

**Tätigkeitsbericht**  
**des Landesbeauftragten für den Datenschutz**  
**und für das Recht auf Akteneinsicht**  
**zum 31. Dezember 2002**

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung jährlich einen Bericht über seine Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz; § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 13. März 2002 vorgelegten Tätigkeitsbericht 2001 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2002 ab.

Die "Dokumente zu Datenschutz und Informationsfreiheit 2002", auf die in diesem Bericht verwiesen wird, hat der Landesbeauftragte gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit als gesonderten Anlagenband veröffentlicht. Tätigkeitsbericht und Anlagenband sind aus unserem Internetangebot unter <http://www.lida.brandenburg.de> abrufbar.

## **Impressum**

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

Telefon: 03 32 03 / 356-0  
Fax: 03 32 03 / 356-49

E-Mail:  
Internet:

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Gallus Druckerei KG  
Gutenbergstraße 6  
10587 Berlin

**Verzeichnis der öffentlichen Stellen.....8**

**Anlagen**

Anlage 1 Allgemeine datenschutzrechtliche Anforderungen an zentrale Telekommunikations-Anlagen bei Behörden im Land Brandenburg.....129

Anlage 2 Datenschutz und Telemedizin – Anforderungen an Medizinetze.....131

Anlage 3 Auszug aus dem Geschäftsverteilungsplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht.....151

Anlage 4 Aktenplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) .....154

Abkürzungsverzeichnis.....155

Stichwortverzeichnis.....158

<b>Verzeichnis der öffentlichen Stellen</b>	<b>Gliederungspunkt</b>
Ämter für Immissionsschutz	A 4.7.2
Amtsgericht Frankfurt (Oder)	A 5.4
Ausländerbehörde	A 4.3.3 B 2.8
Bußgeldstelle	A 4.1.4
Finanzamt	A 10
Finanzgericht Cottbus	A 5.5
Gerichte	A 5.3.2 A 5.5
Grundbuchamt	A 5.3 A 5.4
Grundsicherungsamt	A 7.2
Industrie- und Handelskammer	A 1.2 A 9.2
Kassenärztliche Vereinigung Brandenburg	A 8.1.2.3
Landesamt für Bauen, Verkehr und Straßenwesen	A 1.2
Landesbetrieb für Datenverarbeitung und Statistik	A 4.5.1 A 4.6 A 5.4 B 3
Landeskriminalamt	A 1.2 A 4.1.2 A 5.2
Ministerium der Finanzen	A 3.1.5 A 10
Ministerium der Justiz und für Europaangelegenheiten	A 5.5

Ministerium des Innern	A 1.1 A 1.2 A 4.3.1 A 4.5.2 A 4.7.1 A 4.8.2 B 1.3 B 2.8 C 3
Ministerium für Arbeit, Soziales, Gesundheit und Frauen	A 8
Ministerium für Bildung, Jugend und Sport	A 6.1
Ministerium für Landwirtschaft, Umwelt und Raumordnung	A 4.7.2 B 1.1
Ministerium für Wirtschaft	A 3.1 B 1.4
Oberlandesgericht	A 5.4
Ordnungsamt	A 4.1.3 A 4.3.2.1
Ostdeutscher Rundfunk Brandenburg	A 3.2.1 A 3.2.2
Polizei	A 4.1.1 A 4.3.2.1 A 4.5.2
Sozialamt	A 8.1
Staatliches Schulamt	A 6.2
Staatsanwaltschaft	A 4.3.2.1
Staatskanzlei	A 3.2.1
Strafvollzugsanstalt	A 5.1
Verfassungsschutzbehörde.....	A 4.2

## Einleitung

Die Herausforderungen für den Datenschutz haben im vergangenen Jahr erwartungsgemäß erneut zugenommen<sup>1</sup>. Selbst wenn in Deutschland niemand ausdrücklich nach dem allwissenden Staat ruft, wie er beispielsweise in den USA unter dem an George Orwell erinnernden Stichwort "Total Information Awareness" (Totales Informationsbewusstsein) vorangetrieben werden soll, besteht auch hier zu Lande für den Datenschutzbeauftragten kein Grund zur Sorglosigkeit.

Die Gründe hierfür liegen auf der Hand: So war etwa die polizeiliche Rasterfahndung, die nach dem 11. September 2001 eingeleitet wurde, bei Drucklegung dieses Berichts, also sechzehn Monate später, in Brandenburg noch immer nicht beendet; Hinweise auf Verdächtige hat sie bisher nicht erbracht. Im Zuge dieser Maßnahme wurden die Daten von hunderttausenden unbescholtenen Bürgerinnen und Bürgern einem bundesweiten Datenabgleich unterzogen. Zwar soll die Rasterfahndung nach Angaben der Polizei entsprechend den gesetzlichen Vorgaben in Kürze beendet werden. Sie hat aber im Zusammenhang mit den Terroranschlägen von Djerba und Bali wieder die grundsätzliche Frage aufgeworfen: Welche Maßnahmen sind in einem Rechtsstaat hinnehmbar, um die zwar verständlichen, aber nicht immer auf tatsächlichen Gefährdungen beruhenden Ängste in der Bevölkerung vor solchen Anschlägen zu beschwichtigen und das Sicherheitsgefühl zu steigern?

Die Antwort heißt: Nur solche freiheitsbeschränkende Maßnahmen sind hinnehmbar, die sich im rechtsstaatlichen Rahmen halten. In die Rechte Unverdächtigter darf auch durch Informationserhebung nur eingegriffen werden, soweit dies zur Bekämpfung einer gegenwärtigen Gefahr geeignet und verhältnismäßig erscheint. Sobald diese Voraussetzung nicht mehr vorliegt, ist der Eingriff zu beenden.

Dem Datenschutz wird in dieser Diskussion häufig entgegengehalten, dass die Erhebung personenbezogener Daten von vielen Menschen nicht als fühlbarer Eingriff verstanden werde, wohingegen die Furcht vor Anschlägen existenzieller Natur sei. Es ist zwar richtig, dass die akute Gefährdung menschlichen Lebens weiter reichende Maßnahmen rechtfertigt. In dem Maße allerdings, wie diese Gefahr abnimmt, nicht konkret zu benennen oder mit den ergriffenen Maßnahmen nicht wirkungsvoll zu bekämpfen ist, muss das Grundrecht unverdächtigter Menschen auf Datenschutz vorrangig berücksichtigt werden.

---

1

Vgl. Tätigkeitsbericht 2001, A 1.1

Denn nach wie vor gilt, was das Bundesverfassungsgericht vor zwanzig Jahren betont hat: "Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen<sup>2</sup>."

Eine unbegrenzte Registrierung von persönlichen Daten würde deshalb – so das Gericht – nicht nur den Freiraum des Einzelnen, sondern auch das Gemeinwohl in einer freiheitlichen, demokratischen Gesellschaft beeinträchtigen, die darauf angewiesen ist, dass ihre Mitglieder ohne Furcht vor staatlicher Kontrolle handeln und das Gemeinwesen mitgestalten. Die ehemalige Präsidentin des Bundesverfassungsgerichts, Prof. Jutta Limbach, hat aus Anlass der 25jährigen Geltung des Bundesdatenschutzgesetzes am 11. Juni 2002 daran erinnert, dass diese Feststellungen des höchsten deutschen Gerichts gerade angesichts der Bedrohung durch den Terrorismus nichts von ihrer Berechtigung verloren haben<sup>3</sup>. Dies gilt auch dann, wenn wie bei der gegenwärtigen Rasterfahndung nicht abweichende Verhaltensweisen, sondern unveränderliche Eigenschaften (wie Alter und Geburt im Ausland) zur Grundlage des Datenabgleichs gemacht werden, dem die Betroffenen deshalb nicht einmal durch Verhaltensänderungen entgehen können.

Auch wenn das Grundrecht auf Datenschutz nicht schrankenlos gewährleistet ist, darf es durch ausufernde Einschränkungen nicht in seinem Kern angetastet werden. Darauf hinzuwirken ist Aufgabe der unabhängigen Datenschutzbeauftragten, die insoweit einem vorgezogenen Grundrechtsschutz dienen. Sie müssen eine Vielzahl von Entwicklungen – nicht nur im Sicherheitsbereich – im Blick behalten, die sich möglicherweise nicht in jedem einzelnen Fall, wohl aber in der Gesamtschau auf den "Grundrechtshaushalt" des Einzelnen und damit auch des Gemeinwesens auswirken können. Der vorliegende Tätigkeitsbericht dokumentiert, welche dieser Entwicklungen im vergangenen Jahr in Brandenburg im Vordergrund standen.

Das Spektrum der behandelten Themen reicht von der notwendigen Konzentration der Datenschutzaufsicht im öffentlichen und nicht-öffentlichen Bereich über biometrische Merkmale auf Personalausweisen und Pässen, die zunehmende Videoüberwachung in den verschiedensten

---

<sup>2</sup> BVerfGE 65, 1, 43

<sup>3</sup> 25 Jahre Bundesdatenschutzgesetz, in: Recht der Datenverarbeitung 2002, 163, 164

Zusammenhängen, den Umgang mit Daten von Gefangenen in Strafvollzugsanstalten bis hin zu den komplexen Fragen der Telemedizin.

Den engen Zusammenhang zwischen Datenschutz und Informationszugang macht die aktuelle Diskussion zu den Katastern über Mobilfunkantennen deutlich: Im Zuge des Aufbaus der UMTS-Netze wird die Zahl der Mobilfunkantennen drastisch zunehmen. Gleichzeitig wächst die Zahl der Menschen, die gesundheitliche Risiken durch den von diesen Anlagen ausgehenden Elektrosmog befürchten. Ob diese Befürchtungen begründet sind, wird zwar unterschiedlich beurteilt. Gerade die Diskussion darüber zeigt aber, dass ein erhebliches Interesse der Öffentlichkeit an der genauen Lage der nicht immer von außen erkennbaren Antennenstandorte besteht. Dieses Interesse überwiegt gegenüber dem Wunsch der Eigentümer, Informationen über ihre Grundstücke nicht zu veröffentlichen.

Das Recht auf allgemeinen, voraussetzungslosen Zugang zu Informationen der öffentlichen Verwaltung, das die Verfassung des Landes Brandenburg vor mehr als zehn Jahren erstmals in Deutschland formuliert hat, wird hier zu Lande allmählich zu einem normalen Bestandteil der Verwaltungskultur. Das liegt auch an der zunehmend routinierten Umsetzung des Akteneinsichts- und Informationszugangsgesetzes durch die Behörden des Landes, in Landkreisen und Gemeinden. Da mutet es wie ein unnötiges Rückzugsgefecht an, wenn das zuständige Ministerium des Innern nach Presseberichten jetzt Überlegungen darüber anstellt, dieses Gesetz wieder einzuschränken. Stattdessen ist vielmehr die pragmatische und bürgerfreundliche Weiterentwicklung des Gesetzes notwendig, das im Vergleich zu anderen Bundesländern inzwischen das restriktivste und Belange der Verwaltung am stärksten berücksichtigende Gesetz ist. Für eine solche Weiterentwicklung hatte der Landesbeauftragte bereits im vergangenen Jahr detaillierte Vorschläge gemacht. Der Landtag hat daraufhin der Landesregierung aufgetragen, zwei dieser Vorschläge umzusetzen, was bisher allerdings noch nicht geschehen ist. Brandenburg, das noch vor fünf Jahren bundesweit Vorreiter in Sachen Akteneinsicht war, droht gegenwärtig den Anschluss an die Entwicklung in anderen Ländern zu verlieren.

# Teil A

## Datenschutz

### 1 Brennpunkte des Datenschutzes

#### 1.1 Entwicklung des Datenschutzrechts

Das seit dem Herbst 2001 vorliegende Gutachten zur Modernisierung des Datenschutzrechts<sup>4</sup> enthält detaillierte Vorschläge für die notwendige umfassende Neustrukturierung der rechtlichen Regelungen und der technischen Vorgaben. Dennoch droht die Modernisierung des Datenschutzrechts in Bund und Ländern ins Stocken zu geraten. Der Landesbeauftragte hat deshalb gemeinsam mit Datenschutzbeauftragten anderer Bundesländer den Parteien und Kandidatinnen und Kandidaten für die Bundestagswahl 2002 auch die Frage gestellt, ob sie eine grundlegende Neustrukturierung des deutschen Datenschutzrechts und eine Stärkung marktwirtschaftlicher Instrumente zur Durchsetzung von Datenschutzkonzepten unterstützen werden<sup>5</sup>. Zwar sind entsprechende Absichtserklärungen in die Koalitionsvereinbarung der die Bundesregierung tragenden Parteien eingegangen. Bisher gibt es aber keine Anzeichen dafür, dass diese Absichtserklärungen in absehbarer Zeit verwirklicht würden. Notwendig ist jetzt der politische Wille, ihre Umsetzung in Angriff zu nehmen.

Das gilt auch für die Einführung eines Datenschutzaudits und eines Gütesiegels für informationstechnische Produkte, die im Bundesdatenschutzgesetz 2001 zwar vorgesehen sind, aber noch einer weiteren bundesgesetzlichen Grundlage in einem Auditgesetz bedürfen.

In diesem Zusammenhang sei daran erinnert, dass das Brandenburgische Datenschutzgesetz bereits seit 1999 eine Vorschrift für ein Datenschutzaudit für die öffentliche Verwaltung enthält (§ 11c). Danach können die öffentlichen Stellen zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größtmöglicher Datensparsamkeit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten und das Ergebnis der Prüfung veröffentlichen lassen. Sie können auch bereits geprüfte und bewertete Datenschutzkonzepte und -programme zum Einsatz bringen. Das Brandenburgische Datenschutzgesetz sieht zwar vor, dass die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter durch besonderes Gesetz geregelt werden müssen.

---

<sup>4</sup> siehe Tätigkeitsbericht 2001, A 1.2

<sup>5</sup> Dokumente zu Datenschutz und Informationsfreiheit 2002, A II

Um zu einem möglichst bundesweit einheitlichen und effektiven Verfahren der Auditierung von Datenschutzkonzepten zu gelangen, ist eine Regelung der Gutachterausswahl und Zulassung durch Bundesgesetz anzustreben. Alternativ hierzu könnte der Landtag Brandenburg aber auch die notwendigen Einzelheiten der Gutachterzulassung durch Landesgesetz regeln. Der Landesbeauftragte würde eine entsprechende Regelung unterstützen, damit ein modernes Element des Brandenburgischen Datenschutzgesetzes, das bisher nur auf dem Papier steht – das Datenschutzaudit – mit Leben erfüllt werden kann. In Schleswig-Holstein, wo ein solches Verfahren und die Vergabe von Gütesiegeln für IT-Produkte bereits praktiziert werden, sind damit gute Erfahrungen gemacht worden.

Auch in einem zweiten entscheidenden Punkt sollte das Datenschutzrecht in Brandenburg jetzt den Anforderungen einer modernen Informationsgesellschaft angepasst werden. Zunehmend wenden sich Bürgerinnen und Bürger mit Beschwerden oder mit Fragen zum Datenschutz im Bereich der Privatwirtschaft an den Landesbeauftragten. Für die Bearbeitung solcher Beschwerden und Anfragen, aber auch für die Beratung von Unternehmen in Fragen des betrieblichen Datenschutzes ist jedoch nicht – wie die meisten Anfragenden naturgemäß annehmen – der Landesbeauftragte für den Datenschutz, sondern das Ministerium des Innern als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zuständig. Die Datenschutzkontrolle ist im Land Brandenburg seit 1992 in dieser Weise aufgeteilt. Dies entsprach seinerzeit auch der Organisation der Datenschutzaufsicht in den westlichen Flächenländern der Bundesrepublik. Inzwischen ist aber die Datenschutzaufsicht neben den Stadtstaaten Berlin, Hamburg und Bremen auch in den Flächenländern Niedersachsen, Schleswig-Holstein und Nordrhein-Westfalen bei den Landesbeauftragten für den Datenschutz konzentriert worden.

Der Landesbeauftragte hat sich schon frühzeitig für eine entsprechende Zusammenlegung der Datenschutzaufsicht eingesetzt. Nach der Verabschiedung des novellierten Bundesdatenschutzgesetzes hat er sich erneut an das Ministerium des Innern gewandt und darauf aufmerksam gemacht, dass mit dem Wegfall der Anlassaufsicht im nicht-öffentlichen Bereich neue und umfangreiche Aufgaben auf die Aufsichtsbehörde zukommen.

Für eine Zusammenlegung der Datenschutzaufsicht im öffentlichen und im nicht-öffentlichen Bereich beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sprechen vor allem drei Gesichtspunkte:

- Es entstünden erhebliche Synergieeffekte, wenn sowohl Bürgerinnen und Bürger als auch Unternehmen sich in Datenschutzfragen an ein "Kompetenzzentrum" des Landes wenden könnten. Der beim Landesbeauftragten bereits jetzt vorhandene technische Sachverstand könnte auch für die Beratung und Kontrolle in der Privatwirtschaft nutzbar gemacht werden. Das Ministerium des Innern wiederum könnte sich auf seine Kernaufgaben, zu denen auch die Vorbereitung der Datenschutzgesetzgebung gehört, konzentrieren.
- Die Zuständigkeitsabgrenzung zwischen dem Bereich der öffentlichen Verwaltung auf Landes- und Kommunalebene einerseits und dem nicht-öffentlichen Bereich der privaten Unternehmen ist für Bürgerinnen und Bürger ohnehin kaum noch transparent. Zunehmend lagern öffentliche Stellen die Datenverarbeitung im Rahmen des Outsourcing auf private Unternehmen aus oder kooperieren auf andere Weise mit privaten Datenverarbeitern.
- Schließlich hat die Europäische Kommission darauf hingewiesen, dass sie dem Kriterium der "völligen Unabhängigkeit" der Aufsichtsbehörden nach der Europäischen Datenschutzrichtlinie erhebliche Bedeutung beimisst. So hat sie in den Erweiterungsverhandlungen mit den mittel- und osteuropäischen Beitrittskandidaten darauf gedrängt, dass die dortigen Kontrollstellen für den Datenschutz keinerlei Weisungen unterworfen sind und ihre Entscheidungen nicht durch politische Instanzen beeinflusst oder abgeändert werden können. Es ist davon auszugehen, dass die Kommission das Kriterium der "völligen Unabhängigkeit" gegenüber den gegenwärtigen Mitgliedstaaten in gleicher Weise interpretiert. Das könnte auch Entscheidungen des Ministeriums des Innern als Aufsichtsbehörde für den Datenschutz in der Privatwirtschaft rechtlich angreifbar machen.

Die Zusammenlegung der Datenschutzkontrolle hat sich in allen anderen Bundesländern, in denen sie vollzogen wurde, gut bewährt. Der Landesbeauftragte befürwortet deshalb nach wie vor eine Zusammenlegung der Datenschutzaufsicht in seiner Dienststelle und würde es begrüßen, wenn die Landesregierung dieses Vorhaben unterstützen und die erforderlichen Maßnahmen einleiten würde.

Brandenburg sollte sich dafür einsetzen, dass das Instrument des Datenschutzaudits zur Bewertung und Verbesserung von Datenschutzkonzepten in die Praxis umgesetzt werden kann.

