der Informationsfreiheit vorliegen, hat die Diskussion über die Weiterverwendung öffentlicher Informationen gerade erst begonnen.

Das zweitägige Internationale Symposium wurde von etwa 120 Teilnehmern besucht und gemeinsam mit der Alcatel-Lucent Stiftung für Kommunikationsforschung, der Deutschen Gesellschaft für Recht und Informatik e.V. und der Deutschen Telekom AG veranstaltet. Die Vorträge sind auf unserer Website sowie als gedruckte Broschüre veröffentlicht.

5.2 Die Landesbeauftragte auf dem Brandenburg-Tag und den Tagen der offenen Tür in den Landesparlamenten

Forst (Lausitz) war am 2. September 2006 Gastgeber des alle zwei Jahre stattfindenden Brandenburg-Tags. Unter dem Motto „Rosen für Brandenburg“ erwarteten die Besucher in verschiedensten Veranstaltungsbereichen nicht nur Musik, Unterhaltung und Kulinarisches, sondern auch Wissenswertes rund um die Themen Datenschutz und Akteneinsicht. Die Landesbeauftragte bot den Besuchern in einem eigenen Zelt Informationen und persönliche Gespräche hierzu an.

Fragen zum Datenschutz an den Schulen sowie zum Persönlichkeitsschutz für „Hartz-IV“-Empfänger wurden ebenso beantwortet wie solche zum Umgang der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) mit den Daten der Gebührenzahler. Der Schutz vor unerwünschter Werbung und unerlaubtem Adressenhandel ist für viele Bürger ebenfalls ein großes Anliegen. Das Interesse an der Sicherheit der eigenen Privatsphäre beim Surfen im Internet gewinnt an Bedeutung. Auch erkundigen sich immer mehr Besucher nach den Möglichkeiten des Informationszugangs in den brandenburgischen Landes- und Kommunalbehörden.

Der nächste Brandenburg-Tag findet am 6. September 2008 unter dem Motto „Brandenburg feiert königlich“ in Königs Wusterhausen statt. Auch hier wird die Landesbeauftragte mit ihren Mitarbeitern wieder Informationen und Gespräche anbieten und lädt alle Interessierten ein, vorbeizukommen.

Gemeinsam mit dem Bundesrat präsentiert sich das Abgeordnetenhaus von Berlin einmal im Jahr der Öffentlichkeit. Am 13. Mai 2006 sowie am 23. Juni 2007 unterhielt die brandenburgische Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht einen gemeinsamen Informationsstand mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit auf

dem Tag der offenen Tür des Abgeordnetenhauses. Die Besucher, die zu einem beträchtlichen Teil aus Brandenburg kamen, zeigten großes Interesse an den Informationen.

Erstmals fand am 1. September 2007 der Tag der offenen Tür beim Landtag und der Landesregierung in Potsdam statt. Das Parlament und die Landesregierung berichteten über ihre Arbeit, neben Informationsangeboten und Unterhaltung konnten auch der Plenarsaal sowie andere Räumlichkeiten besichtigt werden.

Auf dem Innenhof des Parlaments auf dem Brauhausberg präsentierte sich auch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht. Die Möglichkeit zur persönlichen Beratung wurde vielfach angenommen; zahlreiche Gäste haben die Anwesenheit der Landesbeauftragten in Potsdam genutzt, Fragen zu stellen oder Beschwerden einzureichen. Begehrt war darüber hinaus eine technische Vorführung biometrischer Verfahren: Am Beispiel der Zugangskontrolle durch Fingerabdrücke wurde auf die Gefährdung des Persönlichkeitsschutzes durch eine unkritische Nutzung der Biometrie aufmerksam gemacht. Unsere Teilnahme am ersten Tag der offenen Tür war aus Sicht der Landesbeauftragten ein voller Erfolg.

5.3 Bürgersprechstunden

Für viele Bürger Brandenburgs sind zwar die jeweiligen Kreisverwaltungen oft ohne Umstände zu erreichen, die eher abgelegene Kleinmachnower Dienststelle der Landesbeauftragten hingegen nicht. Die Fahrt nach Kleinmachnow mit öffentlichen Verkehrsmitteln stellt nicht selten eine Tagesreise dar. Für die Klärung von Problemen ist der persönliche Kontakt jedoch oft sehr hilfreich. Um eine persönliche Beratung zu Fragen des Datenschutzes und Informationszugangs möglichst flächendeckend zu gewährleisten, hat die Landesbeauftragte in den zurückliegenden Monaten damit begonnen, Bürgersprechstunden vor Ort anzubieten. Mit Unterstützung der Landräte war es uns möglich, in den Kreisverwaltungen nicht nur mit Informationsständen präsent zu sein, sondern auch in eigens dafür zur Verfügung gestellten Räumen individuell und vertraulich zu beraten. Die behördlichen Datenschutzbeauftragten der jeweiligen Landkreise leisteten dabei tatkräftige Unterstützung. Als günstig haben sich solche Tage erwiesen, an denen ohnehin starker Publikumsverkehr herrscht, also beispielsweise lange Behördentage oder besondere, lokal bedingte Öffnungszeiten.

Im November 2006 fand die erste Bürgersprechstunde der Landesbeauftragten in Prenzlau (Landkreis Uckermark) statt. Im Frühjahr 2007 folgte ein Tag in Forst (Landkreis Spree-Neiße), im Oktober in Beeskow (Landkreis Oder-Spree) und schließlich im November 2007 in Perleberg (Landkreis Prignitz).

Die Landesbeauftragte war stets mit einigen Mitarbeitern für einen gesamten Tag vor Ort. Themenschwerpunkte waren Datenschutzfragen in der Gesundheits- und Sozialverwaltung sowie in kommunalen Angelegenheiten. Insbesondere in Landkreisen, die sich für das sog. „Optionsmodell“, d. h. für die Betreuung und Vermittlung aller „Hartz-IV“-Empfänger in kommunaler Trägerschaft, entschieden haben, standen Fragen zur Rechtmäßigkeit der behördlichen Datenerhebung im Vordergrund: Welche persönlichen Daten darf die Behörde zum Zweck der Gewährung der Unterstützungsleistungen erfragen und verarbeiten? Beachtlich war auch das Interesse an der Akteneinsicht. Durch die Präsenz der Landesbeauftragten in den Kreisverwaltungen gelang es nicht nur, Fragen der Bürger zu beantworten, sondern auch den Behördenmitarbeitern Hinweise für die datenschutzgerechte Bearbeitung der Anträge zu geben. Sowohl die Bürger als auch die Mitarbeiter der Verwaltungen machten von diesem Angebot rege Gebrauch.

Auf Grund dieser ermutigenden Resonanz werden wir auch künftig weitere Regionen des Landes Brandenburg besuchen. Den Landräten, Verwaltungsbeschäftigten und behördlichen Datenschutzbeauftragten, die uns bei der Durchführung der Bürgersprechstunde sehr unterstützt haben, gilt unser besonderer Dank.

5.4 Fortbildungsangebote

5.4.1 Fortbildungen zum Datenschutz

Vorbeugen ist besser als heilen - Beratung kommt vor Kontrolle! Unter diesem Motto haben wir die Zahl unserer Schulungsangebote nochmals deutlich erhöht. Zu Fragen der Informationstechnologie haben Mitarbeiter der Landesbeauftragten in verschiedenen Einrichtungen Fortbildungen zu folgenden Themen gehalten:

- Datenschutz und Datensicherheit,
- Erstellung von IT-Sicherheitskonzepten,
- Internet, Kriminalität und Sicherheit,
- Internet: Technische Risiken, Angriffszenarien und Schutzmaßnahmen,
- Datenschutzprobleme beim SAP-Outsourcing und,
- Datenschutzrechtliche Vorgaben an Personalverwaltungsverfahren.

Auch zu rechtlichen Fragen des Datenschutzes haben wir Schulungen angeboten. Erstmals fand an der Landesakademie für öffentliche Verwaltung eine Datenschutzveranstaltung für Führungskräfte statt. Hier sollte die Schulung bewirken, dass Führungskräfte Datenschutz als eigene Aufgabe begreifen und damit ihre Verantwortung aktiv übernehmen. Außerdem fand an der Landesakademie auch eine allgemeine Einführung in das Datenschutzrecht statt.

Schulungen für behördliche Datenschutzbeauftragte werden auch weiterhin regelmäßig angeboten.

An der Fachhochschule Brandenburg haben zahlreiche Referentinnen und Referenten der Landesbeauftragten einmalig eine Lehrveranstaltung mit mehreren Blockseminaren übernommen, um die Studierenden in das Datenschutzrecht und die IT-Sicherheit einzuführen. Am Ende der Veranstaltung stand eine Prüfung.

Es wurden außerdem Schulungen zum

- Betreuungsrecht,
- zur Lehrerfortbildung,
- zum Eingliederungsverfahren nach SGB VII und,
- zur rechtssicheren Spam-Abwehr

durchgeführt.

5.4.2 Fortbildungen zum Informationszugang

Die Landesbeauftragte hat die Aufgabe, im Konfliktfall zwischen einem Antragsteller, nach dessen Ansicht Informationen herauszugeben sind, und der Verwaltung, die ein Geheimhaltungsinteresse geltend macht, die Rechtslage zu erläutern und gegebenenfalls zu vermitteln. Viele Beschwerden könnten möglicherweise von vornherein durch eine bessere Qualität der Bearbeitung von Informationszugangsanträgen vermieden werden.