Nach zehn Jahren geteilter Datenschutzaufsicht für den öffentlichen und den nicht-öffentlichen Bereich ist es an der Zeit, die Kräfte zu bündeln und den Bürgerinnen und Bürgern wie auch Verwaltung und Unternehmen datenschutzrechtliche Beratung aus einer Hand anzubieten. Hierzu sollte die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht übertragen werden.

## 1.2 Die Rasterfahndung – eine unendliche Geschichte?

*Seit über einem Jahr werden in Deutschland massenhaft personenbezogene Daten unverdächtiger Personen bei privaten und öffentlichen Stellen auf der Suche nach sog. "Schläfern" erhoben und gerastert – bislang ohne Ergebnis. Auch in Brandenburg sind noch immer nicht alle erhobenen Daten, bei denen sich kein einschlägiger Anfangsverdacht ergeben hat, gelöscht worden. Das Landeskriminalamt (LKA) hat den Abschluss des automatisierten Abgleichs mehrfach verschoben und eine vollständige Löschung für die Zeit nach dem 31. März 2003 angekündigt.*

Wir haben die bereits im vergangenen Jahr begonnene Prüfung der Rasterfahndung<sup>6</sup> im Berichtszeitraum fortgesetzt und dabei Folgendes festgestellt: Zusätzlich zu dem von den Melde- und Ausländerbehörden sowie den Universitäten und Hochschulen stammenden Grunddatenbestand hat das LKA seit Oktober 2001 bei ca. 100 öffentlichen und nicht-öffentlichen Stellen in Brandenburg personenbezogene Daten über gegenwärtige und ehemalige Mitarbeiter, Gefahrguttransportlizenz- und Fluglizenzinhaber sowie Flugschüler entsprechend dem Beschluss des Amtsgerichts Eberswalde vom 01.10.2001 abgefordert und überwiegend auch erhalten. Bei den Stellen handelte es sich um Unternehmen der chemischen Industrie, technische und naturwissenschaftliche Forschungseinrichtungen und Labore, die Industrie- und Handelskammern, Flughäfen sowie das Landesamt für Bauen, Verkehr und Straßenwesen. Das Bundeskriminalamt (BKA) hat darüber hinaus bundesweit ca. 4.000 private Stellen um die Übermittlung personenbezogener Daten ehemaliger und gegenwärtiger Mitarbeiter sowie Kurs- oder Lehrgangsteilnehmer "auf freiwilliger Basis" gebeten. Dieser Bitte kamen jedoch nicht alle angesprochenen Unternehmen und Verbände nach.

<sup>6</sup> Tätigkeitsbericht 2001, A 1.3

Den brandenburgischen Grunddatenbestand von 27.673 Datensätzen und weitere 161 von den genannten Stellen in Brandenburg übermittelte Datensätze hat das LKA in seine Datei "Rasterfahndung Brandenburg" eingestellt und mit dem landeseigenen Polizeilichen Auskunftssystem Straftaten (PASS), dem INPOL-Fahndungsbestand und der Verbunddatei PIOS Innere Sicherheit (APIS) abgeglichen. Die Errichtungsanordnung des LKA für die Datei "Rasterfahndung Brandenburg" enthält zwar eine ausführliche Begründung der Erforderlichkeit dieser Datei, die weitgehend mit dem Antrag auf gerichtliche Anordnung der Rasterfahndung übereinstimmt. Eine ausreichende datenschutzrechtliche Risikoanalyse, wie sie das 1999 novellierte Brandenburgische Datenschutzgesetz (§ 7 Abs. 3) außerdem vorschreibt, ist dagegen nicht erstellt worden. Das Ministerium des Innern hat die Freigabe des Verfahrens erklärt, ohne eine Untersuchung der spezifischen Risiken zu veranlassen, die von der Rasterfahndung für die Rechte und Freiheiten der Betroffenen ausgehen, und ohne festzustellen, ob eine Beherrschung dieser Risiken durch technische und organisatorische Maßnahmen im Rahmen eines Sicherheitskonzepts sichergestellt ist.

Zusätzlich zu dem Abgleich mit polizeilichen Datenbeständen sind 1.000 Datensätze an den brandenburgischen Verfassungsschutz übermittelt worden, um sie dort mit dem von den Verfassungsschutzbehörden des Bundes und der Länder betriebenen Nachrichtendienstlichen Informationssystem (NADIS) abgleichen zu lassen. Die Datensätze sind nach Abschluss an das LKA zurückgegeben worden. Beim Verfassungsschutz wurden weder Rasterfahndungsdaten noch Abgleichsergebnisse gespeichert. Dieses Vorgehen war rechtlich nicht zu beanstanden.

Das LKA hat anschließend 333 als relevant eingestufte Datensätze an das BKA zum Abgleich mit der dort zur Durchführung der Rasterfahndung betriebenen Datei "Schläfer" übermittelt. Das BKA, das seinen Beitrag zur Rasterfahndung in seiner Funktion als Zentralstelle als reine "Serviceleistung" sieht, führt die Rasterung durch und schickt den übermittelten Bestand angereichert um die dabei festgestellten Informationen an die jeweiligen Länder zur Auswertung zurück. Bei den bislang durchgeführten Abgleichsserien mit brandenburgischen Datensätzen sind zwar "Trefferfälle" festgestellt worden. Die anschließend hier vorgenommene konventionelle Abklärung hat jedoch in keinem dieser Fälle einen Anfangsverdacht für terroristische Straftaten ergeben. Gleichwohl hat das LKA eine Auswertungsdatei für Verdachtsfälle ("ADS") in Betrieb genommen und 188 Datensätze eingestellt.

Der Direktor des LKA stellte eine Beendigung des automatisierten Abgleichs zunächst für Mai 2002 in Aussicht; später wurde ein Abschluss der Maßnahme voraussichtlich für Oktober 2002 angekündigt. Mit Schreiben vom 15. November 2002 hat das LKA dem Landesbeauftragten schließlich mitgeteilt, derzeit würden 8.114 Abgleichdatensätze und 19.225 Datensätze aus dem Grunddatenbestand gelöscht, die zur Erfüllung der polizeilichen Aufgaben nicht mehr erforderlich seien. Danach blieben vorerst 333 personenbezogene Datensätze im Rasterfahndungsbestand gespeichert, die den Rückhalt für die vom Land Brandenburg in die Verbunddatei des BKA eingestellten Daten bildeten. Diese würden weiterhin einem bundesweiten Abgleich unterzogen und angereichert. Aufgrund der Absprachen mit dem BKA und den anderen Länderpolizeien sei beabsichtigt, den Abgleich mit der Verbunddatei bis zum 31. März 2003 abzuschließen. Für diesen Zeitpunkt hat das LKA die Löschung der restlichen Daten sowohl in der Verbunddatei als auch im Rasterfahndungsbestand des Landes Brandenburg sowie die Vernichtung der in Folge der Rasterfahndung angelegten Personenakten angekündigt. Auch die Auswertedatei "ADS" ist dann zu löschen. Die bereits im Berichtszeitraum erfolgte Löschung der Datensätze von deutschen Petenten, die lediglich aufgrund ihres Geburtsortes im Ausland (z. B. New York) in den Rasterfahndungsbestand geraten waren, haben wir überprüft.

Datenschutzrechtlich sind bei der Rasterfahndung nach dem Abschluss des automatisierten Abgleichs in Brandenburg bisher folgende Mängel festgestellt worden:

1. Die Anträge des LKA auf richterliche Anordnung einer polizeilichen Rasterfahndung vom September und Oktober 2001 enthielten auch die Sozialämter als auskunftspflichtige Stellen, obwohl diese erst seit dem 1. Januar 2002 aufgrund des Terrorismusbekämpfungsgesetzes in eine Rasterfahndung einbezogen werden dürfen. Allerdings hat das LKA von den Sozialämtern keine Daten angefordert.
2. Zudem listeten diese Anträge – und dementsprechend auch der daraufhin ergangene Beschluss des Amtsgerichts Eberswalde vom 1. Oktober 2001 – zwar die Behörden auf, die zur Datenanlieferung verpflichtet werden sollten; nicht-öffentliche Stellen wurden dagegen nur in allgemeiner Form in die Rasterfahndung einbezogen. Es bestehen erhebliche Zweifel, ob der Antrag auf Einbeziehung "nicht-öffentlicher Stellen" in dieser Form bestimmt genug war. Der Direktor des LKA teilt diese Bedenken bezogen auf die Vergangenheit zwar nicht, hat aber zugesichert, sie bei in der Zukunft notwendig werden den Rasterfahndungen in seine Überlegungen einzubeziehen. In diesem Zusammenhang ist darauf hinzuweisen, dass die Polizei in an-

deren Bundesländern die möglichen Adressaten von Datenanforderungen in der Privatwirtschaft jedenfalls nach Unternehmensart und Wirtschaftszweig im Antrag auf Anordnung einer Rasterfahndung spezifiziert hat.

3. Für die Datei "Rasterfahndung Brandenburg" beim LKA sind weder eine ausreichende datenschutzrechtliche Risikoanalyse noch ein Sicherheitskonzept nach § 7 Abs. 3 BbgDSG erstellt worden.
4. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht betrachtet ebenso wie die Mehrheit der Datenschutzbeauftragten die Art und Weise der Einbeziehung des BKA in die noch laufende Rasterfahndung nicht als rechtmäßig. Das BKA und die Polizeien der Länder berufen sich demgegenüber auf die Zentralstellenfunktion des BKA. Diese ändert jedoch nichts an der datenschutzrechtlichen Verantwortung des LKA für die in Brandenburg erhobenen und in die Verbunddatei eingestellten Daten.

Insgesamt muss bezweifelt werden, ob die Speicherung und der seriellweise Abgleich der Datensätze von rund 20.000 unverdächtigen Personen über einen Zeitraum von mehr als 13 Monaten im datenschutzrechtlichen Sinne geeignet war, um einer gegenwärtigen Gefahr im Sinne der polizeirechtlichen Befugnis zur Rasterfahndung zu begegnen. Die Dauer der Rasterfahndung ist allerdings nicht auf Mängel bei der Polizei des Landes, sondern auf die Organisation des bundesweiten Abgleichs und vor allem auf die unbestimmten Rasterungskriterien zurückzuführen, die zwangsläufig zu einer nicht in überschaubarer Zeit abzuarbeitenden Zahl von sog. "Treffern" führten. Es wird zu überprüfen sein, ob nach Beendigung des bundesweiten automatisierten Abgleichs sämtliche in diesem Zusammenhang in Brandenburg entstandenen polizeilichen Dateien und Personenakten gelöscht und vernichtet worden sind.

Die Rasterfahndung führt zu weitreichenden Eingriffen in die Rechte unverdächtigter Personen und ist deshalb nur unter den engen datenschutzrechtlichen Voraussetzungen zulässig, die das Polizeigesetz vorsieht. Insbesondere muss sie zeitlich begrenzt bleiben. Eine längerfristige oder gar permanente Rasterfahndung wäre mit den Grundsätzen des freiheitlichen Rechtsstaats unvereinbar. Zukünftige notwendige Maßnahmen dieser Art werden sich strenger an den gesetzlichen Vorgaben zur orientieren haben.

### 1.3 Biometrie in Ausweisen – erkennungsdienstliche Behandlung für alle?

*Durch das Terrorismusbekämpfungsgesetz ist die Möglichkeit eröffnet worden, neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern, Händen oder dem Gesicht des Ausweisinhabers in Pässe und Personalausweise aufzunehmen. Welche Arten von biometrischen Merkmalen in die Ausweise aufgenommen werden sollen, bedarf noch einer Regelung durch den Bundesgesetzgeber<sup>7</sup>.*

Der Gesetzgeber hat unter dem Eindruck der Anschläge vom 11. September 2001 eine Vorentscheidung für die Aufnahme weiterer biometrischer Merkmale in Ausweisdokumente getroffen. Für ihn hatte die Feststellung im führenden Kommentar zum Grundgesetz offenbar keine Bedeutung mehr, wonach die Beibehaltung von Fingerabdrücken auf Personalausweisen nach dem Ende des zweiten Weltkrieges noch als Verstoß gegen die Würde des Menschen angesehen worden war<sup>8</sup>, obwohl dies etwa für die Polizei durchaus "zweckmäßig" gewesen wäre.

Angesichts der anhaltenden erheblichen Unsicherheiten hinsichtlich der Zuverlässigkeit biometrischer Erkennungssysteme ist es zwingend geboten, dass vor einer endgültigen Festlegung der zusätzlichen biometrischen Merkmale, die in Personalausweise und Pässe aufgenommen werden sollen, die Einzelheiten der Durchführbarkeit bestimmter Varianten sorgfältig geprüft werden. Da es um eine Registrierung der gesamten Bevölkerung geht, würden auch geringe Fehlerquoten (falsche Zurückweisungen) zu erheblichen Beeinträchtigungen etwa bei Grenzkontrollen führen. Derartige Fehler würden neben der Bewegungsfreiheit auch das Persönlichkeitsrecht der Betroffenen beeinträchtigen, wenn sie nicht sofort und ohne Diskriminierung aufgeklärt werden können.

Die auf den Personalausweisen und Pässen bereits vorhandenen biometrischen Merkmale (Lichtbild und Unterschrift) sind für moderne Erkennungssysteme gegenwärtig nicht verwendbar. Deshalb hat der Gesetzgeber die Möglichkeit zur Aufnahme weiterer biometrischer Merkmale von Fingern, Händen oder Gesicht des Ausweisinhabers geschaffen. Allerdings ist zukünftig auch die Einbringung von Informationen aus dem Lichtbild, der Unterschrift und den zusätzlichen biometrischen Merkmalen in verschlüsselter Form in die Ausweispapiere zulässig. Die Kernfrage betrifft die Art der neuen biometrischen Merkmale, die verwandt werden dürfen. Genetische Informationen wie auch Informationen über den Au-

<sup>7</sup> siehe Tätigkeitsbericht 2001, A 1.1

<sup>8</sup> Dürig in: Maunz–Dürig, Rz. 37 zu Artikel 1 Grundgesetz

genhintergrund (Retina) und die Iris zählen nicht zu den vom Gesetzgeber zugelassenen Merkmalen.

Aus datenschutzrechtlicher Sicht sind solche Merkmale vorzuziehen, deren Erfassung praktisch nur mit Wissen und unter Mitwirkung des Betroffenen möglich ist (kooperative, aktive Systeme). Dies wäre insbesondere bei der digitalisierten Erfassung des Fingerabdrucks oder der Handgeometrie der Fall. Dagegen scheidet eine heimliche, kontaktlose Erfassung von biometrischen Daten aus der Distanz (nicht-kooperative, passive Systeme), wie sie häufig bei der Gesichtserkennung erfolgt, aus verfassungsrechtlichen Gründen aus.

Von entscheidender Bedeutung ist auch die Verwendung der erhobenen biometrischen Merkmale. Der Gesetzgeber hat mit Bedacht den Aufbau einer bundesweiten Referenzdatei ausdrücklich ausgeschlossen. Damit wird bereits organisatorisch sichergestellt, dass die Personalausweise und Pässe mit biometrischen Merkmalen ausschließlich zur Verifikation genutzt werden können, d. h. zur Überprüfung der Zuordnung des Ausweispapiers zum Ausweisinhaber. Der Vorgang der Verifikation beschränkt sich auf den Abgleich der biometrischen Merkmale einer Person mit dem Merkmalen, die auf dem Ausweis gespeichert sind. Die Speicherung biometrischer Merkmale außerhalb des Ausweisdokuments ist dafür nicht erforderlich und hat deshalb zu unterbleiben. Zugleich wird dadurch verhindert, dass die biometrischen Merkmale im Ausweisdokument zweckentfremdet und letztlich zu einem verfassungswidrigen Personenkennzeichen werden. Die echte Identifikation einer unbekannt Person oder die Erkennung von "Doppelidentitäten" ist allerdings ebenfalls ausgeschlossen, weil sie eine Referenzdatei voraussetzen würde. Auch auf Landesebene dürfen aus diesem Grund keine Dateien mit biometrischen Merkmalen aus Ausweisdokumenten errichtet werden.

Schließlich ist bei einem zukünftigen biometrischen Personenerkennungssystem der Grundsatz der Datensparsamkeit von vornherein zu berücksichtigen. Dieses Prinzip des Systemdatenschutzes, das sowohl im Bundesdatenschutzgesetz als auch im Brandenburgischen Datenschutzgesetz verankert ist, erfordert den vorrangigen Einsatz solcher Verfahren, die auf personenbezogene Daten weitgehend verzichten und stattdessen auf anonymisierte oder pseudonymisierte Informationen zurückgreifen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im März 2002 eine entsprechende Entschließung gefasst und ein ausführliches Positionspapier ihres Arbeitskreises Technik zustimmend

zur Kenntnis genommen<sup>9</sup>. Auch der Bundestagsausschuss für Bildung, Forschung und Technikfolgenabschätzung hat vor dem Hintergrund der weitreichenden Konsequenzen für das informationelle Selbstbestimmungsrecht der Menschen zu einem möglichst zurückhaltenden Einsatz biometrischer Erkennungssysteme in verpflichtend vorgeschriebenen staatlichen Verfahren aufgerufen und eine Stärkung der Datenschutzkontrolle gefordert<sup>10</sup>.

Flächendeckende Systeme zur biometrischen Erkennung von Personen anhand von Ausweisdokumenten setzen eine konkrete Entscheidung des Bundesgesetzgebers voraus. In Betracht kommen nur Systeme, die Informationen mit Wissen und unter aktiver Mitwirkung der Betroffenen erheben. Auch sollten solche Systeme den Vorzug erhalten, die eine Anonymisierung oder Pseudonymisierung von Daten zulassen. Sowohl zentrale als auch dezentrale Referenzdateien sind ausgeschlossen.

## **2 Technisch-organisatorische Entwicklungen**

### **2.1 Sicherheit beim Telefonieren im Internet**

*Telefonieren über das Internet entwickelt sich als echte Alternative zur traditionellen Kommunikationsform. Kosten und Wartungsaufwand können so gesenkt werden. Bei aller Euphorie gibt es aber zurzeit noch einen entscheidenden Nachteil dieser Technologie: Gespräche sind leicht zu belauschen.*

Trotz der technischen Vorteile hat sich die Telefonie im Internet (Voice over IP) noch nicht durchgesetzt. Ein Grund hierfür liegt in der Schwierigkeit der Sprachübertragung. Das Internet überträgt die Daten in einzelnen Paketen, die unterschiedlich lange Wege nehmen können. Die Daten kommen in unterschiedlicher Reihenfolge beim Empfänger an und werden dort zur vollen Information zusammengesetzt und ausgegeben. Verzögerungen sowie in vertauschter Reihenfolge eintreffende Daten führen dazu, dass die Sprache unverständlich und eine Kommunikation unmöglich wird. Gesicherte Transportprotokolle des Internet, wie das Transmission Control Protocol (TCP), sind für eine Echtzeitkommunikation ungeeignet, weil der fehlerlose Empfang von Daten mit zu langen zeitlichen Verzögerungen erkauft wird. Dies ist für die Sprachübertragung nicht hinnehmbar.

---

<sup>9</sup> Dokumente zu Datenschutz und Informationsfreiheit 2002, I 1 und 2

<sup>10</sup> Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung, TA-Projekt: Biometrische Identifikationssysteme – Sachstandsbericht, BT-Drs. 14/10005 vom 10.10.2002, S. 51

Die Internet Engineering Task Force (IETF) hat deshalb das Realtime Transport Protocol (RTP) entwickelt, das auf dem ungesicherten Datentransportprotokoll UDP (User Datagram Protocol) des Internet aufsetzt und damit die Übertragung von Echtzeitdatenströmen erlaubt. Die Konzentration auf die Qualität der Sprachübertragung wirkte sich aber zu Lasten einer sicheren Kommunikation aus, so dass Gespräche mit einfachen technischen Mitteln belauscht werden können. Man benötigt lediglich einen Sniffer, der die UDP-Pakete kopiert und an einen beliebigen Host weiterleitet und einen Media-Player, der den Datenstrom korrekt interpretieren, öffnen und abspielen kann. Der Mangel an Vertraulichkeit bei der Übertragung ist datenschutzrechtlich nicht hinnehmbar. Ohne weitere Schutzmaßnahmen ist die Nutzung von Voice over IP daher abzulehnen.

Erst wenn eine End-zu-End-Verschlüsselung der Pakete realisiert wird (z. B. IPSEC), ist ein ausreichender Schutz der Vertraulichkeit von Gesprächen gewährleistet. Diese Technik, die auf Anwenderebene implementiert werden müsste, ist zur Zeit aber noch nicht verfügbar.

Die derzeitigen Mechanismen zur Übertragung von Sprachdaten über das Internet sind zwar qualitativ recht ausgereift. Angriffe auf die Verbindung oder gar das Abhören von Gesprächen sind allerdings technisch einfach möglich. Derzeit gibt es noch keine hinreichende Sicherheit, so dass bei der Nutzung des Internet zum Zweck der Telekommunikation Vorsicht geboten ist.

## **2.2 Datenschutzfragen bei der Nutzung von Windows XP**

*Mit Windows XP entwickelte der weltweit führende Software-Hersteller Microsoft Ende 2001 das wohl neugierigste Betriebssystem aller Zeiten. Es enthält eine Menge neuer Komponenten, die ohne das Wissen des Nutzers über das Internet Kontakt mit den Microsoft-Servern aufnehmen. Welche Daten dabei im Einzelnen übertragen werden, ist bis heute nicht vollständig geklärt.*

Das neue Betriebssystem Windows XP kann erst nach einer erfolgreichen Aktivierung vollständig freigeschaltet werden. Bei dieser Produktaktivierung wird ein 50-stelliger Zahlencode, der sich hauptsächlich aus den Seriennummern der Hardware errechnet und so verschiedene Merkmale des Computers enthält, an Microsoft übermittelt. Diese Zwangsaktivierung kann wahlweise über das Internet weitest gehend automatisch erfolgen, oder per Telefon. Während der gesamten Prozedur wird nur der Zahlencode übertragen. Erst wenn ein Benutzer eine freiwillige

liche Registrierung durchführt, werden nach Abfrage der expliziten Zustimmung personenbezogene Daten übertragen. Dies gilt auch für eine telefonische Registrierung. Um die Daten während der Übertragung ausreichend zu schützen, werden diese verschlüsselt gesendet. Angesichts dieser Verfahrensweisen kann man davon ausgehen, dass für die Produktaktivierung ohne Registrierung keine personenbezogenen Informationen weitergereicht werden. Es stellt sich nur die Frage, was mit den weltweit gesammelten Daten geschehen soll. Dazu trifft Microsoft keine Aussage.

Neben der Produktaktivierung existieren noch weitere Dienste, wie der Zeitabgleich und die Fehlerberichterstattung, die standardmäßig Kontakt zu Microsoft-Servern aufnehmen. Auch der Internet Explorer und Messenger suchen dort selbstständig nach Aktualisierungen. Doch welche Daten letztendlich übermittelt werden, bleibt ungewiss. Microsoft hält die dafür genutzten Techniken geheim und beteuert immer wieder, dass keine personenbezogenen Daten erhoben werden. Wer dieser Aussage nicht traut, sollte diese Komfortmerkmale von Windows XP deaktivieren. Anlass dazu gibt jedenfalls die Übertragung von persönlichen Daten bei der Nutzung des integrierten Microsoft Mediaplayers. Dieser übermittelt die Medien-ID der eingelegten CD, die der Mediaplayer von der CD ausliest, sowie die Identifikationsnummer des installierten Mediaplayers. Daraufhin erhält man aus dem Netz die Begleitinformationen zum gespielten Titel und zum entsprechenden Künstler. Die übertragene Identifikationsnummer gibt zunächst keine Auskunft über den Benutzer und ist daher datenschutzrechtlich unbedenklich. Bedenklich ist jedoch, dass dieselbe Identifikationsnummer zusammen mit dem Namen und der E-Mail Adresse erneut auftaucht, sobald sich der Nutzer für den Windows Media Newsletter anmeldet. In einer Stellungnahme erklärte ein Microsoft-Sprecher dazu, dass der Konzern derzeit nicht plane, die gesammelten Daten über die Seh- und Hörgewohnheiten der Kunden zu vermarkten, dies aber für die Zukunft nicht auszuschließen sei.

Um möglichen datenschutzrechtlichen Problemen entgegenzuwirken, sollten öffentliche Stellen, die dieses Produkt einsetzen wollen, ein angemessenes Sicherheitskonzept für die Nutzung von Windows XP erstellen. Anregungen und Hintergrundinformationen sind in der "Orientierungshilfe zu Datenschutz bei Windows XP", die vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt wurde, nachzulesen. Das Dokument kann von unserer Homepage (<http://www.lida.brandenburg.de>) bezogen werden.

Die enge Verflechtung von Windows XP mit dem Internet und die Ungewissheit, welche Daten von kontaktfreudigen Anwendungen übermittelt werden, zwingen zu erhöhter Vorsicht beim Einsatz dieses Betriebssystems. Eine höhere Benutzerfreundlichkeit darf nicht zu einem Verlust an Sicherheit im Umgang mit Bürgerdaten führen.

## 2.3 Elektronische Signatur – Praktikable Lösungen und neue Fragen

*Bereits im letzten Tätigkeitsbericht<sup>11</sup> berichteten wir darüber, dass eine interministerielle Arbeitsgruppe Elektronische Signaturen, an der wir uns beteiligen, ins Leben gerufen wurde, die sich mit den rechtlichen Voraussetzungen und der zu schaffenden Infrastruktur bei der Einführung von Signaturen auf der Basis einheitlicher Standards beschäftigt.*

Im Berichtszeitraum wurde das Dritte Gesetz zur Änderung verwal-  
tungsverfahrenrechtlicher Vorschriften im Bundesgesetzblatt<sup>12</sup> verkün-  
det. Dieses Gesetz schafft den Rahmen für rechtsverbindliche elektro-  
nische Kommunikation im Verwaltungsrecht auf Bundesebene. Die  
Bundesländer sind nun verpflichtet, ihre Verwaltungsverfahrensgesetze  
entsprechend anzupassen. Das Ministerium des Innern bereitet daher  
derzeit den Entwurf eines Artikelgesetzes zur Anpassung verwal-  
tungrechtlicher Vorschriften an den elektronischen Rechtsverkehr vor. Damit  
wird die Verwaltung in die Lage versetzt, elektronische Bürgerdienste  
auch in rechtlich verbindlicher Form anzubieten.

Die Arbeitsgruppe hat mit einem Test zur Einführung der elektronischen  
Signatur und Verschlüsselung begonnen. Das Ziel besteht darin, erste  
Praxis-Erfahrungen zu sammeln und ihre Nutzung im Land Brandenburg  
vorzubereiten.

Das Bestreben nach einer möglichst zügigen Verbreitung der elektroni-  
schen Signatur wirft aber auch neue Fragen auf. So erwägt das Bun-  
deswirtschaftsministerium, im Rahmen einer Machbarkeitsstudie unter-  
suchen zu lassen, ob in Zukunft alle Personalausweise mit einem Sig-  
naturchip ausgestattet werden können, um so die flächendeckende Ein-  
führung der elektronischen Signatur zu beschleunigen. Häufig wird in  
diesem Zusammenhang auf das Beispiel Finnland verwiesen, wo dieser  
Weg beschritten wurde.

---

<sup>11</sup> siehe Tätigkeitsbericht 2001, A 2.1

<sup>12</sup> BGBl. I S. 3322

Die Verknüpfung des Personalausweises mit der elektronischen Signatur würde allerdings neue gravierende Risiken für das Grundrecht auf Datenschutz mit sich bringen, wenn die Wahlfreiheit der Bürger rechtlich oder faktisch eingeschränkt würde. Es muss jedem freigestellt bleiben, ob er einen Personalausweis mit oder ohne elektronischer Signatur erhält. Andernfalls droht die elektronische Signatur in Verbindung mit der Personalausweisnummer zu einem verfassungswidrigen Personenkennzeichen zu werden.

Derzeit wird an einem Entwurf eines Artikelgesetzes zur Anpassung verwaltungsrechtlicher Vorschriften an den elektronischen Rechtsverkehr im Land gearbeitet. Dessen Verabschiedung wird die rechtlichen Voraussetzungen für die Verwaltung schaffen, elektronische Bürgerdienste auch in rechtlich verbindlicher Form anbieten zu können. Die technische Umsetzung wird wesentlich von der Schaffung einheitlicher Signaturstandards abhängen.

Bei der Einführung der elektronischen Signatur muss die Wahlfreiheit der Bürger erhalten bleiben. Es muss sichergestellt werden, dass aus dieser Form der Identifizierung kein faktisches Personenkennzeichen wird.

## **3 Telekommunikation und Medien**

### **3.1 Telekommunikation, Multimedia und Post**

#### **3.1.1 Neue europäische Datenschutzregeln für die elektronische Kommunikation**

*Bisher hat die Europäische Union neben der allgemeinen Datenschutzrichtlinie von 1995 lediglich eine besondere Richtlinie über den Datenschutz im Bereich der Telekommunikation<sup>13</sup> erlassen, die sich in erster Linie auf digitale Fest- und Mobilfunknetze bezieht. Diese Richtlinie wird zum 31. Oktober 2003 durch die neue Datenschutzrichtlinie für elektronische Kommunikation<sup>14</sup> ersetzt werden. Der europäische Gesetzgeber hat im Rahmen eines größeren Maßnahmenpaketes zur endgültigen Liberalisierung des Telekommunikationsmarktes die bisherige Datenschutzrichtlinie auf nahezu alle Formen der elektronischen Kommunikation ausgedehnt. Lediglich Rundfunkdienste werden von ihr nicht erfasst.*

Die neue Richtlinie, die noch in deutsches Recht umgesetzt werden muss, stärkt in mehreren Punkten die Rechte des Nutzers von elektronischen Kommunikationsnetzen. So werden die Betreiber solcher Netze und die Anbieter entsprechender Kommunikationsdienste zur Weitergehenden Information des Nutzers verpflichtet. Die Verarbeitung von Standortdaten, die in Zukunft beim Angebot von standortbezogenen Diensten mit Zusatznutzen<sup>15</sup> anfallen, werden strikten Regeln unterworfen (Art. 9). Unerbetene elektronische Post für Zwecke der Direktwerbung (sog. SPAM) ist zukünftig nur bei vorheriger Einwilligung der Adressaten zulässig (Art. 13 Abs. 1). Damit wird das Problem der "Überschwemmung" von elektronischen Postfächern mit unerbetenen Mitteilungen (Werbe-Müll, "Junk Mail") zwar noch nicht praktisch gelöst, immerhin sind die Mitgliedstaaten aber jetzt verpflichtet, einen einheitlichen Rechtsrahmen zur Bekämpfung unaufgeforderter elektronischer Werbung zu schaffen.

Außerdem wird die Kommission ihrerseits durch die neue Richtlinie ermächtigt, Maßnahmen zu treffen, die sicherstellen, dass Endgeräte für die elektronische Kommunikation in einer Weise gebaut werden, die mit

---

<sup>13</sup> Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABIEU L 24/1 vom 30.1.1998

<sup>14</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABIEU L 201/37

<sup>15</sup> siehe dazu unten A 3.1.2

dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist (Artikel 14 Abs. 3). Damit hat sich die Kommission die Möglichkeit vorbehalten, Vorschriften für die datenschutzfreundliche Gestaltung von Endgerätetechnik zu erlassen, wenn die Normen und technischen Vorschriften in den Mitgliedstaaten diesem Ziel zu widerlaufen sollten. Die neue europäische Richtlinie beschränkt sich also nicht auf die Festlegung allgemeiner rechtlicher Grundsätze, sondern enthält auch konkrete Regelungen für eine datenschutzfreundliche Gestaltung der Kommunikationstechnik.

Darüber hinaus dürfen die Mitgliedstaaten Ausnahmen vom Grundsatz der Löschung von Verkehrsdaten nach dem Ende der Verbindung zulassen, wenn dies für die nationale Verteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist (Artikel 15 Abs. 1). Diese eher umstrittene Regelung wurde insbesondere auf Betreiben derjenigen EU-Mitgliedstaaten in die Richtlinie aufgenommen, in denen bereits gesetzliche Pflichten zur Speicherung von Verkehrsdaten auf Vorrat gelten. Die neue Richtlinie enthält keine Verpflichtung des deutschen Gesetzgebers, derartige Pflichten zur anlassunabhängigen, verdachtslosen Speicherung von Verkehrsdaten vorzusehen. Eine solche Verpflichtung würde in Deutschland auch an verfassungsrechtliche Grenzen stoßen<sup>16</sup>.

Die neue EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation stärkt überwiegend die Rechte derjenigen, die elektronische Kommunikationsnetze nutzen. Allerdings ist der Gesetzgeber aufgefordert, diesen Rechten auch auf nationaler Ebene Geltung zu verschaffen.

### **3.1.2 Location Based Services (LBS) – standortbezogene Dienste**

*Die Mobilfunkbetreiber bieten ihren Kunden zunehmend standortbezogene Dienste (Location Based Services) an. Damit erhalten die Mobilfunkbetreiber die Möglichkeit, dem Handy-Nutzer auf seine Position bezogene Informationen zur Verfügung zu stellen. Der Handy-Nutzer kann sich so z. B. die in seiner Nähe befindlichen Restaurants, Apotheken oder andere Einrichtungen auf seinem Handy anzeigen lassen. Auch ist die Lokalisierung anderer Handy-Nutzer technisch möglich.*

<sup>16</sup>

siehe dazu näher unten A 3.1.4

Es werden drei Arten von Diensten unterschieden. Tracking-Dienste dienen ausschließlich dem Zweck, den Standort eines Endgerätes festzustellen. Diese Dienste finden beispielsweise bei der Überwachung von Fahrzeugflotten oder bei der Feststellung von Standorten von Mitarbeitern (z. B. Taxi-Gewerbe) Anwendung. Pull-Dienste sind solche, bei denen der Informationsaustausch vom Endkunden initiiert wird. Bei den Push-Diensten schließlich wird der Informationsaustausch vom Betreiber initiiert und ist vom Endkunden nicht vorhersehbar. Dies spielt z. B. bei der vom Standort des Endgerätes abhängigen Zusendung von Werbebotschaften auf das Handy eine Rolle. Die Dienste werden dabei in der Regel nicht vom Netzbetreiber selbst, sondern von einem dritten Anbieter (Content Provider) unter Nutzung der Infrastruktur des Netzbetreibers erbracht. Auch öffentliche Stellen können im Rahmen von E-Government-Anwendungen Lokalisierungsdienste nutzen, z. B. wenn Bürger in einer kreisfreien Stadt über ihr Handy feststellen wollen, wo sich die nächste Meldestelle oder das nächste Bürgerbüro befindet.

Ein im Netz angemeldetes (eingeschaltetes) Handy wird mit Hilfe der sogenannten Zellen-Identifikationsnummer (Cell ID) insofern eindeutig lokalisiert, als sein Standort im Verhältnis zur nächsten Basisstation ermittelt werden muss, um jederzeit eine Verbindung herstellen zu können. Die Genauigkeit der Funkzellenortung ist abhängig von der jeweiligen Funkzelle und der Funkzellendichte. Während im städtischen Bereich die Ortung bis auf wenige hundert Meter genau erfolgen kann, liegt die Ortungsgenauigkeit in ländlichen Gebieten lediglich im Kilometer-Bereich.

Für Dienste, die eine genauere Ortung erfordern, werden verbesserte Varianten der Standortbestimmung des Mobilfunknutzers entwickelt. Dazu gehört vor allem die Technologie mit der Bezeichnung "Enhanced Observed Time Difference (E-OTD)". Dabei werden am mobilen Endgerät die Laufzeiten der empfangenen Signale zwischen der Basisstation, welche die Funkzelle versorgt, und zwei weiteren benachbarten Basisstationen bestimmt. Die Ergebnisse werden ins Verhältnis zueinander gestellt. Da die Koordinaten der Basisstationen bekannt sind, kann die Position des Handy-Nutzers berechnet werden. Damit lässt sich eine Genauigkeit zwischen 50 und 500 m erreichen. Sie kann bei Endgeräten mit eingebauten GPS-Empfängern (Global Positioning System) bis auf wenige Meter gesteigert werden.

Aus datenschutzrechtlicher Sicht ist dabei relevant, dass zum einen die Cell ID für andere Zwecke als zur Ermöglichung der Telekommunikation genutzt wird. Bei allen Lokalisierungstechnologien, die nicht ausschließlich auf der Nutzung der Cell ID basieren, müssen zudem personenbezogene Daten des Nutzers verarbeitet werden, die über das hinausgehen, was zur Führung der Telekommunikation erforderlich ist. In der gel-

tenden Telekommunikations–Datenschutzverordnung findet sich keine Rechtsgrundlage, um Standortdaten für solche standortbezogenen Dienste zu verarbeiten. Dies wäre nur aufgrund einer Einwilligung des Nutzers zulässig.

Entscheidend ist, dass zusätzliche Standortinformationen nur unter der vollen Kontrolle des Nutzers generiert werden dürfen. Vorzuziehen sind daher solche Lösungen, bei denen die Entstehung präziser Aufenthaltsinformationen durch das Endgerät selbst initiiert wird, da diese ein höheres Maß an Datenschutz bieten als netzwerkbasierte, vom Nutzer unabhängig arbeitende Lösungen. Bei der Gestaltung von LBS ist deshalb großer Wert auf die Grundsätze von Datenvermeidung und Datensparsamkeit zu legen. Technisch ist es dabei in der Regel möglich, dass der Handy–Nutzer gegenüber dem Content Provider zumindest pseudonym auftreten kann. Schließlich muss auch die – rechtlich unzulässige – Erstellung personenbezogener Bewegungs– und Nutzerprofile ohne Einwilligung des Nutzers bereits auf technischer Ebene unterbunden werden. Art. 9 der bis zum 31. Oktober 2003 in deutsches Recht umzusetzenden Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation schreibt entsprechend vor, dass solche Daten nur anonymisiert oder aufgrund einer informierten Einwilligung verarbeitet werden dürfen. Dabei muss auch bei erteilter Einwilligung die Möglichkeit bestehen, die Verarbeitung der Daten hinsichtlich einzelner Dienste zeitweise zu untersagen.

Für die Erbringung von Location Based Services erforderliche Standortdaten dürfen nur in anonymisierter Form oder aufgrund einer Einwilligung des Handy–Nutzers durch den Netzbetreiber sowie den Anbieter des Dienstes verarbeitet werden.