Allerdings ist das Informationszugangsrecht zersplittert und kompliziert. Häufig ist schon unklar, auf welcher Rechtsgrundlage die Bearbeitung eines Antrags überhaupt zu erfolgen hat: Neben dem Akteneinsichts- und Informationszugangsgesetz sind spezielle Gesetze wie das Umweltinformationsgesetz, die verfahrensrechtlichen Einsichtsansprüche Beteiligter oder die datenschutzrechtlichen Auskunftsrechte von Personen, deren Daten von der Verwaltung verarbeitet werden, zu beachten. Jede dieser Regelungen basiert auf

eigenen Voraussetzungen und bringt unterschiedliche Rechtsfolgen mit sich. Hinzu kommt, dass sich dieses noch junge Rechtsgebiet sehr schnell verändert. So ist es verständlich, dass die Beschäftigten öffentlicher Stellen eine Hilfestellung bei der Bearbeitung von Anträgen erwarten.

In den Jahren 2006 und 2007 hat die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht vor diesem Hintergrund Schulungen zur Informationsfreiheit angeboten. Die Seminare fanden entweder in den jeweiligen Behörden selbst statt oder wurden durch externe Fortbildungseinrichtungen organisiert. Sie richteten sich beispielsweise an Bauämter, Planungsbehörden, Zweckverbände, Denkmalbehörden oder auch allgemein an Amtsverwaltungen und Gemeinden. Im Mittelpunkt standen die Regelungen des Akteneinsichts- und Informationszugangsgesetzes sowie des Umweltinformationsrechts, aber auch die informationszugangsrechtlichen Besonderheiten der jeweiligen Fachämter fanden Berücksichtigung.

Obwohl die beschränkten personellen Kapazitäten der Landesbeauftragten eine umfangreiche Fortbildungstätigkeit auf dem Gebiet der Informationsfreiheit nicht zulassen, sollen auch künftig weitere Schulungen durchgeführt werden.

5.5 Neue Publikationen der Landesbeauftragten

Um die Grundrechte auf Datenschutz und Informationszugang bekannt zu machen, veröffentlicht die Landesbeauftragte die wichtigsten Rechtsgrundlagen auch als gedruckte Broschüren. In den beiden zurückliegenden Jahren wurden das Informationsfreiheitsgesetz des Bundes sowie Umweltinformationsrecht als neue Bestandteile der Reihe „Brandenburgisches Informationsgesetzbuch“ herausgegeben. Das Akteneinsichts- und Informationszugangsgesetz sowie das Bundesdatenschutzgesetz haben wir – letzteres in aktualisierter Form – neu aufgelegt.

Als Ratgeber, der sich vor allem an die öffentlichen Stellen richtet, hat die Landesbeauftragte ihre Anwendungshinweise zum Akteneinsichts- und Informationszugangsgesetz ebenfalls als Druckbroschüre veröffentlicht. Dabei handelt es sich nicht um einen umfassenden, theoretischen Kommentar, sondern um Hinweise, die ausschließlich aus den Praxiserfahrungen der Landesbeauftragten resultieren sowie um einige Schemata zur Vereinfachung der Fallbearbeitung. Die Anwendungshinweise eignen sich natürlich auch als Information für Antragsteller, die Einzelheiten zu ihrem Recht auf Informationszugang erfahren möchten.

Auch das im Jahr 2006 in Kraft getretene Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende führte bei Antragstellern zu Verunsiche-

rungen beim Ausfüllen der umfangreichen Fragebögen im Rahmen der Beantragung des Arbeitslosengeldes II. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat deshalb zusammen mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit den „Ratgeber zu Hartz IV“ herausgegeben. Er beantwortet unter anderem die Fragen, welche Angaben für die Prüfung der Leistungsgewährung wirklich notwendig sind und welche persönlichen Daten nicht preisgegeben werden müssen. Auch für Behörden, die entsprechende Formulare versenden bzw. die Anträge bearbeiten, enthält der Ratgeber Hinweise.

Umfassend aktualisiert und neu aufgelegt wurde das „Datenscheckheft“, welches es den Betroffenen erleichtern soll, ihre datenschutzrechtlichen Auskunftsansprüche in Anspruch zu nehmen. Es enthält Musterschreiben an unterschiedliche Behörden, mit denen die Auskunft über dort gespeicherte Daten zur eigenen Person oder gegebenenfalls deren Berichtigung beziehungsweise Löschung beantragt wird. Zu den einzelnen Lebensbereichen erläutert das „Datenscheckheft“ zudem in kurzen Hinweisen die geltende Rechtslage.

Die Beiträge der einzelnen Referenten auf dem Internationalen Symposium „Öffentliche Daten auf dem privaten Markt – neue Regelungen zur Weiterverwendung öffentlicher Informationen“, das die Landesbeauftragte am 4. und 5. Juni 2007 in Potsdam durchführte, wurde in einer weiteren Broschüre dokumentiert.

Unter der Überschrift „Vom Fingerabdruck bis zur DNA-Analyse – Datenschutz beim Einsatz biometrischer Verfahren“ hat die Landesbeauftragte anlässlich der Aufnahme des digitalen Fingerabdrucks in den Reisepass ein neues Faltblatt herausgegeben. Es zeigt datenschutzrechtliche Eckpunkte zur Wahrung der Persönlichkeitsrechte bei der Nutzung biometrischer Verfahren. Das ebenfalls neu erschienene Faltblatt „RFID-Technologie – Funkchips im Alltag“ weist auf mögliche Risiken der Ausweitung dieser „Funketiketten“ hin, die in der Lage sind, Objekte und somit auch Personen zu identifizieren und zu lokalisieren.

Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, an denen auch die Landesbeauftragte beteiligt war, haben im Berichtszeitraum vier neue Orientierungshilfen erstellt, die sich vor allem an die öffentlichen Stellen des Bundes und der Länder richten: Die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz informiert über die Anforderungen an den Datenschutz hinsichtlich der bei einer solchen Nutzung anfallenden personenbezogenen Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener. Die Orientierungshilfe zu Datenschutzfragen des Anschlusses

von Netzen der öffentlichen Verwaltung an das Internet zeigt auf, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Auch die Umstellung der Schriftgutverwaltung auf eine datenbankgestützte Verwaltung elektronischer Dokumente muss sich den Anforderungen an den Datenschutz und die Datensicherheit stellen. Die Orientierungshilfe zum Datenschutz bei Dokumentenmanagementsystemen leistet dabei Hilfestellung. Darüber, was bei der Einführung automatisierter Personalinformationssysteme und Personalmanagementverfahren sowie bei Verfahren zur betriebswirtschaftlichen Steuerung der Haushaltswirtschaft einschließlich der Kosten- und Leistungsrechnung aus datenschutzrechtlicher Sicht zu beachten ist, informiert die Handlungsempfehlung „Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung“. Die Orientierungshilfen sind auf der Website der Landesbeauftragten verfügbar.[83] Dies gilt auch für die übrigen hier aufgeführten Publikationen, die zudem kostenlos in gedruckter Form erhältlich sind.

[83] siehe Anlage 5

Anlagen

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

Stand: 31. Dezember 2007

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

Bereich Recht und Verwaltung

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

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

Susann Burghardt
App. 45

Arbeitsgebiete:
- Akteneinsicht und Informationszugang
- Redaktion von Veröffentlichungen
- Koordination des Internetangebots
- Öffentlichkeitsarbeit (außer Presse)

Sven Müller
App. 20

Arbeitsgebiete:
- Bildung, Jugend und Sport

Gabriele Peschenz
App. 22

Arbeitsgebiete:
- Gesundheit
- Gesundheitsdaten allgemein

Marion Bultmann
App. 44

Arbeitsgebiete:
- Arbeit, Soziales und Familie
- Sozialdaten allgemein
- Finanzen

Astrid Oehme
App. 66

Arbeitsgebiete:
- Inneres
- Wirtschaft

Oliver F. Hoff
App. 36

Arbeitsgebiete:
- Personal- und Verwaltungsangelegenheiten
- Büroleitungsaufgaben
- Haushaltsangelegenheiten
- Beschaffungen

Gabriela Berndt
App. 12

Arbeitsgebiete:
- Bibliothek
- Schreibdienst
- Informationsmaterialien

Monika Schäfer
App. 43

Arbeitsgebiete:
- Schreibdienst
- Mitarbeit bei der Öffentlichkeitsarbeit

Sille Abel
App. 42

Bereich Technik und Organisation

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

Gleichstellungsbeauftragte	Gabriela Berndt App. 12
Personalrat	Dr. Thomas Reinke App. 31
Behördlicher Datenschutzbeauftragter	Sven Hermerschmidt App. 40

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

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

3 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

3.1 74. Konferenz vom 25. bis 26. Oktober 2007 in Saalfeld

3.1.1 Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z. B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

3.1.2 Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche – teilweise sensible – Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool

gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

3.1.3 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen

Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematischstatistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

3.1.4 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemei-

nen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

3.2 Entschließung zwischen der 73. und 74. Konferenz vom 8. Juni 2007

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die

europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven, grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die be-

troffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

3.3 73. Konferenz vom 8. bis 9. März 2007 in Erfurt

3.3.1 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i. S. v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S .v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

3.3.2 Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische

Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

3.3.3 GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,

- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

3.3.4 Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

3.3.5 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.

- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.

- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.

- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

3.3.6. Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u. a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z. B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

3.4 72. Konferenz vom 26. bis 27. Oktober 2006 in Naumburg

3.4.1 Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben“ ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten: Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen „Bildungsregisters“ nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

3.4.2 Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung

korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz – Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

- Kennzeichnungspflicht – Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

- Keine heimliche Profilbildung – Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme – Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

- Deaktivierung – Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

3.4.3 Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat – sollen in der Bundesrepublik Deutschland erstmals die

rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z. B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

3.4.4 Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes“ kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden

immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes“ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

3.5 Entschließung zwischen der 71. und 72. Konferenz vom 11. Oktober 2006

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

(bei Enthaltung von Schleswig-Holstein)

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den techni-

schen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,

- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,

- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und

- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,

- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,

- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

3.6 71. Konferenz vom 16. bis 17. März 2006 in Magdeburg

3.6.1 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z. B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