### **3.1.3 Orientierungshilfe für Internet–Anbieter**

*Beim Umgang mit den für das Internet geltenden datenschutzrechtlichen Bestimmungen stellen wir nach wie vor eine große Unsicherheit fest. Dies betrifft nicht nur die Anbieter von Internetdiensten, zu denen auch öffentliche Stellen des Landes Brandenburg gehören, sondern auch beispielsweise die Strafverfolgungs– und Sicherheitsbehörden bei der Überwachung der Kommunikation im Netz.*

Der vom Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht geleitete Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb eine Orientierungshilfe entworfen, in der die wesentlichen datenschutzrechtlichen

Pflichten der Anbieter sowie die Befugnisse der Strafverfolgungs- und Sicherheitsbehörden dargestellt werden. Diese wird derzeit mit den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich abgestimmt.

Die Orientierungshilfe geht von folgenden Grundsätzen aus:

- Internet-Anbieter dürfen Daten der Nutzer über die inhaltliche Ausgestaltung, Begründung oder Änderung eines Vertragsverhältnisses (Bestandsdaten) nur verarbeiten, soweit dies für die genannten Zwecke unabdingbar ist; Inhaltsanbieter (Content Provider) dürfen deshalb in der Regel keine Bestandsdaten erheben, weil mit ihnen nur selten vertragliche Beziehungen bestehen.
- Internet-Anbieter dürfen Daten der Nutzer über die Inanspruchnahme des Dienstes (Datum, Uhrzeit und Dauer der Nutzung, IP-Adressen genutzter Webserver, dynamische IP-Adressen der Nutzer) grundsätzlich nur verarbeiten, soweit dies zur Erbringung des jeweiligen Dienstes erforderlich ist. Diese Daten sind nach Ende der Nutzung zu löschen, wenn sie nicht zu Abrechnungszwecken benötigt werden.
- E-Mail-Dienste, die Zugangvermittlung zum Internet (Access Providing) sowie das Telefonieren über das Internet (Voice over IP) sind Telekommunikationsdienste. Die bei der Inanspruchnahme des Dienstes verarbeiteten Daten sind daher unter das Fernmeldegeheimnis fallende Verbindungsdaten, die nur im Rahmen der §§ 6 ff. der Telekommunikations-Datenschutzverordnung verarbeitet werden dürfen.
- Alle übrigen Internet-Dienste sind Tele- oder Mediendienste. Die bei der Inanspruchnahme des Dienstes verarbeiteten Daten sind Nutzungsdaten, die nur nach §§ 6 Teledienstedatenschutzgesetz, 19 Abs. 2 Mediendienste-Staatsvertrag verarbeitet werden dürfen.
- Kein Internet-Anbieter ist gegenwärtig berechtigt, für die Interessen von Strafverfolgungs- und Sicherheitsbehörden personenbezogene Daten der Nutzer auf Vorrat zu speichern, die er nicht für eigene Zwecke speichern dürfte.<sup>17</sup>
- Access Provider oder Anbieter von E-Mail-Diensten müssen Bestandsdaten an Strafverfolgungs- und Sicherheitsbehörden nach § 89 Abs. 6 Telekommunikationsgesetz herausgeben.

---

17

Zu Plänen für eine Verpflichtung zur Datenspeicherung auf Vorrat, s. unten A 3.1.4

- Access Provider oder Anbieter von E-Mail-Diensten müssen Verbindungsdaten (Datum, Uhrzeit und Dauer der Nutzung, Domainnamen, IP-Adressen, E-Mail-Adressen) unter den Voraussetzungen der §§ 100g, 100h Strafprozessordnung (StPO) an Strafverfolgungsbehörden herausgeben. Alle darüber hinausgehenden Daten (Bezeichnungen von Dateianlagen, Betreff oder Inhalte von E-Mails sowie Bestandteile des Uniform Resource Locator [URL], die über den bloßen Domännennamen, die Bezeichnung des Protokolls bzw. Dienstes oder der IP-Adresse hinausgehen) sind Inhalte der Telekommunikation und dürfen deshalb nur im Rahmen einer Überwachung der Telekommunikation nach §§ 100a, 100b StPO an Strafverfolgungsbehörden weitergegeben werden.
- Soweit bei einem Content Provider Bestandsdaten vorliegen, können die entsprechenden Datenträger nach der Strafprozessordnung beschlagnahmt werden. Für dort anfallende Verbindungs- und Inhaltsdaten gelten die obigen Ausführungen entsprechend.
- Die Nachrichtendienste verfügen über besondere Auskunftsrechte hinsichtlich der von den Anbietern gespeicherten Daten.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht erteilt im Rahmen seiner Zuständigkeit jederzeit Auskünfte zur Verarbeitung personenbezogener Daten durch Internet-Anbieter sowie zu den Befugnissen der Strafverfolgungs- und Sicherheitsbehörden.

### **3.1.4 Vorratsdatenspeicherung bei Telekommunikations- und Telediensteanbietern**

*Der Bundesrat hat einen Gesetzentwurf beschlossen, mit dem unter anderem sämtliche Anbieter von Telekommunikations- und Telediensten verpflichtet werden sollen, die bei ihnen anfallenden Verbindungs- und Nutzungsdaten für Zwecke der Strafverfolgung, der Sicherheitsbehörden und Nachrichtendienste ohne Anlass für eine bestimmte Mindestfrist zu speichern.*

Zwar haben die Bundesregierung diesen Vorschlag unter Hinweis auf verfassungsrechtliche Bedenken bisher abgelehnt und der Deutsche Bundestag über diesen Gesetzentwurf in der vergangenen Legislaturperiode nicht mehr entschieden. Dennoch gibt es sowohl auf nationaler als auch auf europäischer Ebene nach wie vor starke Bestrebungen, die Anbieter zur einer Datenspeicherung auf Vorrat zu verpflichten. Derartige Vorschläge würden den Grundrechtsschutz im Bereich der Telekommu-

nikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses prinzipiell in Frage stellen.

Dabei ist geplant, alle Anbieter von Telekommunikations- und Multimedien Diensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Auf das so entstehende umfassende Datenreservoir sollen die Strafverfolgungsbehörden, die Polizei und der Verfassungsschutz bei möglichen Anlässen in der Zukunft zugreifen können. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen "Justiz und Inneres" entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder sind diesen Überlegungen mit Entschiedenheit entgegengetreten und haben deshalb auf ihrer 64. Konferenz in Trier eine EntschlieÙung dazu verabschiedet.

Die Möglichkeit, unbeobachtet miteinander zu kommunizieren, ist eine unabdingbare Voraussetzung für eine freiheitliche demokratische Gesellschaft. Immer mehr menschliche Lebensäußerungen finden heute per Telefon, Internet oder in anderen elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen außerhalb der virtuellen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist daher ebenso wenig hinnehmbar<sup>18</sup>.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Auch die Konferenz der europäischen Datenschutzbeauftragten hält eine flächendeckende anlassfreie Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, für unverhältnismäßig und für nicht mit dem Menschenrecht auf

---

<sup>18</sup> Der Text der EntschlieÙung ist in dem bei uns erhältlichen Band "Dokumente zu Datenschutz und Informationsfreiheit 2002" abgedruckt und ebenso wie alle anderen Dokumente auf unserer Website abrufbar.

Achtung des Privatlebens vereinbar. Selbst in den unter dem Eindruck der Terroranschläge vom 11. September 2001 stehenden Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Weder ist eine verdachtslose, routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat mit dem deutschen Verfassungsrecht noch mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu vereinbaren.

Wir fordern die Landesregierung auf, Bestrebungen zur verdachtslosen Speicherung von Daten, die bei der Nutzung der elektronischen Kommunikation entstehen, entgegenzutreten und entsprechenden Gesetzentwürfen im Bundesrat nicht zuzustimmen. Eine pauschale, anlassabhängige Speicherung sämtlicher Verbindungs- und Nutzungsdaten würde die unbeobachtete Kommunikation in unserer Gesellschaft weitgehend unmöglich machen.

### **3.1.5 Erneuerung des TK-Anlagenverbundes der obersten Landesbehörden**

*Mit Ablauf des Jahres 2003 endet die Servicevereinbarung für die einzelnen TK-Anlagen des TK-Anlagenverbundes der obersten Landesbehörden. Als Konsequenz daraus hat die Landesregierung zur Erneuerung und Modernisierung des gesamten TK-Anlagenverbundes einen Arbeitskreis gebildet. Von diesem Arbeitskreis wurden wir einbezogen, um datenschutzrechtliche Forderungen bereits bei der Ausschreibung der neuen TK-Anlagen berücksichtigen zu können.*

Die neusten computergesteuerten TK-Anlagen bieten dem Nutzer mit ihren umfangreichen Leistungsmerkmalen nicht nur schnelle, effektive und komfortable Kommunikationsmöglichkeiten, sondern bergen auch oft unterschätzte Risiken für die Rechte des Einzelnen, dessen Privatsphäre dadurch erheblich beeinträchtigt werden kann. In den Vermittlungs- und Gebührencomputern entstehen umfangreiche Sammlungen sensibler personenbezogener Daten, die sich auch zur Verhaltens- und Leistungskontrolle der Mitarbeiter eignen und Hinweise auf das Kommunikationsverhalten ihrer Gesprächspartner geben. Unter den Schutz des Fernmeldegeheimnisses fallen nicht nur die Inhalte der geführten Gespräche, sondern auch die näheren Umstände des Fernmeldeverkehrs, insbesondere wer wann mit wem mittels welches Mediums kommuniziert hat. Unter diesem Gesichtspunkt und in Anbetracht der Tatsache, dass häufig von dienstlichen Telefonapparaten auch private Gespräche geführt werden dürfen, sind die Verbindungsdaten, falls sie über das Gespräch-

sende für Zwecke der Kontrolle und Gebührenerfassung gespeichert werden, als besonders sensibel einzustufen und durch technische und organisatorische Maßnahmen, wie sie im § 10 des Brandenburgischen Datenschutzgesetzes vorgeschrieben werden, zu sichern.

Mit dem Ministerium der Finanzen besteht Einigkeit darüber, dass für die Nutzung von TK-Anlagen in der Landesverwaltung auch künftig die allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg (Dienstanschluss-Vorschriften – DAV) und die darauf aufbauende Musterdienstvereinbarung verbindlich sein sollen. Auf dieser Grundlage haben wir die in Anlage 1 dieses Berichtes enthaltenen allgemeinen datenschutzrechtlichen Anforderungen an zentrale TK-Anlagen bei Behörden im Land Brandenburg mit dem Ziel formuliert, sie in die Ausschreibungsunterlagen einfließen zu lassen. Ferner haben wir unsere Bereitschaft erklärt, auf Anfrage die Konzepte und Produkte für Gebührenverarbeitungsanlagen von TK-Anbietern auf ihre Datenschutzverträglichkeit zu prüfen.

Im Rahmen einer Umfrage des Landesbetriebs für Datenverarbeitung und Statistik als Betreiber bei den künftigen Nutzern der neuen TK-Anlage haben sich mehrere Ressorts für die Schaffung einer Möglichkeit zur Aufzeichnung von Telefongesprächen ausgesprochen, um Bedrohungen oder Beschimpfungen von Mitarbeitern beweisen zu können. Wir sind der Einrichtung solcher "Drohanrufaufzeichnungsanlagen" stets entschieden entgegengetreten, weil ihre einseitige oder heimliche Verwendung dem Recht am gesprochenen Wort widerspricht. Dieses Recht ist wie das Grundrecht auf Datenschutz Teil des allgemeinen Persönlichkeitsrechts und als solches von der Verfassung geschützt. Dies hat das Bundesverfassungsgericht im Berichtszeitraum in einem grundlegenden Beschluss betont<sup>19</sup>. Zudem setzen Dienstbehörden, die solche technischen Einrichtungen installieren, ihre Bediensteten der Gefahr der strafrechtlichen Verfolgung wegen Verletzung der Vertraulichkeit des nicht öffentlich gesprochenen Wortes durch deren unbefugte Aufnahme aus, was mit ihrer Fürsorgepflicht nicht zu vereinbaren ist. Etwas anderes gilt nur bei Notrufleitstellen, bei denen eingehende Notrufe generell aufgezeichnet werden, um der anrufenden Person in jedem Fall helfen zu können.

Wir gehen davon aus, dass durch die weitere gute Zusammenarbeit mit dem Landesbauamt künftig ein hohes Datenschutzniveau beim Betrieb des neuen TK-Anlagenverbundes der obersten Landesbehörden gesichert werden kann.

### 3.1.6 Registrierung des Nutzerverhaltens zum Schutz des Urheberrechts?

*Zunehmend werden Forderungen laut, der Gesetzgeber solle die Nutzung von digitalen Werken, also von Musik, Bildern und Texten, die aus dem Internet herunter geladen werden können, einer individuellen Vergütungspflicht unterwerfen. Zugleich bieten Unternehmen der Multimedia-Industrie verstärkt Plattformen im Internet (sog. digitale Wohnzimmer) an, auf denen Nutzer zum Beispiel ihre persönliche Musikauswahl ablegen können, um sie später unterwegs oder bei Freunden abrufen und nutzen zu können.*

Die Bundesregierung hat im Berichtsjahr einen Gesetzentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft<sup>20</sup> vorgelegt, der das deutsche Recht an die Europäische Urheberrechts-Richtlinie<sup>21</sup> angleichen soll. Der Entwurf sieht vor, dass die bisherige Kostenfreiheit von Privatkopien, die nicht für Erwerbszwecke gemacht werden, auch für digitale Kopien von urheberrechtlich geschützten Werken im World Wide Web gelten soll. Das gegenwärtige System der urheberrechtlichen Vergütung über eine Pauschalabgabe auf Geräte wie Drucker, Fax-Geräte oder PC's soll beibehalten werden. Hiergegen hatte sich der Bundesrat in seiner Stellungnahme gewandt und die Forderung erhoben, statt einer Pauschalvergütung für die digitale Vervielfältigung in Zukunft vorrangig auf eine individuelle Lizenzierung der Nutzung von digitalen Werken zu setzen.

Das Urheberrecht in Deutschland sichert die wirtschaftlichen Interessen der Urheber bisher in der Weise, dass die Vergütung durch Geräteabgaben pauschal erhoben und über Verwertungsgesellschaften an die Urheber ausgeschüttet werden. Dieses System geht zurück auf die Rechtsprechung des Bundesgerichtshofs, der sich mehrfach mit dem Verhältnis zwischen dem Urheberrechtsschutz und dem Schutz der Privatsphäre des Nutzers vor Ausspähung auseinandergesetzt hat. So hat das höchste deutsche Zivilgericht schon 1964 eine urheberrechtliche Verpflichtung der Käufer von Tonbandgeräten abgelehnt, beim Kauf ihren Personalausweis vorzulegen<sup>22</sup>. Später lehnte es der Bundesgerichtshof ab, die Betreiber von Kopierläden zu verpflichten, die Vorlagen der Kunden daraufhin zu überprüfen, ob ihre Ablichtungen mit dem Urheberrecht vereinbar sind<sup>23</sup>. In beiden Fällen hat er den Vorrang verfassungsrechtlich geschützter persönlicher Freiheitsrechte der Käufer und

---

<sup>20</sup> BT-Drs. 15/38

<sup>21</sup> 2001/29/EG vom 22.5.2001, ABIEU L 167/10

<sup>22</sup> Urteil vom 29.5.1964, GRUR 1965, 104

<sup>23</sup> Urteil vom 9.6.1983 GRUR 1984, 54

Kunden betont, die durch entsprechende Kontrollmaßnahmen in unangemessener Weise beeinträchtigt würden. Auf dieser Rechtsprechung beruht das datenschutzfreundliche System der Verteilung von Geräteabgaben durch Verwertungsgesellschaften (z. B. die GEMA), bei der eine Registrierung des individuellen Nutzerverhaltens von vornherein ausgeschlossen wird. Demgegenüber könnten die vom Bundesrat geforderten individuellen Lizenzvereinbarungen bei digitaler Verwertung letztlich dazu führen, dass der Urheber oder Dritte beispielsweise feststellen können, welche Seite ein Leser in einem digitalen Buch wann und wie lange aufgeschlagen hat. Damit würden weit reichende personenbezogene Nutzungsprofile ermöglicht, die bei der Nutzung herkömmlicher Medien mit gutem Grund stets seit jeher ausgeschlossen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb auf Vorschlag des Landesbeauftragten eine EntschlieÙung zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht gefasst<sup>24</sup>, in der sie den Gesetzgeber aufgefordert hat, an dem bewährten datenschutzfreundlichen Verfahren der Pauschalvergütung im Grundsatz festzuhalten. Soweit davon abgegangen werden soll, muss sichergestellt werden, dass die Ausspähung und Registrierung personenbezogener Informationen über das individuelle Nutzungsverhalten auch bei der Nutzung digitaler Werke ausgeschlossen bleibt und die urheberrechtliche Vergütung nur anhand von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke ermittelt wird.

Auch die zunehmend angebotenen "digitalen Wohnzimmer" oder elektronischen Systeme zur Verwaltung von Urheberrechten (Elektronic Copyright Management Systems, Digital Rights Management) können mit datenschutzrechtlichen Grundsätzen nur vereinbart werden, wenn sie sich strikt am Grundsatz der Datenvermeidung orientieren. Derartige Geschäftsmodelle dürften wenig aussichtsreich sein, wenn die Nutzer befürchten müssen, dass ihnen in "ihrem digitalen Wohnzimmer" jemand (die Betreiberfirma oder Dritte) elektronisch über die Schulter sieht.

Die berechtigten wirtschaftlichen Interessen von Urhebern müssen mit dem Recht der Nutzer auf unbeobachteten Medienkonsum in Einklang gebracht werden. Dazu sollte das Recht auf eine vergütungsfreie Privatkopie auch bei digitalen Werken beibehalten werden. Dabei sind pauschale Geräteabgaben zu bevorzugen. Systeme der digitalen Rechteverwaltung müssen von vornherein datenschutzfreundlich gestaltet werden.

### **3.1.7 Kettenbriefe und falsche Virenwarnungen**

*Immer wieder tauchen Kettenbriefe auf, in denen die Empfänger aufgefordert werden, für einen vermeintlich guten Zweck Postkarten an eine bestimmte Adresse zu versenden und zugleich den erhaltenen Brief an weitere Empfängern weiterzuleiten. Der Landesbeauftragte hat mehrfach derartige Kettenbriefe von Behörden in Brandenburg mit der Bitte um Beteiligung erhalten. Auch per elektronischer Post können solche Aktionen nach dem Schneeballprinzip ausgelöst werden. Auf ähnliche Weise werden zunehmend Virenwarnungen versandt, die im günstigsten Fall harmlos sind, im ungünstigsten Fall aber den Adressaten zur Löschung bestimmter Eintragungen in seinem Betriebssystem auffordern oder sogar selbst Viren transportieren.*

Bekannt geworden ist der Fall des an einem Gehirntumor erkrankten Jungen in Großbritannien, zu dessen Gunsten bereits 1989 eine Kettenbriefaktion gestartet wurde. Ziel war es, möglichst viele Adressaten dazu zu veranlassen, dem Jungen im Krankenhaus möglichst viele Postkarten, Visitenkarten oder Kopfbögen zukommen zu lassen und ihm auf diese Weise zu einem Eintrag in das Guinness-Buch der Rekorde zu verhelfen. Die Aktion war in dieser Beziehung erfolgreich. Auch verhalf sie dem Jungen zu so viel öffentlicher Aufmerksamkeit, dass ihm ein vermöglicher Amerikaner die lebensrettende Operation in einer Spezialklinik bezahlte. Der Junge ist inzwischen gesund, die Kettenbriefaktion läuft aber sowohl papiergebunden als auch elektronisch (per E-Mail) ungebremst weiter. Das zuständige Postamt in Großbritannien muss täglich massenhaft eingehende Karten und Briefe entsorgen. Die Flut an sinnlos gewordenen Genesungswünschen beeinträchtigt aber auch die persönliche Lebensführung des Adressaten: er war gezwungen, mit seiner Familie umzuziehen, um dem Problem aus dem Wege zu gehen.