3.6.2 Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

3.6.3 Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat*. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u. a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt – einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Daten-

* KOM (2005) 475 vom 4. Oktober 2005

schutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

3.6.4 Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte – Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung wirtschaftlicher Interessen – zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

4 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

4.1 14. Konferenz am 11. Juni 2007 in Kiel

„Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken!“

Die Wahrung von Betriebs- und Geschäftsgeheimnissen hat für Unternehmen eine besondere Bedeutung. Betriebs- und Geschäftsgeheimnisse können den Wert eines Unternehmens und seine Stellung am Markt erheblich beeinflussen. Bei ihrer Aufgabenerfüllung erhalten öffentliche Stellen bisweilen Kenntnis von Betriebs- und Geschäftsgeheimnissen. Als Bestandteil amtlicher Aufzeichnungen unterliegen die Betriebs- und Geschäftsgeheimnisse den

Informationsfreiheitsgesetzen, sie werden hier aber durch einen Ausnahmetatbestand geschützt.

Die Konferenz der Informationsfreiheitsbeauftragten stellt fest, dass die Auslegung und Anwendung des Ausnahmetatbestandes das Informationsfreiheitsrecht der Bürgerinnen und Bürger übermäßig einschränkt. So führt oft die beträchtliche Rechtsunsicherheit der Behörden bei der Anwendung dieser Bestimmung zu einer besonders restriktiven Auskunftspraxis. Aber nicht jedes Unternehmensdatum ist ein Betriebs- oder Geschäftsgeheimnis. Nach der Rechtsprechung des Bundesgerichtshofes zum Wettbewerbsrecht müssen hierfür folgende Voraussetzungen kumulativ vorliegen:

Es muss sich um Tatsachen handeln, die

- im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehen,
- nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig sind,
- (subjektiv) nach dem erkennbaren Willen des Unternehmens und
- (objektiv) nach dessen berechtigten und schutzwürdigen wirtschaftlichen Interessen geheim gehalten werden sollen (insbesondere, wenn bei Offenbarung ein Schaden eintritt).

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb den Bundes- und die Landesgesetzgeber auf, die gesetzlichen Regeln zu ergänzen und zu präzisieren.

1. Es gibt Betriebs- oder Geschäftsgeheimnisse, bei denen das öffentliche Interesse an der Offenbarung den Schutzbedarf überwiegt. Soweit daher eine Abwägungsklausel in den gesetzlichen Grundlagen noch nicht vorhanden ist, soll sie aufgenommen werden. Dabei muss auch verdeutlicht werden, dass Verträge, die mit der öffentlichen Hand geschlossen werden, nicht grundsätzlich geheimhaltungsbedürftig sind: Wer mit dem Staat Geschäftsbeziehungen eingeht, muss sich darüber im Klaren sein, dass staatliches Handeln besonderen Kontrollrechten unterliegt und damit nicht alle Vertragsinhalte geheim bleiben können.

2. Nach dem Beispiel des Gentechnik- und Chemikalienrechts sollte in Form eines Kataloges klargestellt werden, welche Unternehmensinformationen keine Betriebs- oder Geschäftsgeheimnisse darstellen (z. B. rechtswidriges Verhalten).

3. Kennzeichnungs- und Darlegungspflichten des Unternehmens können die Prüfung des Geheimhaltungsinteresses erleichtern. Vergleichbare Regelungen existieren bereits in anderen Bereichen.

4.2 13. Konferenz am 12. Dezember 2006 in Bonn

4.2.1 Transparenz der Verwaltung im Internet: Eigeninitiative ist gefragt!

Auf Bundesebene sowie in acht Bundesländern gibt es mittlerweile Informationsfreiheitsgesetze, die allen Interessierten die Einsicht in Behördenakten ermöglichen. Wer von diesem Recht Gebrauch machen möchte, steht erst einmal vor der Frage, welche Akten in den Ämtern überhaupt geführt werden. Der Blick auf die Internet-Seiten der einzelnen Behörden hilft dabei nur selten weiter. Übersichtliche Darstellungen des Aktenbestands? Inhaltlich aussagekräftige Dokumente, die über offizielle Verlautbarungen hinausgehen? Leider häufig Fehlanzeige!

Die Praxis in Großbritannien, Slowenien und den Vereinigten Staaten von Amerika zeigt, dass eine andere Herangehensweise durchaus Erfolg verspricht. Dort sind alle Behörden per Gesetz verpflichtet, eine spezielle Website zur Informationsfreiheit anzubieten. Auf dieser Seite informieren sie nicht nur über die Rechtslage zur Akteneinsicht, über die behördlichen Ansprechpersonen und den eigenen Informationsbestand, sondern halten auch einen virtuellen Lesesaal bereit. Dort müssen Dokumente, die bereits mehrfach zur Einsicht beantragt wurden und Daten von allgemeinem Interesse eingestellt werden. Seit Einführung dieser Regelung geht die Anzahl der Anfragen nach Akteneinsicht bei den Behörden deutlich zurück.