Obwohl diese Zusammenhänge wiederholt publik gemacht worden sind, beteiligen sich auch Behörden im Land Brandenburg weiterhin daran. Der Landesbeauftragte hat die Absender der Kettenbriefe, die ihn erreicht haben, eindringlich gebeten, die übrigen Empfänger des Kettenbriefes über diesen Hintergrund zu informieren und zu einem Abbruch dieser für den vermeintlich Hilfsbedürftigen massiven Beeinträchtigungen beizutragen.

Auch bei elektronischen Kettenbriefen ist Skepsis geboten: Virenwarnungen, die auf diese Weise verbreitet werden, sind in aller Regel unseriös. Sie können sogar ihrerseits die Ordnungsmäßigkeit der Datenverarbeitung beim Empfänger beeinträchtigen, wenn dieser die gegebenen Empfehlungen befolgt. Seriöse Virenwarnungen werden inzwischen von verschiedenen Seiten angeboten und sollten nur bei diesen abgerufen

werden. Es gibt überdies zuverlässige Informationsquellen im Internet, die sich speziell mit falschen Virenwarnungen (Hoaxes) beschäftigen und sie entlarven<sup>25</sup>.

Behörden im Land Brandenburg sollten sich auch aus Gründen des Persönlichkeitsschutzes nicht an Kettenbriefaktionen beteiligen. Virenwarnungen per E-Mail, die nach dem Schneeballprinzip verbreitet werden, sind in aller Regel unseriös, möglicherweise sogar ihrerseits gefährlich. Aktuelle Virendefinitionen sollten von den Herstellern der eingesetzten Virenerkennungssoftware oder vom Bundesamt für die Sicherheit in der Informationstechnik bezogen werden.

### 3.1.8 Privater Botendienst in einer Kommune

*Eine kreisfreie Stadt beabsichtigte, ihren Postversand neu zu ordnen. Zum einen sollte mit dem externen Postversand innerhalb des Stadtgebietes ein anderes Unternehmen beauftragt werden als die Deutsche Post AG, die bisher diese Leistung erbrachte. Zum anderen sollte der Botendienst der Postleitstelle, also der internen Postversand zwischen den einzelnen Standorten und Fachämtern der Stadtverwaltung ausgegliedert und an ein privates Unternehmen übergeben werden.*

Gegen die Vergabe von Teilen des externen Postversands an ein anderes Unternehmen als die Deutsche Post AG bestehen keine datenschutzrechtlichen Bedenken. Wie bei der Telekommunikation ist der Markt für das Erbringen von Postdiensten grundsätzlich dem Wettbewerb geöffnet. Abgesehen von dem zum Teil noch geltenden Monopol der Deutschen Post AG bestehen für alle Anbieter deshalb nach dem Postgesetz (PostG) die gleichen rechtlichen Anforderungen. Jeder Anbieter von Postdiensten ist verpflichtet, das Postgeheimnis gemäß § 39 PostG zu wahren und die Bestimmungen der Postdienste-Datenschutzverordnung (PDSV) einzuhalten. Sendungen sind dem Anbieter daher in verschlossenen Umschlägen zu übergeben; Absenderangaben sollten stets so gestaltet sein, dass Rückschlüsse auf den Inhalt der Sendung – etwa durch konkrete Bezeichnung des Fachamtes – nicht ohne Weiteres möglich sind.

Die Durchführung des Botendienstes innerhalb der Stadtverwaltung durch eine Fremdfirma ist ebenso wie der externe Postversand als geschäftsmäßiges Erbringen von Postdiensten anzusehen. Nach dem Postgesetz kommt es nur darauf an, dass es sich um ein auf Dauer angelegtes Angebot an Dritte handelt. Es spielt deshalb keine Rolle, ob der

<sup>25</sup> siehe <<http://www.tu-berlin.de/www/software/hoax.shtml>>  
und <<http://www.bsi.bund.de/av/vb/hoaxes.htm>>

Anbieter die Post nur innerhalb der Behörde oder an externe Empfänger befördert.

Daraus folgt, dass die öffentliche Stelle bei der Durchführung des Botendienstes durch einen Dritten in technischer und organisatorischer Hinsicht grundsätzlich die gleichen Vorkehrungen zu treffen hat wie bei der Vergabe des externen Postversandes.

Sendungen, deren Empfänger (vorgesehenes Fachamt) schon aus der ersichtlichen Anschrift ersichtlich sind, können dem Auftragnehmer ungeöffnet zur Weiterverteilung übergeben werden. Für Sendungen, die zur Feststellung des konkreten Adressaten innerhalb der Verwaltung geöffnet werden müssen, sind zur Weiterverteilung durch den Auftragnehmer verschließbare Behältnisse (verschließbare Versandtaschen, -kästen usw.) zu verwenden. Diese sind so zu gestalten, dass sie grundsätzlich nur durch Bedienstete der öffentlichen Stelle geöffnet werden können. Aufgaben wie das Öffnen, interne Zuordnen und Kuvertieren von Briefsendungen können einem privaten Auftragnehmer hingegen nicht ohne Weiteres übertragen werden.

Gegen die Beauftragung eines privaten Dienstleisters mit dem externen Postversand oder der Durchführung des Botendienstes innerhalb der eigenen Verwaltung durch eine öffentliche Stelle bestehen keine datenschutzrechtlichen Bedenken. Die öffentliche Stelle hat dabei geeignete technische und organisatorische Maßnahmen zu treffen, um eine Kenntnisnahme des Inhalts der Postsendungen durch den Auftragnehmer auszuschließen.

## **3.2 Presse und Rundfunk**

### **3.2.1 Hohes Datenschutzniveau auch beim Rundfunk Berlin-Brandenburg**

*Die Regierungschefs der Länder Berlin und Brandenburg haben den Staatsvertrag über die Errichtung der gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg mit dem Namen "Rundfunk Berlin-Brandenburg (RBB)" unterzeichnet. Der RBB soll Mitte des Jahres 2003 seinen Betrieb aufnehmen und die bisherigen Rundfunkanstalten Ostdeutscher Rundfunk Brandenburg (ORB) und Sender Freies Berlin (SFB) ersetzen. Die Berliner Senatskanzlei sowie die Staatskanzlei des Landes Brandenburg haben den Berliner Beauftragten für Datenschutz und Informationsfreiheit und den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg bei der Ausarbeitung des Staatsvertrages beteiligt.*

Der Staatsvertrag behält das bisher für ORB und SFB geltende hohe Datenschutzniveau auch für den RBB bei. Wie bereits das ORB-Gesetz enthält der Staatsvertrag selbst alle notwendigen Vorschriften für die Verarbeitung personenbezogener Daten im journalistisch-redaktionellen Bereich. Dabei beschränkt sich der Staatsvertrag – anders als im Preserecht – nicht darauf, lediglich die Vorgaben des Bundesdatenschutzgesetzes für die Datenverarbeitung durch Journalisten umzusetzen. Vielmehr räumt er betroffenen Personen weitere Rechte ein. Dabei ist vor allem hervorzuheben, dass Betroffene auch im journalistisch-redaktionellen Bereich ein umfassendes Recht auf Auskunft über die vom RBB über sie gespeicherten Daten erhalten sollen. Dieses kann vor allem aus Gründen des Quellenschutzes eingeschränkt werden. Außerdem enthält der Staatsvertrag Regelungen zum Umgang mit Gegendarstellungen sowie das Jedermann-Recht, sich unmittelbar an den Datenschutzbeauftragten des RBB wenden zu können.

Verarbeitet der RBB personenbezogene Daten außerhalb des journalistischen Bereichs, so gelten für diesen so genannten wirtschaftlich-administrativen Bereich die allgemeinen Bestimmungen des Berliner Datenschutzgesetzes. Dies bedeutet, dass sich der RBB beispielsweise bei der Verarbeitung personenbezogener Daten des bei ihm beschäftigten Personals und vor allem der Gebührenzahlerinnen und Gebührenzahler an die gleichen Vorschriften halten muss, wie alle anderen öffentlichen Stellen auch. Hervorzuheben ist, dass die Verarbeitung personenbezogener Daten im wirtschaftlich-administrativen Bereich beim RBB (und bei der Gebühreneinzugszentrale [GEZ], soweit sie vom RBB beauftragt

wird) durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit im Benehmen mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg kontrolliert wird. Allein auf diese Weise kann die vom europäischen Recht vorgeschriebene völlig unabhängige Datenschutzkontrolle außerhalb des von der Pressefreiheit geschützten journalistisch-redaktionellen Bereichs auch in Zukunft gewährleistet werden.

Das bisher für den Ostdeutschen Rundfunk Brandenburg bestehende hohe Datenschutzniveau wird auch in Zukunft beim Rundfunk Berlin-Brandenburg gewährleistet.

### **3.2.2 Darf sich die GEZ auf dem Adressenmarkt bedienen?**

*Aufgrund der Beschwerde einer Bürgerin haben wir uns erneut mit der Erhebung von personenbezogenen Daten zur Ermittlung von "Schwarzsehern und -hörern" durch die GEZ befasst. Gegenstand unserer Prüfung war die Praxis der vom Ostdeutschen Rundfunk Brandenburg (ORB) beauftragten Gebühreneinzugszentrale (GEZ), Anschriften bei privaten Adresshändlern zu erwerben, um nicht angemeldete Personen anzuschreiben.*

Die GEZ vertrat dazu gegenüber der Bürgerin die Auffassung, dass sie aufgrund der §§ 28, 29 des Bundesdatenschutzgesetzes (BDSG) befugt sei, Anschriften bei privaten Adresshändlern durch Kauf, Miete oder Leasing zu erheben und diese für "werblich-informierende Zwecke" zu nutzen. Diese Auffassung trifft nicht zu.

Die Verarbeitung personenbezogener Daten durch die GEZ im Zusammenhang mit der Erhebung der Rundfunkgebühren richtet sich mangels spezieller Rechtsgrundlage im Rundfunkgebührenstaatsvertrag im Zuständigkeitsbereich des ORB ausschließlich nach dem Brandenburgischen Datenschutzgesetz. Auf die für nicht-öffentliche Stellen geltenden §§ 28, 29 BDSG kann der ORB als öffentliche Stelle die Verarbeitung personenbezogener Daten nicht stützen. Die GEZ ist nach dem Rundfunkgebührenstaatsvertrag Auftragnehmerin einer Datenverarbeitung im Auftrag. Insoweit bleibt rechtlich der ORB Daten verarbeitende Stelle, sodass auch für die Verarbeitung personenbezogener Daten brandenburgischer Teilnehmer durch die GEZ die Vorschriften des Brandenburgischen Datenschutzgesetzes gelten. Diese Auffassung wird vom ORB inzwischen geteilt.

Zweifelhaft ist darüber hinaus, ob die mit dem Erwerb der Anschriften verbundene Erhebung personenbezogener Daten zur Aufgabenerfüllung

der GEZ erforderlich ist. Da davon auszugehen ist, dass die GEZ überwiegend Anschriften von Personen erhält, die bereits angemeldet oder nicht Rundfunkteilnehmer sind, erhebt sie mehr personenbezogene Daten, als sie für die Ermittlung von "Schwarzsehern bzw. Schwarzhörern" benötigt.

Zudem erhebt die GEZ hier personenbezogene Daten bei Dritten ohne Kenntnis der Betroffenen. Dies ist öffentlichen Stellen nur unter engen Voraussetzungen erlaubt. Nach Auffassung des ORB lässt es das Brandenburgische Datenschutzgesetz zu, die Anschriften bei den Adresshändlern zu erheben, weil es sich dabei um Daten handelt, die aus allgemein zugänglichen Quellen entnommen werden können. Auch diese Ansicht trifft nicht zu.

Die bei privaten Adresshändlern erworbenen Anschriften stammen nicht aus allgemein zugänglichen Quellen im Sinne des Datenschutzrechts. Allgemein zugänglich Quellen sind solche Informationsquellen, die technisch geeignet und bestimmt sind, der Allgemeinheit, d. h. einem individuell nicht bestimmbar Personenkreis, Informationen zu verschaffen. Diese Informationsquellen müssen der Allgemeinheit so zur Verfügung stehen, dass sie ohne rechtliche oder tatsächliche Einschränkungen oder Hindernisse genutzt werden können. Dazu gehören beispielsweise die veröffentlichten Medien (z. B. Zeitungen, Rundfunk), Adressbücher, Telefonbücher oder auch öffentlichen Register (z. B. Handels- oder Vereinsregister), nicht aber Anschriften, die sich im Besitz privater Adresshändler befinden.

Auch der für die Datenschutzkontrolle im wirtschaftlich-administrativen Bereich beim Sender Freies Berlin zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie der für den Hessischen Rundfunk in gleicher Weise zuständige Hessische Datenschutzbeauftragte sehen in ihrem Landesrecht keine Rechtsgrundlage für die hier geschilderte Praxis der GEZ.

Die Praxis der GEZ, Anschriften bei privaten Adresshändlern zu erwerben, ist mangels Rechtsgrundlage nicht zulässig. Wir haben den ORB daher aufgefordert, in Zukunft keine personenbezogenen Daten bei privaten Adresshändlern mehr zu erheben.

## **4 Inneres**

### **4.1 Polizei- und Ordnungsbehörden**

#### **4.1.1 Videoüberwachung bei Fußballspielen und Demonstrationen**

*Dass nicht nur öffentliche Straßen und Plätze durch die Polizei Video überwacht werden, sondern auch Fußballspiele und Demonstrationen, hat im Berichtszeitraum einige Bürger veranlasst, sich mit der Frage an den Datenschutzbeauftragten zu wenden, ob dies zulässig sei.*

Nach dem Brandenburgischen Polizeigesetz (§ 31 Abs. 1) darf die Polizei auch bei Fußballspielen und anderen öffentlichen Veranstaltungen, die nicht dem Versammlungsgesetz unterliegen, Videokameras einsetzen, wenn Tatsachen die Annahme rechtfertigen, dass Straftaten oder Ordnungswidrigkeiten begangen werden sollen. Im Gegensatz zur offenen Videoüberwachung öffentlicher Straßen und Plätze muss hier nicht durch Hinweisschilder über die Videoüberwachung informiert werden. Anfallende Videoaufzeichnungen und personenbezogene Daten sind spätestens nach einem Monat zu löschen, falls sie nicht zur Verfolgung von Ordnungswidrigkeiten oder Straftaten im Einzelfall benötigt werden oder Tatsachen die Annahme rechtfertigen, dass Betroffene auch in Zukunft Straftaten von erheblicher Bedeutung begehen wollen.

Anders als Fußballspiele unterliegen Demonstrationen dem Versammlungsgesetz. Der Einsatz von Videokameras ist dabei nicht im gleichen Umfang zulässig wie bei sonstigen Veranstaltungen, weil die Teilnehmer an einer Versammlung sich auf das Grundrecht der Versammlungsfreiheit berufen können. Nach § 12a Versammlungsgesetz (VersammlG) dürfen Aufzeichnungen nur unter engeren Voraussetzungen erstellt werden, wenn nämlich tatsächliche Anhaltspunkte für die Annahme bestehen, dass die Verwirklichung erheblicher Gefahren für die öffentliche Sicherheit und Ordnung unmittelbar bevorsteht. Daraus ergibt sich, dass die Polizei alle zur Anfertigung von Aufzeichnungen notwendigen Maßnahmen von der Bereitstellung der Geräte bis zur Beobachtung der Demonstrationsteilnehmer bereits vor Eintritt einer konkreten Gefahr treffen darf. Die Polizei kann auch auf eine bereits vorhandene private Überwachungsanlage unter der Voraussetzung zurückgreifen, dass die Grundrechtseingriffe – beginnend von der Auswahl des geeigneten Überwachungsstandortes bis zur Verarbeitung und Auswertung der Aufzeichnungen – ausschließlich durch die Polizei selbst erfolgen. Bisher hat die brandenburgische Polizei bei Demonstrationen jedoch noch nicht auf privat betriebene Videoüberwachungsanlagen zurückgegriffen.

Die Aufzeichnungen müssen gem. § 12a Abs. 2 VersammlG unverzüglich nach der Demonstration vernichtet werden, wenn sie nicht für die Verfolgung von Straftaten oder im Einzelfall zur Gefahrenabwehr benötigt werden. Letzteres kann dann der Fall sein, wenn jemand verdächtig ist, Straftaten bei oder im Zusammenhang mit der Demonstration vorbereitet oder begangen zu haben und vermutet wird, dass die betreffende Person in gleicher Weise bei zukünftigen Demonstrationen wieder in Erscheinung treten wird. In solchen Ausnahmefällen beträgt die zulässige Aufbewahrungsfrist drei Jahre.

Zur Videoüberwachung setzt die Polizei speziell ausgebildete Beweissicherungsgruppen ein. Die Aufnahmen werden durch szenekundige Polizeibeamte ausgewertet. Wenn sich Erkenntnisse über Straftaten oder Ordnungswidrigkeiten ergeben, wird die Aufnahme kopiert und an die Kriminalpolizei weitergeleitet und das Original bis zum Abschluss des staatsanwaltschaftlichen bzw. des gerichtlichen Verfahrens archiviert. Ein Protokoll dokumentiert den Verbleib der einzelnen Videobänder.

Bei der Überprüfung der Beschwerde eines Demonstrationsteilnehmers, der sich von einer Kamera auf einem öffentlichen Platz der Landeshauptstadt überwacht fühlte, stellten wir folgendes fest: Es handelte sich nicht um eine Videokamera der Polizei, sondern um eine Webkamera (Webcam), die auf einer katholischen Kirche angebracht war. Da die katholische Kirche als Rechtsträger nicht der Kontrolle durch den Landesbeauftragten unterliegt, haben wir dem Petenten geraten, sich an den kirchlichen Datenschutzbeauftragten zu wenden. Der Fall macht deutlich, dass die Zahl der Videokameras mit unterschiedlicher Zielrichtung wächst und nicht alle Bürger gewillt sind, dies ungeprüft hinzunehmen.

Die Polizei darf zur Überwachung von Veranstaltungen und Versammlungen unter bestimmten gesetzlichen Voraussetzungen Videokameras einsetzen und sowohl den allgemeinen Geschehensablauf als auch Personen aufnehmen. Diese Voraussetzungen sind bei Versammlungen enger gefasst, weil die Teilnehmer ihr Grundrecht auf Versammlungsfreiheit ausüben. Alle Aufzeichnungen müssen innerhalb einer kurzen Frist ausgewertet und vernichtet werden, es sei denn, sie werden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, sowie im Einzelfall auch zur Gefahrenabwehr benötigt.

#### 4.1.2 Datenexport vor und nach Weltwirtschaftskonferenzen – ein Nachtrag

*Bereits im vergangenen Jahr haben wir über den Datenexport vor und nach Weltwirtschaftskonferenzen an die Polizeien der ausländischen Konferenzorte berichtet<sup>26</sup>. Ein Petent war während des G-10-Treffens bei einer nächtlichen Razzia in einer Schule in Genua festgenommen worden. Das Bundeskriminalamt (BKA) teilte der italienischen Polizei mit, dass gegen ihn bereits u. a. wegen Waffenbesitzes ermittelt worden sei. Die Prüfung des Sachverhalts hat bislang ergeben, dass gegen den Betroffenen nur ein Ermittlungsverfahren wegen Widerstands gegen Vollstreckungsbeamte eingeleitet wurde – nicht aber wegen Waffenbesitzes. Das zuletzt genannte Datum war fälschlicherweise aufgenommen worden.*

Zuständig für die Einstellung von Daten in der beim BKA betriebenen Verbunddatei PIOS Innere Sicherheit (APIS) ist das Landeskriminalamt Brandenburg (LKA). Im Fall des Petenten ist dort versehentlich neben dem richtigen Tatvorwurf auch das falsche Datum "Waffenbesitz" eingegeben worden. Aufgrund unserer Nachfrage hat das LKA als anliefernde Stelle das BKA gem. § 32 Abs. 8 Bundeskriminalamtsgesetz (BKAG) unterrichtet, dass ihm mit dem Tatbestand "Waffenbesitz" ein falsches Datum übermittelt worden ist und die APIS-Speicherung zu dem Petenten entsprechend dem oben beschriebenen Verfahren gelöscht. Die Praxis des BKA, die Löschung eines Bundeslandes als Besitzer des von ihm in APIS eingestellten Datensatzes nicht nachzuvollziehen, sondern sich ohne Prüfung des Einzelfalls automatisch als Alleinbesitzer einzutragen, verstößt gegen § 32 Abs. 2 i. V. m. Abs. 8 BKAG, wonach übermittelte Daten zu löschen sind, wenn die übermittelnde Stelle das BKA über die Löschung informiert. Ob das BKA seiner gesetzlichen Verpflichtung gem. § 32 Abs. 6 BKAG nachgekommen ist, die falsche Übermittlung gegenüber der italienischen Polizei zu korrigieren, hat sich noch nicht klären lassen.

Auch die Datenverarbeitung des zuständigen Polizeipräsidiums war im vorliegenden Fall mangelhaft. Zwar hat das Polizeipräsidium die zu dem Petenten geführte Kriminalakte vernichtet und die Datensätze im Polizeilichen Auskunftssystem Straftaten (PASS) sowie im Landeskriminalaktennachweis (KAN Land) gelöscht, nachdem von der Staatsanwaltschaft die Einstellung des Ermittlungsverfahrens wegen Widerstands gegen Vollstreckungsbeamte gem. § 153 Abs. 1 Strafprozessordnung mitgeteilt worden war. Seinen eigenen Mitteilungspflichten gegenüber dem LKA ist es jedoch nicht nachgekommen. Nach den Richtlinien für

den kriminalpolizeilichen Meldedienst in Fällen politisch motivierter Kriminalität sollen die Staatsschutzdienststellen in den Polizeipräsidiien das LKA unterrichten, wenn sich aus den Entscheidungen der Staatsanwaltschaft oder des Gerichts ergibt, dass die Gründe, die zu einer Meldung in den o. g. Fällen geführt haben, nicht zutreffen. Das LKA ist aufgrund dieser Unterrichtung verpflichtet, die von ihm vorgenommene Datenspeicherung in APIS zu prüfen.

Diese Meldungen, die das Polizeipräsidium nach eigener Aussage noch nie vorgenommen hat, sind unerlässlich, weil ohne sie das LKA nicht in der Lage ist, die erforderliche Datenpflege in APIS zu betreiben. Informationen über den Ausgang der staatsanwaltschaftlichen oder gerichtlichen Verfahren im Fall von APIS-Datensätzen können nur von den Polizeipräsidiien kommen, weil nur sie die Verknüpfung von APIS-Speicherung und Verfahrensausgang herstellen können. Unterlassene Mitteilungen über den Verfahrensausgang sind in jedem Fall ein schwerwiegender datenschutzrechtlicher Mangel, weil die aus diesem Grund unterbliebenen Erforderlichkeitsprüfungen der Datenspeicherungen in APIS zu unzulässigen Eingriffen in die Persönlichkeitsrechte der Betroffenen führen und ihnen dadurch schwerer Schaden entstehen kann: Im Fall des Petenten hätte die Mitteilung, dass das Ermittlungsverfahren wegen Widerstands gegen Vollstreckungsbeamte eingestellt worden ist, eine Prüfung der APIS-Speicherung auslösen müssen, bei der die falsche Datenspeicherung "Waffenbesitz" aufgefallen wäre.

Die Polizeipräsidiien sind verpflichtet, das LKA über den Ausgang von staatsanwaltschaftlichen Ermittlungen und gerichtlichen Verfahren zu informieren. Nur so kann ausgeschlossen werden, dass Daten von Betroffenen zu Unrecht weiter in polizeilichen Dateien gespeichert werden.

#### **4.1.3    Überschießende Datenerhebung und "geheime" Führungszeugnisse von Hundehaltern**

*Eine Gemeinde nutzte den Fragebogen zur Anmeldung von als gefährlich eingestuften Hunden zur Erhebung von Gesundheitsdaten der Bürger. So waren Fragen nach Drogen- und Alkoholabhängigkeit zu beantworten. In einem anderen Fall sollte der Bürger seine Steuernummer angeben. Unklar war auch, ob Bürger das den Behörden vorliegende Führungszeugnis selbst einsehen dürfen.*

Die Gemeinden, die die Hundeanmeldung zur umfassenden Datenerhebung nutzten, wurden von uns auf die rechtlichen Grundlagen hingewiesen und änderten im Ergebnis ihre Fragebögen, sodass nunmehr nur die zulässigen Daten der Bürger erhoben werden.

Bei dem nach § 12 Hundehalterverordnung vorzulegenden Führungszeugnis handelt es sich um ein "Führungszeugnis zur Vorlage bei einer Behörde". Dieses wird direkt – ohne vorherige Kenntnisnahme des Antragstellers – an die entsprechende Behörde, hier die Ordnungsämter der Gemeinden, Ämter oder Städte, übersandt, die dies zur Prüfung der Zuverlässigkeit des Hundehalters benötigen. Selbstverständlich hat der Bürger das Recht, sein Führungszeugnis beim Ordnungsamt einzusehen.

Eine darüber hinausgehende Weitergabe der im Führungszeugnis vorhandenen personenbezogenen Daten an Dritte oder andere Behörden ist ohne gesetzliche Grundlage nicht zulässig. Hierauf wurden die Behörden in den genannten Fällen ausdrücklich hingewiesen und die anfragenden Bürger entsprechend aufgeklärt.

In den Fragebögen zur Anmeldung eines Hundes dürfen nur solche Daten abgefragt werden, die hierfür auch erforderlich sind. Führungszeugnisse der Hundehalter sind diesen auf Wunsch offen zu legen.

#### **4.1.4 Datenschutz in Bußgeldverfahren**

*Wie lange dürfen Datensätze von Bußgeldverfahren nach dem Eingang der Zahlung bei der Bußgeldstelle im aktuellen Bestand verbleiben und für andere Zwecke genutzt werden?*

Nach Zahlung der Geldbuße ist der Bußgeldbescheid rechtskräftig geworden und die Wiederaufnahme des Verfahrens als Ordnungswidrigkeit oder Straftat gem. § 84 Ordnungswidrigkeitengesetz ausgeschlossen. Das Bußgeldverfahren ist erledigt oder wird nach Zahlung des Verwarnungsgeldes gar nicht erst eingeleitet. Nach Zahlungseingang ist die personenbezogene Speicherung somit nur solange erforderlich, bis die ordnungsgemäße Erledigung geprüft und festgestellt worden ist. Nach unserer Auffassung sollte dieser Zeitraum nicht länger als drei Monate sein. Die weitere Speicherung des Datensatzes im aktuellen Datenbestand wird unzulässig, weil er nicht mehr erforderlich ist. Daher ist auch die Nutzung des personenbezogenen Datensatzes zu anderen Verwaltungszwecken unzulässig. Zur Erfüllung der gesetzlichen Aufbewahrungsfristen von drei bzw. von fünf Jahren genügt es, die Bußgeldakten aufzuheben. Einer Speicherung der entsprechenden Datensätze im automatisierten Verfahren bedarf es zu diesem Zweck nicht. Auch für Statistikzwecke sind die Identdaten des Betroffenen nicht erforderlich. Dazu reichen die Datenfelder "Tatbestand", "Höhe der Geldbuße" und "Tatort".

Die gebotene Dateipflege kann am besten durch ein automatisches Lösungsverfahren sichergestellt werden. Bei der überwiegenden Mehrzahl der von den hiesigen Bußgeldstellen betriebenen Verfahren erfolgt die Löschung des Datensatzes nach Zahlungseingang bereits automatisch. Vereinzelt haben die angeschriebenen Stellen dies zum Anlass genommen, ihr Bußgeldverfahren nachzurüsten. Bei mehreren Stellen, so auch bei der Zentralen Bußgeldstelle der Polizei, werden die Daten nach rechtskräftigem Abschluss des Verfahrens in eine Vorgangsverwaltungsdatei überführt und im eigentlichen Bußgeldbestand gelöscht. Solange die dort gespeicherten Daten nur zum Zwecke der Verwaltung der Zahlungsunterlagen genutzt und nach einer angemessenen Frist auch dort gelöscht werden, bestehen dagegen keine datenschutzrechtlichen Einwände.

Datensätze, die im Zusammenhang mit der Bearbeitung von Verwarungs- und Bußgeldverfahren gespeichert wurden, müssen nach rechtskräftigem Abschluss des Verfahrens und Zahlungseingang des Verwar- bzw. des Bußgeldes in der Bußgelddatei gelöscht werden.

Soweit die Datensätze in eine automatisierte Vorgangsverwaltungsdatei überführt und ausschließlich zum Zweck der Vorgangsverwaltung der Bußgeldakten genutzt und nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist von drei bzw. von fünf Jahren zusammen mit der entsprechenden Zahlungsunterlage vernichtet bzw. gelöscht werden, ist dies zulässig.

## **4.2 Verfassungsschutz**

### **Novellierung des Verfassungsschutzgesetzes und Stärkung der parlamentarischen Kontrolle**

*Nachdem das Verfassungsschutzgesetz des Bundes durch das zu Jahresbeginn in Kraft getretene Terrorismusbekämpfungsgesetz um neue Eingriffsbefugnisse ergänzt worden war<sup>27</sup>, wurde das brandenburgische Landesrecht mit dem Gesetz zur Umsetzung des Terrorismusbekämpfungsgesetzes und zur Stärkung der parlamentarischen Kontrolle vom 24.10.2002<sup>28</sup> dieser Rechtslage angepasst.*

So sind auch in Brandenburg die Aufgaben des Verfassungsschutzes auf die Untersuchung von Bestrebungen, die sich gegen den Gedanken der Völkerverständigung und das friedliche Zusammenleben der Völker wenden, erweitert worden. In der Begründung zum Gesetz wurde das Aufgabenfeld dahingehend eingegrenzt, dass nicht jede Bestrebung für

<sup>27</sup> siehe Tätigkeitsbericht 2001, A 1.1

<sup>28</sup> GVBl. I S. 154

sich genommen ausreicht, um ein Tätigwerden der Brandenburgischen Verfassungsschutzbehörde zu rechtfertigen. Sie muss sich vielmehr auf die innere Sicherheit des Landes auswirken.

Weiterhin ist die Speicherdauer für personenbezogene Daten über verfassungsfeindliche Bestrebungen, die auswärtige Belange der Bundesrepublik Deutschland gefährden sowie über Bestrebungen, die gegen den Gedanken der Völkerverständigung und das friedliche Zusammenleben der Völker gerichtet sind, von zehn auf fünfzehn Jahre ausgedehnt worden.

Die Verlängerung der Speicherdauer wird mit den Anschlägen vom 11. September 2001 in den USA begründet. Es habe sich im Nachhinein erwiesen, dass bei Personen in diesen Beobachtungsfeldern u. U. erst nach zehn Jahren Erkenntnisse anfallen würden. Tatsächlich haben die als Tatverdächtige in Betracht kommenden Personen in den Monaten vor den Anschlägen allerdings zahlreiche Hinweise und Spuren hinterlassen, die jedoch von den Sicherheitsbehörden entweder nicht wahrgenommen oder nicht entsprechend verfolgt worden sind. Problematisch in solchen Fällen ist nicht das zu frühe Vernichten von Erkenntnissen, sondern die rechtzeitige Gewinnung relevanter Informationen für künftige Taten. Mit der Ausweitung der Speicherdauer wird den Betroffenen ein erheblicher Grundrechtseingriff zugemutet, obwohl sich die Ermittlungslage dadurch nicht wesentlich verbessert.

Auch die Brandenburgische Verfassungsschutzbehörde hat nunmehr die Befugnis, von Luftverkehrsunternehmen einschließlich Reiseveranstaltern, Kreditinstituten im weitesten Sinne, Postdienstleistern sowie Telekommunikations- und Teledienstleistern Auskunft über deren Kunden zu verlangen. Die angefragten Firmen dürfen den Betroffenen über das Auskunftersuchen und die erteilten Auskünfte nicht informieren. Sie sind jedoch weder nach dieser noch nach einer anderen gesetzlichen Vorschrift verpflichtet, dem Ersuchen Folge zu leisten.

Der Landesgesetzgeber ist der Empfehlung des Landesbeauftragten nicht gefolgt, die erweiterten Befugnisse des Verfassungsschutzes auf Landesebene zu evaluieren, obwohl die Situation in Brandenburg anders zu bewerten sein kann als in anderen Bundesländern.

Auch wenn das Gesetz zur Änderung des Brandenburgischen Verfassungsschutzgesetzes<sup>29</sup> nicht über die Vorgaben des Terrorismusbekämpfungsgesetzes des Bundes hinausgeht, entspricht es doch der vom Vizepräsidenten des Bundesverfassungsgerichts festgestellten Tendenz

---

<sup>29</sup> W. Hassemer, Staat, Sicherheit und Information in: Bizer/Lutterbeck/Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft 2002, S. 225, 236

der gegenwärtigen Gesetzgebung, "bei der Risikoprävention jegliches Maß aufzugeben und dabei der ... Kontrolle vorbehaltlos zu trauen".

Mit der gleichzeitigen Novellierung des Gesetzes zur Ausführung des G 10-Gesetzes werden andererseits die Kontrollrechte der G 10-Kommission zum Schutz der Grundrechte verstärkt. Sie ist das Kontrollorgan des Landtags für die auf der Grundlage des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10-Gesetz) durchgeführten Überwachungsmaßnahmen der Verfassungsschutzbehörde. Ihre Mitglieder werden vom Innenministerium monatlich über beabsichtigte Überwachungsmaßnahmen unterrichtet. Dazu gehört nach der neuen gesetzlichen Regelung auch die Unterrichtung über die vorgesehenen Ersuchen bei Luftverkehrsunternehmen und anderen nicht-öffentlichen Stellen. Damit sie ihren damit erheblich erweiterten Kontrollaufgaben nachkommen kann, verpflichtet das Verfassungsschutzgesetz die Landesregierung, der Kommission ausreichende Sach- und Personalmittel zur Verfügung zu stellen. Auch kann die Kommission den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht hinzuziehen und sich von ihm zu datenschutzrechtlichen Problemen bei einzelnen Überwachungsmaßnahmen beraten lassen.

Während die Kommission den gesamten Prozess der Erhebung, Verarbeitung und Nutzung der bei Abhörmaßnahmen oder Befragungen nach dem neuen Verfassungsschutzgesetz erlangten Daten durch die Verfassungsschutzbehörde kontrolliert, unterliegen öffentliche Stellen, die solche Daten vom Verfassungsschutz erhalten, der Kontrolle durch den Landesbeauftragten.

Mit der Novellierung sind die Eingriffsbefugnisse der Verfassungsschutzbehörde in die Persönlichkeitsrechte der Bürger erheblich ausgeweitet worden. Dem steht die datenschutzrechtlich zu begrüßende Verpflichtung gegenüber, die parlamentarische Kontrolle durch eine angemessene Ausstattung der G 10-Kommission mit Sachmitteln und Personal und eine Berichtspflicht der Landesregierung über die vorgesehenen Überwachungsmaßnahmen zu verstärken.

## 4.3 Ausländer

### 4.3.1 Zentrale Datenbank "Passabgleich"

*Im Herbst 2001 hat die Innenministerkonferenz das Bund-Länder-Gremium "AG Rückführung" beauftragt, eine endgültige Konzeption für ein bundesweites Verfahren zu erarbeiten, das die Zuordnung von den ca. 20.000 aufgefundenen oder aufbewahrten Passdokumenten zu in Deutschland lebenden Ausländern ermöglicht. Die Erforderlichkeit einer solchen Passabgleichstelle wird damit begründet, dass Asylbewerber oder sich illegal in Deutschland aufhaltende Ausländer zum Vertuschen ihrer Identität ihre Ausweispapiere wegwerfen und andere Namen annehmen, um eine Abschiebung zu verhindern oder zumindest zu erschweren. Für die Zuordnung der Pässe sind Passlichtbilder und aktuelle Fotos der Betroffenen die ausschlaggebenden Abgleichsmerkmale der Datenbank.*

Nach der ersten Konzeption sollten bei einer Bundeszentralstelle die digitalisierten Lichtbilder sowie die Identdaten und Merkmale wie Größe, Geschlecht und Staatsangehörigkeit aus den nicht zuordenbaren Dokumenten gespeichert und verwaltet werden. Die in den Ländern als Landeszentralstelle bestimmte Ausländerbehörde sollte die Daten der neu eingegangenen Ausweisdokumente übermitteln, sodass bei der Bundeszentralstelle stets eine Datensammlung aus allen nicht zuordenbaren Ausweisdokumenten zur Verfügung stehen würde, die allen Landeszentralstellen regelmäßig zu überspielen wäre. Der automatisierte Abgleich und die Zuordnung eines Lichtbilds aus dem Bestand "herrenloser Pässe" zu dem Foto einer Person, das im Rahmen einer erkennungsdienstlichen Behandlung eines Ausländers mit ungeklärter Identität gefertigt wird, sollte in der Zentralstelle des Bundeslandes erfolgen, in dem der Betroffene sich aufhält.