Einige Informationsfreiheitsgesetze sehen die Veröffentlichung bestimmter Dokumente bzw. die Meldung an ein zentrales elektronisches Informationsregister für öffentliche Stellen bereits jetzt zwingend vor. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland empfiehlt den Akten führenden Stellen deshalb, ihre Tätigkeit gegenüber der Öffentlichkeit im Internet transparenter zu machen. Damit wird auf der einen Seite den Bürgerinnen und Bürgern der Informationszugang erleichtert und gleichzeitig der Verwaltungsaufwand der öffentlichen Stellen reduziert.

1. Die Veröffentlichung von Organigrammen, Geschäftsverteilungsplänen und Listen mit Ansprechpersonen gehört bereits zum Standard. Darüber hinaus sollten vorhandene Aktenpläne und -verzeichnisse ebenfalls im Internet veröffentlicht werden, damit leichter zu erkennen ist, welche Kategorien von Akten überhaupt geführt werden.

2. Gerade bei größeren Behörden ist der Aktenplan allerdings oft so kompliziert, dass bereits seine interne Verwendung auf Schwierigkeiten stößt. Sinnvoll ist die Veröffentlichung in einem solchen Fall nur, wenn der Aktenplan erläutert oder vereinfacht dargestellt wird. Niemand wird sich freiwillig durch ein hundertseitiges Verzeichnis quälen. Handhabbare Findmittel sind somit Voraussetzung für die Wahrnehmung des Rechts auf Informationszugang.

3. Die meisten öffentlichen Stellen verfügen über Dokumente, die von allgemeinem Interesse sind und ohne weiteres eingesehen werden können. Grundsätzlich gilt: Stehen einem Informationszugang keine Ausnahmegründe entgegen, können die Dokumente im Regelfall auch ins Netz gestellt werden. Viele Kommunen stellen so bereits jetzt die Protokolle öffentlicher Sitzungen ihrer Vertretungen zur Verfügung. Einmal eingestellt, kann jede Person darauf zugreifen. Der Aufwand zur Bearbeitung von Anträgen auf Informationszugang entfällt.

4. Ein Indikator dafür, welche Informationen von allgemeinem Interesse sind, könnte das Kriterium sein, dass ein Dokument bereits zur Einsicht beantragt wurde. Soweit die Behörde diesem Antrag stattgegeben hat, kann das Dokument automatisch ins Netz gestellt werden, um Informationswünsche Anderer zu erfüllen und den Verwaltungsaufwand mit künftigen Anträgen zu vermeiden.

5. Was bedeutet Informationsfreiheit? Wie stellt man einen Antrag auf Akteneinsicht? Und welche Erfolgsaussichten hätte ein solches Begehren? Um solche Fragen zu beantworten, könnte ein Leitfaden oder die Beantwortung häufig gestellter Fragen (FAQ) auf den Seiten der einzelnen Behörden zur Klärung beitragen.

In der Bundesrepublik setzt die Bundesagentur für Arbeit auf diesem Gebiet erste Maßstäbe, indem sie ehemals „interne“ Weisungen und Dokumente nun im Internet veröffentlicht. Die Bürgerinnen und Bürgern können dadurch behördliche Handlungen besser nachvollziehen und ihr Mitspracherecht leichter wahrnehmen.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder stehen Verwaltungen, die ihr Informationsangebot verbessern möchten, jederzeit gerne für eine Beratung zur Verfügung.

4.2.2 „Verbraucherinformation unverzüglich regeln“

Das Verbraucherinformationsgesetz ist vorerst gescheitert. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland bedauert, dass dieses Anliegen damit zunächst ungeregelt bleibt. Das verfolgte Ziel, als Konsequenz aus den Lebensmittelskandalen der letzten Zeit die Informationsansprüche der Verbraucherinnen und Verbraucher zu stärken und mehr Transparenz zu schaffen, ist aber aktueller denn je und bedarf weiterhin dringend einer möglichst umfassenden Regelung. Bund und Länder sind deswegen aufgefordert, dieses für einen wirksamen Verbraucherschutz so wichtige Anliegen mit Nachdruck weiterzuverfolgen und gegebenenfalls auch auf Landesebene umzusetzen.

4.3 12. Konferenz am 26. Juni 2006 in Bonn

Verbraucherinformationsgesetz nachbessern

Die Informationsfreiheitsgesetze im Bund und in einigen Ländern stellen einen wichtigen Beitrag zu mehr Transparenz, Bürgerbeteiligung und gesellschaftlicher Offenheit dar. Folgerichtig bedarf es auch einer größeren Transparenz im Bereich des Verbraucherschutzes. Unter bestimmten Voraussetzungen sollte ein unmittelbarer Informationsanspruch gegen private Unternehmen gesetzlich verankert werden. Auch Daten, die in Unternehmen gespeichert werden, berühren unmittelbar Rechte der Bürgerinnen und Bürger und damit ihr Lebensumfeld. Dies gilt insbesondere bei verbraucherschutzrelevanten Produkten sowie Produkten des Energiemarktes. Die Transparenzrechte der Bürgerinnen und Bürger sollten deshalb in diesem Bereich ebenfalls durch Auskunftsansprüche gesetzlich geregelt werden.

Der Entwurf des Verbraucherinformationsgesetzes, der derzeit im Deutschen Bundestag beraten wird, schafft aber nur unzureichende Transparenzregelungen, die außerdem die Unternehmen nicht ausreichend zur Offenlegung der verbraucherschutzrelevanten Daten verpflichten. Die Informationsfreiheitsbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Verbraucherinformationsschutzgesetz erste Schritte für mehr Transparenz in der Wirtschaft umzusetzen.

Dazu gehören zumindest folgende Verbesserungen:

- die Erweiterung des Gesetzes über Lebens- und Futtermittel hinaus auf sonstige Produkte und Dienstleistungen,

- die Schaffung eines unmittelbaren Rechtsanspruchs auf Informationszugang gegenüber Unternehmen,

- die Schaffung einer Abwägungsregelung zwischen den unterschiedlichen Interessen, die unter Beachtung der tatsächlichen Betriebs- und Geschäftsgeheimnisse der Unternehmen den Betroffenen den Informationsanspruch sichert; amtlich festgestellte Verstöße der Unternehmen gegen verbraucherschutzrelevante Regelungen dürfen dabei nicht als Betriebs- und Geschäftsgeheimnis geltend gemacht werden,

- die Reduzierung der Ausnahmen vom Informationszugang auf wesentliche Ausnahmen und eine verbraucherschutzfreundliche Ausgestaltung des Verfahrens,

- Höchstgrenzen bei der Regelung von Gebühren für die Beauskunftung durch die Betroffenen.

5 Übersicht aller Orientierungshilfen der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat folgende Orientierungshilfen und Handreichungen erarbeitet. Auf der Website der Landesbeauftragten[84] können die einzelnen Dokumente heruntergeladen werden.

- Orientierungshilfe „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (November 2007)
- Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (September 2007)
- Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ (Dezember 2006)
- Orientierungshilfe "Datenschutz bei Dokumentenmanagementsystemen" (März 2006)
- Handlungsempfehlungen „Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung“ (März 2006)
- Orientierungshilfe "Datenschutz in drahtlosen Netzen" (September 2005)
- Handreichung „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“ (November 2004)
- Orientierungshilfe "Datensicherheit bei USB-Geräten“ (November 2004)
- Orientierungshilfe "Sicheres Löschen magnetischer Datenträger" (2004)
- Orientierungshilfe zum Einsatz kryptografischer Verfahren (September 2003)
- Orientierungshilfe "Datenschutz bei Windows XP Professional" (2003)
- Handreichung „Datenschutzgerechtes eGovernment“ (November 2002)
- Empfehlungen zum Datenschutz bei Windows 2000 (2002)

[84] siehe http://www.lda.brandenburg.de → Informationsmaterial

- Orientierungshilfe "Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten" (August 2000)

- Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“ (Oktober 1997)

- Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ (Dezember 1996)

- Orientierungshilfe "Datenschutzrechtliche Protokollierung beim Betrieb Informationstechnischer Systeme" (1994)

6 Abkürzungsverzeichnis

Abs.	=	Absatz
AES	=	Advanced Encryption Standard
AFIS	=	Amtliches Festpunktinformationssystem
AG	=	Arbeitsgruppe
AGID	=	Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland
ALG II	=	Arbeitslosengeld II
ALKIS	=	Amtliches Liegenschaftskataster-Informationssystem
Alt.	=	Alternative
AO	=	Abgabenordnung
App.	=	Apparat
APSIS	=	Automatisierte Personalverwaltung und Stellenbewirtschaftung im Schulamt
ARGE	=	Arbeitsgemeinschaft
Art.	=	Artikel
ATDG	=	Antiterrordateigesetz
ATKIS	=	Amtliches Topographisch-Kartographisches Informationssystem
BA	=	Bundesagentur für Arbeit
BAföG	=	(Förderung nach dem) Bundesausbildungsförderungsgesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgGesBAG	=	Gesundheitsberufeanerkennungsgesetz
BbgMeldG	=	Brandenburgisches Meldegesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgRettG	=	Brandenburgisches Rettungsdienstgesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgStEG	=	Brandenburgisches Standarderprobungsgesetz
BGBl.	=	Bundesgesetzblatt
BKAG	=	Bundeskriminalamtgesetz
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BT	=	Bundestag
BT-Drs.	=	Bundestag-Drucksache
bzgl.	=	bezüglich
BZSt	=	Bundeszentralamt für Steuern
bzw.	=	beziehungsweise
ca.	=	circa
CD	=	Compact Disc
CERT	=	Computer Emergency Response Team