Diese erste Konzeption war mit dem Ausländergesetz nicht vereinbar, auch wenn an der Notwendigkeit des Vorhabens als solchem keine grundsätzlichen Zweifel bestanden. Dem gegenüber hat das brandenburgische Innenministerium die Auffassung vertreten, dass aufgrund des § 63 Abs. 2 Ausländergesetz (AuslG) das Bundesinnenministerium mit einer Verwaltungsvorschrift eine Ausländerbehörde in einem Bundesland als Bundeszentralstelle bestimmen kann. Rechtsgrundlage für die Landeszentralstellen der Bundesländer sei dementsprechend § 63 Abs. 1 AuslG, mit dem die Länder ermächtigt werden, eine Ausländerbehörde als Landeszentralstelle zu bestimmen. Die Befugnis der Landeszentralstellen zur Erhebung und Verarbeitung der zum Abgleich notwendigen Daten wie Lichtbild, aus biometrischen Merkmalen des Gesichtes errechnete Formeln, Geburtsdatum, Größe, Geschlecht und Staatsange-

hörigkeit sollte sich aus der Ausländerdateiverordnung ergeben, die noch entsprechend zu ergänzen wäre.

Die Ermächtigungsnorm zur Schaffung einer Bundeszentralstelle ist allerdings begrenzt auf die Bestimmung der zuständigen Ausländerbehörde für die Fälle, in denen Ausländerbehörden mehrerer Bundesländer zuständig sein können oder der Ausländer sich nicht mehr im Bundesgebiet aufhält. Diese Voraussetzungen liegen hier nicht vor. Wir haben daher vorgeschlagen, die Einrichtung einer Bundeszentralstelle im Wege eines Verwaltungsabkommens zwischen den Bundesländern als Datenverarbeitung im Auftrag zu realisieren.

Ebenso wenig ist § 63 Abs. 1 AuslG eine ausreichende Ermächtigungsgrundlage für die Einrichtung einer brandenburgischen Landeszentralstelle, die anhand des Datenbestandes einer Bundeszentralstelle den Abgleich vornehmen sollte. Bei der Vorschrift handelt es sich um eine reine Zuständigkeitsnorm, die keine neuen Befugnisse einräumt. Die Schaffung eines neuen bundesweiten Registers hätte keine ausreichende gesetzliche Grundlage.

Unterdessen hat die AG "Rückführung" einen Abschlussbericht vorgelegt, in dem ein dezentraler Aufbau der Passabgleichstellen vorgeschlagen wird. Danach werden nur bei den auf der Grundlage des § 63 Abs. 1 Satz 2 AuslG als Landeszentralstellen bestimmten Ausländerbehörden ein Zentralserver mit den Bestandsbildern und -daten aus nicht zuordenbaren Dokumenten eingerichtet und das Vorhaben zur Einrichtung einer Bundeszentralstelle aufgegeben. Der bei allen Landeszentralstellen identische Anfangsbestand wird dort ständig durch die Bestandsdaten neu aufgefunderer Dokumente aktualisiert. Durch einen regelmäßigen Datenaustausch steht allen Landeszentralstellen jeweils ein aktualisierter Datenbestand zum Abgleich mit Suchanfragen zur Verfügung. Die digitalisierten Suchbilder werden nur zum automatisierten Abgleich genutzt, aber nicht selbst im tagesaktuellen Bestand des Landesrechners gespeichert.

Angesichts der dezentralen Lösung haben wir unsere Bedenken zurückgestellt.

Eine bei einer noch zu bestimmenden Ausländerbehörde in Brandenburg eingerichtete Passabgleichstelle kann auf der Grundlage des bestehenden Ausländergesetzes betrieben werden. Ihre Befugnisse zur Erhebung und Verarbeitung der dazu erforderlichen Daten müssen in der Ausländerdateiverordnung auf der Grundlage des § 80 Abs. 1 Nr. 3 AuslG geregelt werden.

## 4.3.2 Kontrollen in Asylbewerberunterkünften

### 4.3.2.1 Besucherbücher und Einlasskontrollen

*In Asylbewerberunterkünften werden sog. "Besucherbücher" geführt, in die der Wachschutz Name und Ziel der Besucher sowie Dauer des Aufenthalts einträgt. Dazu muss sich jeder Besucher beim Betreten der Unterkunft ausweisen oder sogar den Ausweis für die Dauer seines Besuches hinterlegen. In einigen Unterkünften kontrolliert der Wachschutz bei Besuchern, die ihrer äußeren Erscheinung nach Asylbewerber sein könnten, auch, ob sie gültige Bescheinigungen zum Verlassen ihres Aufenthaltsorts haben und verweigert den Zutritt, wenn sie nicht vorgelegt werden.*

Die zuständigen Ordnungsämter in den Landkreisen und kreisfreien Städten halten Besucherbücher und Ausweiskontrollen zum Schutz von Bewohnern und Gästen und zur Aufrechterhaltung der Ordnung in den Unterkünften für erforderlich und verweisen auf § 23 Ordnungsbehördengesetz (OBG) i. V. m. § 12 Abs. 1 Nr. 1 Brandenburgisches Polizeigesetz (BbgPolG) als Rechtsgrundlage für die Maßnahmen. Polizei und Staatsanwaltschaft nutzen die Besucherbücher, die ständig weitergeführt werden, für ihre strafrechtliche Ermittlungstätigkeit.

Die routinemäßige Datenspeicherung über die Besucher von Asylbewerberunterkünften kann nicht auf § 23 OBG gestützt werden. In dieser Vorschrift werden durch Verweis auf die entsprechenden Regelungen des Polizeigesetzes die zulässigen Eingriffsbefugnisse aufgelistet, die den Ordnungsbehörden im Einzelfall zur Erfüllung ihrer Aufgabe zustehen. Wie die Polizei sind sie jedoch an den Grundsatz der Verhältnismäßigkeit gebunden und müssen bei der Auswahl ihrer Mittel jenes wählen, das den Betroffenen am wenigsten beeinträchtigt (§ 14 Abs. 1 OBG). Die den Ordnungsbehörden zustehenden hoheitlichen Eingriffsbefugnisse gehen zudem nicht auf private Stellen wie Wachschutz oder den privaten Betreiber einer Asylbewerberunterkunft über, selbst wenn diese für eine Ordnungsbehörde tätig werden.

Auch das Brandenburgische Polizeigesetz bietet keine Rechtsgrundlage für die mit der Führung eines sog. "Besucherbuchs" verbundene Datenverarbeitung über Besucher in Asylbewerberunterkünften. Voraussetzung für eine Identitätsfeststellung gem. § 12 Abs. 1 Nr. 1 BbgPolG ist das Bestehen einer konkreten Gefahr, zu deren Abwehr es erforderlich ist, die Identität des Störers festzustellen. Dass diese Voraussetzung nicht in jedem Besuchsfall zutreffen kann, liegt auf der Hand, da nicht jeder Besucher einer Asylbewerberunterkunft ein "Störer" im Sinne des Polizeirechts ist. Aber auch die weiteren in der Vorschrift aufgeführten Voraus-

setzungen sind nicht erfüllt. Eine Asylbewerberunterkunft ist kein gefährlicher oder gefährdeter Ort im Sinne der Vorschrift. Es besteht somit weder eine generelle Verpflichtung der Besucher, sich auszuweisen oder einen Identitätsnachweis zu hinterlegen, noch müssen sie hinnehmen, dass ihre Identdaten sowie Zeitpunkt und Ziel ihres Besuches in einem sog. "Besucherbuch" über die Dauer ihres Aufenthalts in der Asylbewerberunterkunft hinaus aufbewahrt werden. Die Führung eines solchen Buches stellt einen unrechtmäßigen Eingriff in die Persönlichkeitsrechte der Besucher und der gastgebenden Asylbewerber dar.

Die Rechtmäßigkeit der Datenerhebung und -speicherung von Besuchern lässt sich nur im Rahmen der zulässigen Ausübung des dem Betreiber zustehenden Hausrechts beurteilen. Berücksichtigt werden muss hierbei auch der Anspruch der Asylbewerber, Besuche empfangen zu können, der sich aus ihrem Recht auf freie Entfaltung der Persönlichkeit ableitet, das nicht übermäßig eingeschränkt werden darf. Um die störungsfreie Funktionsfähigkeit des Betriebs der Asylbewerberunterkunft sicherzustellen, kann der Betreiber zu Recht verlangen, dass er weiß, wer sich in der Unterkunft aufhält und dazu die Namen der Besucher erfragen sowie für die Dauer des Besuchs notieren. Einer Ausweiskontrolle bedarf es dazu im Allgemeinen nicht. Es wäre daher ein unzulässiger Eingriff in die Persönlichkeitsrechte der Asylbewerber, einen Besucher nur deswegen abzuweisen, weil er sich nicht ausweisen kann oder will.

Wenn der Besucher die Unterkunft verlassen hat, ist der Speicherungsgrund entfallen und die Daten sind zu löschen. Weitere Informationseingriffe sind erst nach Eintritt einer konkreten Gefahr erforderlich und nur dann zulässig. Das gilt auch für die Aufbewahrung der Identdaten über den Zeitraum des Besuchs hinaus.

Schließlich kann die Führung eines Besucherbuchs auch nicht aus der Befugnis der Polizei hergeleitet werden, zur Gefahrenabwehr gem. § 45 Abs. 2 BbgPolG oder zur Strafverfolgung gem. §§ 161 oder 163 Strafprozessordnung (StPO) den Betreiber einer Asylbewerberunterkunft um Auskunft zu ersuchen. Dieser fungiert nicht als verlängerter Arm der Strafverfolgungsbehörden, daher dürfen Besucherbücher auch nicht deswegen geführt werden, weil sie Polizei bzw. Staatsanwaltschaft möglicherweise zur Erfüllung ihrer Aufgaben von Nutzen sein könnten. Eben so wenig kommen § 8 Abs. 3 Asylverfahrensgesetz oder gar die Heimordnung als Rechtsgrundlage in Betracht, auf die verschiedentlich verwiesen wurde. Die Vorschrift des Asylverfahrensgesetzes verpflichtet die Betreiber nur zur Übermittlung solcher Daten, die sie zu ihrer Aufgabenerfüllung in Ausführung des Asylverfahrensgesetzes rechtmäßig erhoben haben. Das Gesetz befasst sich nicht mit Datenerhebungen über Besucher.

Es hat sich herausgestellt, dass ungeachtet der fehlenden Rechtsgrundlage viele Landkreise Besucherbücher samt Ausweis- und Bescheinigungskontrolle aus den eingangs genannten Gründen beibehalten wollen. Allerdings gibt es mehrere Landkreise und kreisfreie Städte, die in ihren Unterkünften keine Besucherbücher führen lassen und nicht auf einer Ausweisvorlage bestehen, sondern höchstens Namen und Ziel der Besucher für die Dauer des Besuchs notieren. In einigen Fällen sind nach unserem Schreiben die Besucherbücher abgeschafft worden und z. T. durch Besucherkarten ersetzt worden, die nach Beendigung des Besuches vernichtet werden.

In Asylbewerberheimen ist die Kontrolle von Identitätsnachweisen ebenso wie eine Datenspeicherung über den Besuchszeitraum hinaus nur in Einzelfällen zur Abwehr einer konkreten Gefahr zulässig.

#### **4.3.2.2 Videoüberwachung**

*Viele Asylbewerberunterkünfte in Brandenburg werden zum Schutz vor Anschlägen mit Videokameras überwacht. Die Heimbewohner haben häufig das Gefühl, dass sie – und nicht potenzielle Angreifer – die Überwachten sind.*

Der Betreiber einer Asylbewerberunterkunft kann die Einrichtung zwar im Rahmen seines Hausrechts überwachen lassen. Allerdings sind dabei die Vorgaben des Bundes- bzw. des Brandenburgischen Datenschutzgesetzes zu beachten. Letzteres gilt für Heime in öffentlicher Trägerschaft, während für privat betriebene Heime das Bundesdatenschutzgesetz gilt. Beide Gesetze enthalten insoweit zwar keine identischen, aber doch gleich gerichtete Regelungen. Selbstverständlich darf die Überwachungsanlage nicht die Privatsphäre der Heimbewohner und Nachbarn der Einrichtung verletzen. Die Kameras müssen so angebracht und ein-gerichtet werden, dass die Fenster und Innenräume der Gebäude oder andere Grundstücke nicht eingesehen werden können. Weiterhin hat der Betreiber bei der Installation der Kameras darauf zu achten, dass nur der seinem Hausrecht unterliegende Bereich erfasst wird, weil die Befugnis zur Videoüberwachung öffentlicher Straßen und Plätze ausschließlich der Polizei zusteht. Als zu überwachender Raum bleibt somit nur der Bereich zwischen Grundstücksgrenze und Hausmauer. Daraus ergibt sich, dass die dort sich aufhaltenden Personen – in der überwiegenden Mehrzahl die Heimbewohner selbst – von der Videoüberwachung erfasst werden.

Die Beeinträchtigungen durch die Videoüberwachung lassen sich jedoch vermindern, wenn die Anlage nur in Zeiten höherer Gefährdungswahrscheinlichkeit – also in den Nachtstunden – in Betrieb genommen und insbesondere nur in diesem Zeitraum aufgezeichnet wird. Tagsüber dürfte es in vielen Asylbewerberunterkünften ausreichen, lediglich den Eingangsbereich durch die Kamera überwachen zu lassen und die Bilder nur auf einen Bildschirm in einem ständig besetzten Raum zu übertragen, statt sie aufzuzeichnen. Aufzeichnungen müssen gem. § 33c Abs. 1 Satz 3 BbgDSG bzw. § 6b Abs. 5 BDSG gelöscht werden, soweit sie nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen eine weitere Speicherung entgegenstehen. Sowohl das brandenburgische als auch das Bundesdatenschutzgesetz verlangen außerdem, dass für jeden deutlich sichtbar auf die Videoüberwachung hingewiesen wird, wenn auch aufgezeichnet werden soll.

Die Videoüberwachung von Asylbewerberunterkünften ist zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen entgegenstehen oder überwiegen. Der Betrieb der Überwachungsanlage muss an die örtlichen Gegebenheiten und die Gefährdungswahrscheinlichkeit angepasst werden. Durch ein geeignetes Verfahren hat der Betreiber sicherzustellen, dass Aufnahmen regelmäßig zeitnah gelöscht werden.

#### **4.3.3 Taschen- und Handykontrolle in der Ausländerbehörde**

*Die Mitarbeiter einer Ausländerbehörde haben die Taschen von Besuchern kontrolliert und dabei mitgeführte Unterlagen sowie Handys überprüft. Die Unterlagen sollen im Beisein der Betroffenen – jedoch ohne ihre Zustimmung – gesichtet und als Kopien zur Ausländerakte genommen sowie die auf den Handys eingespeicherten Telefonnummern überprüft worden sein. Erst danach seien den Betroffenen die Sachen wieder ausgehändigt worden. Dass sie die Handys überprüft habe, um mittels der dort gespeicherten Verbindungsnummern das Herkunftsland festzustellen, wird von der Ausländerbehörde bestritten.*

Mit Ausnahme der Kontrolle der Handys kann ein solches Vorgehen der Ausländerbehörden im Einzelfall zulässig sein, wenn der Verdacht besteht, dass ein Ausländer seine Identität verschleiert und die Ausländerbehörde Anhaltspunkte für die Annahme hat, dass er Dokumente oder Gegenstände mit sich führt, die Auskunft über seine Identität geben könnten.

Rechtsgrundlage ist § 15 Asylverfahrensgesetz (AsylVfG), der einen Ausländer verpflichtet, an der Feststellung seiner Identität und seines Herkunftslands mitzuwirken und den Ausländerbehörden dazu zum Nachweis seinen Pass oder Passersatz sowie alle erforderlichen Urkunden und sonstigen Unterlagen, die in seinem Besitz sind, auszuhändigen. Kommt er dem nicht nach, darf die Ausländerbehörde ihn durchsuchen, um Unterlagen, die seine Identifizierung ermöglichen, zu erlangen, wenn ihr Hinweise auf falsche Personalangaben vorliegen und Anhaltspunkte bestehen, der Betroffene sei in Besitz von Unterlagen über seine Identität.

Das Asylverfahrensgesetz bietet jedoch keine Rechtsgrundlage für eine Überprüfung des Handys oder der dort gespeicherten Verbindungsdaten. Letztere unterliegen dem durch Art. 10 Grundgesetz geschützten Fernmeldegeheimnis. Da der Artikel nicht im Katalog der durch das Gesetz eingeschränkten Grundrechte des § 89 AsylVfG enthalten ist, dürfen Handys bei der ansonsten zulässigen Durchsuchung auch dann nicht kontrolliert werden, wenn – wie eine Ausländerbehörde meinte – die auf einem Handy gespeicherten Ländervorwahlnummern von gewisser Bedeutung sein könnten, da sich daraus Rückschlüsse auf die wahrscheinliche Herkunft des Betroffenen ziehen ließen.

Ein Ausländer, der keine ihn identifizierenden Dokumente beibringt, muss es hinnehmen, wenn die zuständige Ausländerbehörde von ihrer gesetzlichen Befugnis Gebrauch macht und seine Taschen mit dem Ziel durchsucht, Nachweise über seine Identität oder sein Herkunftsland zu finden. Die Kontrolle seines Handys hingegen ist unzulässig.

#### **4.4 Meldewesen** **"Zentrales elektronisches Melderegister" (MDIS)**

*Das Ministerium des Innern plant, die regelmäßige Meldedatenübermittlung der einzelnen Meldebehörden an die Polizeipräsidien zu vereinheitlichen und zentral aufzubereiten. Dazu soll der Landesbetrieb für Datenverarbeitung und Statistik die aktualisierten Meldedaten regelmäßig von den Meldebehörden in Empfang nehmen und zum Abruf für die Polizei bereithalten.*

Durch das neue Verfahren "Zentrales elektronisches Melderegister" (MDIS), über das das Ministerium den Landesbeauftragten frühzeitig informiert hat, soll eine vereinfachte und damit effektivere Möglichkeit zur polizeilichen Aufgabenerfüllung geschaffen werden. Im täglichen Polizeihandeln müssen vielfach Meldedaten von Personen erhoben werden. Das vorgeschlagene Verfahren würde den unkomplizierten Zugriff der

Polizei auf die Meldedaten rund um die Uhr erlauben. Gleichzeitig wären die Meldebehörden von den wirtschaftlichen Belastungen eines Notdienstes zur Gewährleistung des Zugriffs der Polizei auf Meldedaten außerhalb der Dienstzeiten und der Einrichtung eines automatisierten Abrufsystems freigestellt.

In keinem Fall darf aber beim Landesbetrieb für Datenverarbeitung und Statistik dadurch ein zentrales Melderegister durch Zusammenführung der Meldedaten der einzelnen Meldebehörden entstehen. Die Datensätze der einzelnen Meldebehörden sind, obwohl sie an einem Ort verarbeitet werden, getrennt von einander zum Abruf bereitzuhalten.

Es ist zudem sicherzustellen, dass die Daten nur mittels gesicherter Verbindungen übertragen werden und bei der Identifizierung der abfragenden Stelle nur rechtlich autorisierte Personen Zugriff auf die Meldedaten der Bürger erhalten. Schließlich sind auch beim Landesbetrieb für Datenverarbeitung und Statistik, der die Datenbereitstellung im Auftrag der Polizeipräsidien vornimmt, technische Vorkehrungen nötig, die einen Zugriff unbefugter Dritter verhindern.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird das noch in der Entwicklungsphase befindliche Projekt "Zentrales Elektronisches Melderegister" intensiv begleiten, um sicherzustellen, dass das Ergebnis sowohl den datenschutzrechtlichen Interessen der Bürgerinnen und Bürger des Landes als auch den Belangen der Polizei gerecht wird.