ComVor	=	Computergestützte Vorgangsbearbeitung
DDR	=	Deutsche Demokratische Republik
DFB	=	Deutscher Fußballbund
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DMS/VBS	=	Dokumentenmanagement- und Vorgangsbearbeitungs-system
DNA	=	Desoxyribonuclein Acid (Desoxyribonukleinsäure*)*
Drs.	=	Drucksache
DV	=	Datenverarbeitung
DVB-T	=	Digital Video Broadcasting Terrestrial
EG	=	Europäische Gemeinschaft
ELENA	=	Elektronischer Einkommensnachweis
ELSTER	=	Elektronische Steuererklärung
ENISA	=	Europäische Agentur für Netzwerk- und Informationssi-cherheit
ERP	=	Enterprise Resource Planning
etc.	=	et cetera
EU	=	Europäische Union
FALKE	=	Forcierte Automatisierte Liegenschaftskarte-Einrichtung
FAQ	=	Frequently Asked Questions
ff.	=	folgende (Seiten)
GbR	=	Gesellschaft bürgerlichen Rechts
GewO	=	Gewerbeordnung
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GmbH	=	Gesellschaft mit beschränkter Haftung
GPS	=	Global Positioning System
GPRS	=	General Packet Radio Service
GSTOOL	=	Grundschutztool
GVBl.	=	Gesetz- und Verordnungsblatt
HBCI	=	Homebanking Computer Interface
HeilBerG	=	Heilberufsgesetz
HIDS	=	hostbasierte Intrusion-Detection-Systeme
HKR	=	Haushalts-, Kassen- und Rechnungswesen
HTML	=	Hypertext Markup Language
i. d. R.	=	in der Regel
IDS	=	Intrusion-Detection-Systeme
IFK	=	Konferenz der Informationsfreiheitsbeauftragten
IGLU	=	Internationale Grundschul-Lese-Untersuchung
IMA-IT	=	Interministerieller Ausschuss für Informationstechnik
IMEI	=	International Mobile Equipment Identity
IMSI	=	International Mobile Subscriber Identity

INPOL	=	Informationssystem der Polizeien des Bundes und der Länder
IP	=	Internet Protocol
iPSv	=	Integrierte Personal- und Stellenverwaltung
ISDN	=	Integrated Services Digital Network
i. S. v.	=	im Sinne von
IT	=	Informationstechnik
iTAN	=	indizierte Transaktionsnummer
i. V. m.	=	in Verbindung mit
KBSt	=	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
Kfz	=	Kraftfahrzeug
KG	=	Kommanditgesellschaft
KLR	=	Kosten- und Leistungsrechnung
LAN	=	Local Area Network
LDS	=	Landesbetrieb für Datenverarbeitung und Statistik
LiKa	=	Liegenschaftskataster
LKGBbg	=	Krankenhausgesetz des Landes Brandenburg
LVN	=	Landesverwaltungsnetz
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
NFC	=	Near Field Communication
NFM	=	Neues Finanzmanagement
NIDS	=	Netzbasierte Intrusion-Detection-Systeme
Nr.	=	Nummer
o. g.	=	oben genannt
OHG	=	Offene Handelsgesellschaft
PASS	=	Polizeiliches Auskunftssystem Straftaten
PC	=	Personal Computer
PDA	=	Personal Digital Assistant
PERIS	=	Personalinformationssystem
PIN	=	persönliche Identifikationsnummer
PIM	=	Personal Information Manager
PISA	=	Programm for International Student Assessment
PKI	=	Public Key Infrastruktur
Pkt.	=	Punkt
POLAS	=	Polizeiliches Auskunftssystem
QoS	=	Quality of Service
RBB	=	Rundfunk Berlin-Brandenburg
RFID	=	Radio Frequency Identification
RFS	=	Remote Forensic Software
S.	=	Seite
SGB	=	Sozialgesetzbuch
sog.	=	so genannte
SQL	=	Structured Query Language

SSL	=	Secure Sockets Layer
Steuer-ID	=	Steuer-Identifikationsnummer
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
TAN	=	Transaktionsnummer
TIMSS	=	Trends in Mathematics and Science Study (früher: Third International Mathematics and Science Study)
TK	=	Telekommunikation
U 6 − 9	=	Früherkennungsuntersuchung 6 − 9
u. a.	=	unter anderem
UMTS	=	Universal Mobile Telecommunications System
USB	=	Universal Serial Bus
usw.	=	und so weiter
u. U.	=	unter Umständen
vgl.	=	vergleiche
Viper	=	Verfassungsschutz-Informationsportal für Ermittlung und Recherche
VN	=	Vereinte Nationen
VoIP	=	Voice over IP
WLAN	=	Wireless Local Area Network
WM	=	Weltmeisterschaft
WPA2	=	Protected Access 2
XML	=	Extensible Markup Language
z. B.	=	zum Beispiel
ZEVIS	=	Zentrales Verkehrsinformationssystem
z. T.	=	zum Teil
z. Zt.	=	zurzeit

7 Stichwortverzeichnis