## **4.5 Personaldaten**

### **4.5.1 Daten aller Landesbediensteten in eine zentrale Datenbank?**

*Einige Ministerien wollten aus Rationalisierungsgründen die Personaldaten ihrer Beschäftigten, die sie mit dem automatisierten Personalinformationssystem PERIS verarbeiten, auf einem zentralen Server im Brandenburgischen Landesbetrieb für Datenverarbeitung und Statistik (LDS) speichern.*

Grundsätzlich bestehen keine datenschutzrechtlichen Bedenken gegen eine Verarbeitung von Personaldaten im Auftrag durch eine andere öffentliche Stelle. Zu beachten ist jedoch, dass die Personaldatenverarbeitung mit dem System PERIS für die einzelnen Landesbehörden weiterhin getrennt erfolgen muss; ein einheitlicher Personaldaten-Pool darf nicht entstehen. Ferner müssen sich die datenschutzrechtlichen Anforderungen in den technischen und organisatorischen Sicherheitslösungen

widerspiegeln. Auch ist zu beachten, dass das neue Verarbeitungsverfahren der Personaldaten eine wesentliche Änderung des bisherigen darstellt und daher gem. § 65 Nr. 1 Landespersonalvertretungsgesetz einen Mitbestimmungstatbestand erfüllt.

Der LDS hatte ein IT-Sicherheitskonzept zum Einsatz von PERIS auf einer "Zentralanlage im LDS" vorgelegt. Dieses beinhaltet, dass die Personaldatenbestände der beteiligten Behörden in entsprechend vielen PERIS-Servern auf dem Zentralrechner gespeichert werden. Der einzelne PERIS-Server ist dabei nur über die für die jeweils zuständige Behörde definierte Portnummer des Zentralrechners ansprechbar. Die Fachadministration der einzelnen PERIS-Server obliegt weiterhin der jeweils zuständigen Behörde. Diese steuert wie bisher die Verschlüsselung ihrer Personaldatenbank (Serververschlüsselung) und die eigene Netzverschlüsselung.

Räumlich befindet sich der Zentralrechner in einem besonderen Sicherheitsbereich des LDS (Lampertz-Zelle mit integriertem Einbruchs- und Brandschutz). Die Datensicherung wird zentral im LDS durchgeführt; dabei werden die zu sichernden Daten mit PGP in der Version 2.6.3 verschlüsselt.

Auch wir sind der Ansicht, dass diese ausgewählte Verfahrensalternative grundsätzlich die datenschutzschutzfreundlichste ist. Sie lässt am ehesten erwarten, dass der Einsatz von PERIS auf einem Zentralrechner im LDS auch bei dem hohen Schutzbedarf der Personaldaten beherrschbar ist.

Allerdings sind datenschutzrechtlich aus technisch-organisatorischer Sicht noch einige wesentliche Einzelprobleme zu klären:

- *PERIS-Clients in den beteiligten Behörden*

Das IT-Sicherheitskonzept des LDS befasst sich im Wesentlichen mit der Sicherung des Zentralrechners für die PERIS-Server im LDS. Zur Absicherung der PERIS-Clients in den Behörden wird nur auf den unerlässlichen IT-Grundschutz hingewiesen. Auf notwendige Sicherheitskonzepte der beteiligten Behörden wird aufmerksam gemacht. Über die tatsächliche Existenz derartiger Konzepte, die die zentrale PERIS-Speicherung berücksichtigen, ist uns allerdings bisher nichts bekannt geworden. Aber auch diese Konzepte der beteiligten Behörden gehören zu den unverzichtbaren organisatorisch-technischen Voraussetzungen für eine gesicherte und verantwortbare zentrale PERIS-Speicherung im LDS.

– *Verschlüsselungsverfahren bei PERIS*

Zu den bei PERIS einzusetzenden Verschlüsselungsverfahren<sup>30</sup> weisen wir darauf hin, dass für die Leitungsübertragung das Hybridverfahren von PERIS mit einer Schlüssellänge von mindestens 1024 Bit für die RSA-Verschlüsselung und dem DES3 als Sitzungsschlüssel als Mindeststandard gilt. Hierbei ist auch zu beachten, dass nach Einschätzung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) ab 2006 RSA-Schlüssellängen von 2048 Bit erforderlich sein werden. Für die Serververschlüsselung sollte ebenfalls der DES3 genutzt werden. Bei der Netzverschlüsselung ist seitens der PERIS-Clients in den Behörden auf eine Kompletต์verschlüsselung der Datensätze zu achten, andernfalls wären Gefährdungen der Vertraulichkeit zu befürchten<sup>31</sup>. Dies müsste auch in den Sicherheitskonzepten der Behörden geregelt werden.

Üblich ist bisher, eine nur teilweise Verschlüsselung der PERIS-Datenbanken. Es sollte jedoch bedacht werden, dass es bei der PERIS-Datenbankverschlüsselung nicht nur um die Abschottung der Personaldaten gegenüber dem PERIS-Systemverwalter geht, sondern auch um deren Sicherung für den Fall, dass ein Einbruch in das LDS-Netz erfolgt. Aus diesem Grund halten wir auch die Kompletต์verschlüsselung der PERIS-Datenbanken für erforderlich. In den Sicherheitskonzepten der Behörden sollte zudem festgelegt werden, in welchen Zeitintervallen die PERIS-Datenbanken neu verschlüsselt werden. Dies trägt zur Sicherung der Vertraulichkeit bei. Wird an den PERIS-Clients Textverarbeitung eingesetzt, müssen diese jeweils mit lokalen Druckern ausgerüstet werden, weil Druckerdaten üblicherweise nicht verschlüsselt werden.

– *Verfügbarkeit der PERIS-Clients und des Zentralrechners im LDS*

Kommt es durch die Speicherung der PERIS-Datenbanken auf einem zentralen Rechner im LDS zu höheren Anforderungen an die Rechen-technik wegen der Datenverschlüsselung und der Häufigkeit der Zugriffe, ist es zumindest möglich, dass gelegentlich spürbare Performance-Probleme auftreten. Diese Verfügbarkeitsprobleme dürfen nicht auf Kosten der Sicherheit und der Vertraulichkeit der zu schützenden Personaldaten gelöst werden, indem man beispielsweise weniger stark oder nur noch eingeschränkt verschlüsselt. Abhilfe lässt sich z. B. dadurch schaffen, dass man Rechner mit stärkerer Rechenleistung und größerem Arbeitsspeicher anschafft. Notfalls ist auch an eine größere Bandbreite für die Übertragungsleitungen zu denken.

---

<sup>30</sup> s. dazu 6. Tätigkeitsbericht, 13.2.9

<sup>31</sup> siehe Tätigkeitsbericht 2001, A 4.4.6

Es bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die zentrale Speicherung der mit dem automatisierten Personalinformationssystem PERIS zu verarbeitenden Personaldaten der Landesbeschäftigten im LDS, wenn die Speicherung für jede Behörde getrennt erfolgt, und weitere technisch-organisatorische Sicherheitsmaßnahmen sowohl im LDS als auch in den Ministerien ergriffen werden.

#### **4.5.2 Chipkarten für die Polizei**

*Im Rahmen der Polizeistrukturereform beabsichtigte das Ministerium des Innern für Heilfürsorgeberechtigte der Polizei eine Chipkarte einzuführen, der den bisherigen Behandlungsschein ersetzen sollte. Darüber hinaus wurden an alle Polizeibediensteten Dienstausweise ausgereicht, die mit einem Datenchip ausgestattet waren.*

Die Einführung einer Chipkarte zur Verarbeitung personenbezogener Daten stellt nicht nur einen Medienwechsel im Rahmen einer ohnehin erlaubten Datenverarbeitung dar, sondern löst zusätzliche Risiken für die Betroffenen aus und bedarf deshalb unabhängig von § 5 Abs. 3 BbgDSG einer eigenständigen Rechtsgrundlage. Das ergibt sich auch aus der Begründung der Landesregierung zum Brandenburgischen Datenschutzgesetz. Nur eine Rechtsgrundlage in Form einer Rechtsverordnung nach § 9 Abs. 2 BbgDSG, die die Art und den Umfang der Datenverarbeitung beschreibt, kann für den Nutzer zur Rechtsklarheit beitragen und das datenschutzrechtliche Risiko begrenzen.

Das Ministerium des Innern hat uns daraufhin zugesagt, die Verordnung über die Heilfürsorge der Polizeivollzugsbeamten zu überarbeiten und die Verwendung von Chipkarten und den Umfang der auf dem Datenchip enthaltenen personenbezogenen Daten sowie deren Verwendung ausdrücklich zu regeln. Aus technisch-organisatorischer Sicht haben wir derzeit keine Bedenken, da bei der Herstellung und Nutzung der Beihilfechipkarten die technische Spezifikation zur Erstellung von Krankenversichertenkarten zur Anwendung kommt, die zwischen den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung vereinbart wurden. Diese technische Spezifikation wurde bereits im Jahr 1993 mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt.

Für den Einsatz von Datenchips auf den Dienstausweisen im Bereich der Polizei hat das Ministerium des Innern aufgrund unserer Empfehlung mittlerweile eine Rechtsverordnung geschaffen<sup>32</sup>. Die mit Umsetzung der

Polizeistrukturreform am 1. Juli 2002 verteilten neuen Dienstaussweise dienen zunächst ausschließlich der Legitimation des Ausweisinhabers. Der integrierte Datenchip soll aber kurzfristig als "Zugangsschlüssel" für den PC und später für eine Vielzahl weiterer Zwecke (z. B. Zugangsbe- rechtigung zu elektronisch gesicherten Räumen oder Gebäuden, Zugang zur elektronischen Zeiterfassung oder zum Bekleidungskonto) eingesetzt werden können. Diese multifunktionale Verwendung wird in der Rechts- verordnung nur allgemein umschrieben. Einzelheiten der künftigen Ver- wendung und zum Inhalt und Umfang der gespeicherten Daten werden aufgrund der Verordnung noch durch Verwaltungsvorschriften zu regeln sein. Diese Präzisierung des erforderlichen Rechtsrahmens durch einen Regelungsmix aus Rechtsverordnung und Verwaltungsvorschriften ver- bindet die gebotene Rechtsgrundlage für die verpflichtende Einführung eines mobilen Datenträgers mit der für die technische Entwicklung not- wendigen Flexibilität.

Die Verordnung des Innenministerium über den Einsatz von Datenchips auf den Dienstaussweisen im Bereich der Polizei könnte deshalb Modell- charakter für die gesamte Landesverwaltung haben. Denn auch die Ein- führung von Dienstaussweisen mit Datenchip in anderen Ministerien oder nachgeordneten Behörden bedarf einer vergleichbaren Rechtsgrundlage. Der Landesbeauftragte hatte deshalb angeregt, dass das Innenministe- rium eine (Muster-) Verordnung für die Dienstaussweise mit integriertem Prozessor für die gesamte Landesverwaltung erlässt.

Für den verpflichtenden Einsatz von Chipkarten bedarf es einer ent- sprechenden Ermächtigungsgrundlage. Die Rechtsverordnung über den Einsatz von Datenchips auf Dienstaussweisen der Polizei könnte Modellcharakter für die übrige Landesverwaltung haben.

#### **4.5.3 Leistungs- und Verhaltenskontrolle von Mitarbeitern**

*Ein Landesamt wollte mit einem EDV-Programm nicht nur den Be- arbeitern von Anträgen selbst, sondern auch deren Vorgesetzten einen Überblick über die Antragseingänge und den Bearbeitungs- stand sowie die Erledigungsmengen ermöglichen. Darüber hinaus sollte eine Analyse über die Qualität der Bescheide erstellt und evtl. Qualifizierungsbedarf ermittelt werden.*

Das EDV-Programm soll zum einen den Beschäftigten selbst dienen, in dem es ihnen einen Überblick über die eigene Vorgangsbearbeitung gibt, und so das eigenverantwortliche Arbeiten fördern. Darüber hinaus kann der unmittelbare Vorgesetzte nach § 29 Brandenburgisches Daten- schutzgesetz (BbgDSG) im Rahmen der Erforderlichkeit Leistungs- und

Verhaltenskontrollen durchführen. Eine jederzeitige, lückenlose Kontrolle ist dagegen mit dem Schutz der Persönlichkeit des Beschäftigten am Arbeitsplatz unvereinbar.

Um die beabsichtigte Analyse der Qualität und Quantität der Bescheide zu erstellen, ist ein abgestuftes Verfahren unter den Gesichtspunkten der Erforderlichkeit, der Datensparsamkeit und der Datenvermeidung datenschutzrechtlich geboten. Den personenbezogenen Zugriff auf die Leistungsdaten der Beschäftigten sollte nur der unmittelbare (Fach-) Vorgesetzte haben, weil er die konkrete Arbeitssituation seiner Mitarbeiter am besten beurteilen kann. Für die weiteren Vorgesetzten dürften in der Regel allgemeine Übersichten für die Qualitäts- bzw. Quantitätsanalyse genügen.

Soweit die Personalvertretung einer Verhaltens- und Leistungskontrolle im Rahmen ihrer Mitbestimmung zustimmt, sollte sie dafür Sorge tragen, dass konkrete Festlegungen für ein solches abgestuftes Verfahren getroffen werden und der Schutz der Persönlichkeit des Beschäftigten in keiner Weise gefährdet wird. Beispielsweise muss eine permanente Beobachtung des Beschäftigten ausgeschlossen sein. Ohne Zustimmung der Personalvertretung darf ein Verfahren, das die Verhaltens- und Leistungskontrolle ermöglicht, nicht eingeführt werden.

Darüber hinaus sind die Vorschriften des § 29 BbgDSG und § 64 Abs. 4 Landesbeamtengesetz zu beachten, nach denen Beurteilungen und personalrechtliche Entscheidungen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden dürfen, die unmittelbar durch die automatisierte Verarbeitung von personenbezogenen Daten gewonnen werden.

Soweit es erforderlich ist, kann der unmittelbare Vorgesetzte im Rahmen von § 29 Brandenburgisches Datenschutzgesetz Verhaltens- und Leistungskontrollen auch unter Einsatz eines ADV-Programms durchführen. Sie unterliegen der Mitbestimmung nach dem Personalvertretungsgesetz.

#### **4.5.4 Personalüberleitung bei Gemeindeneugliederung**

*Drei Gemeinden eines Amtes sollten (freiwillig) in eine Stadt eingegliedert werden. Dementsprechend erhielt die Stadt auch Personalstellen dieses Amtes. Es war zu klären, ob und in welchem Umfang bei Gemeindeneugliederungen Personaldaten übermittelt werden dürfen.*

Bei der Verhandlung, welche Beschäftigten übernommen und wie sie eingesetzt werden sollen, benötigte die Stadt für eine sachgerechte Entscheidung konkrete Personalangaben. Rechtsgrundlage für die Übermittlung von Personaldaten an die aufnehmende Körperschaft ist § 29 Brandenburgisches Datenschutzgesetz (BbgDSG). Danach dürfen Personaldaten im erforderlichen Umfang zu Zwecken der Personalplanung und des Personaleinsatzes verarbeitet werden. Dieser Zweck wird auch bei der Personalplanung im Rahmen einer Gemeindeneugliederung erfüllt.

Für die praktische Umsetzung bietet sich ein Stufenverfahren an. Im eigentlichen Gebietsänderungsvertrag nach § 9 Abs. 3 Gemeindeordnung (GO) sind gemäß § 10a Abs. 1 Satz 1 GO Regelungen zur Überleitung des Personals zu treffen. Da der Gebietsänderungsvertrag von den Gemeindevertretungen beschlossen wird und diese im Normalfall keine Detailkenntnisse hinsichtlich des Personals der Amtsverwaltung besitzen, können hier lediglich allgemeine Fragen der Personalüberleitung geklärt werden. Der Gebietsänderungsvertrag sollte daher nur die Anzahl – ggf. aufgeschlüsselt nach Laufbahngruppen – der zu übernehmenden Bediensteten enthalten.

Die Entscheidung, welche konkreten Personen übernommen werden, wird nicht in den Gemeindevertretungen, sondern in den jeweiligen Verwaltungen getroffen. Das Verfahren zur Überleitung kann im Rahmen der kommunalen Selbstverwaltung unter Beachtung des § 29 BbgDSG frei gewählt werden. Allerdings liegt es nahe, nach den Grundsätzen des § 4 des Funktionalreformgrundgesetzes zu verfahren. Dabei haben wir den beiden beteiligten Körperschaften geraten, Personalüberleitungskommissionen zu bilden.

Anhand des Stellenplanes ist zunächst zu ermitteln, welche Bediensteten von vornherein nicht für die Überleitung in Betracht kommen, sodass deren Personaldaten nicht übermittelt werden müssen. Von den Übrigen können die erforderlichen Personaldaten der Kommission zur Verfügung gestellt werden. Im Einzelnen können folgende Daten erforderlich sein:

- Alter
- Vergütungs-/Besoldungsgruppe einschl. Bewährungsaufstieg
- Tätigkeit
- Qualifikation und Fähigkeiten
- Vortätigkeiten.

Nicht relevant sind (zunächst) Namen, Wohnort, konkrete Geburtsdaten, Geschlecht und die familiäre Situation. In der letzten Stufe werden dann die konkreten Personen ausgewählt. Dabei können weitere Daten zur Sozialauswahl erheblich werden.

Eine Übermittlung von Personaldaten bei Personalüberleitung infolge Gemeindeneugliederung ist nach Maßgabe des § 29 Brandenburgisches Datenschutzgesetz grundsätzlich möglich. Dem strikten Erforderlichkeitsprinzip der Datenübermittlung trägt man Rechnung, indem ein Stufenverfahren mit genauen Auswahlkriterien durchgeführt wird.

#### 4.5.5 "Überleben" Personalratsunterlagen bei Privatisierung?

*Ein städtisches Krankenhaus ging in eine private Rechtsform über. Somit endete auch die Amtszeit des bisherigen Personalrates. Was geschieht nun mit den bei ihm gespeicherten personenbezogenen Daten der Mitarbeiter? Können sie dem neu gewählten Betriebsrat übergeben werden?*

Das Personalvertretungsrecht regelt diesen Fall nicht. Es enthält lediglich in der Wahlordnung zum Personalvertretungsgesetz eine Festlegung, dass die Wahlunterlagen nach Abschluss der nächsten Wahl zu vernichten sind. Nach § 94 Abs. 3 Personalvertretungsgesetz (PersVG) hat der Personalrat personenbezogene Daten grundsätzlich zu löschen, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Der bisherige Personalrat hat also in einem ersten Schritt zu prüfen, welche seiner Unterlagen weder für die Erfüllung seiner eigenen Aufgaben noch für die des künftigen Betriebsrats erforderlich sind. Diese Unterlagen müssen auf jeden Fall vernichtet werden.

Zu den Aufgaben des scheidenden Personalrates gehört es aber auch, die Amtsgeschäfte ordnungsgemäß an die neue Personalvertretung zu übergeben. Da es sich jedenfalls bei der Überführung in eine private Rechtsform beim Betriebsrat rechtlich um eine völlig neue Daten verarbeitende Stelle handelt, bedarf es zur Übergabe der vom Betriebsrat weiterhin benötigten Unterlagen einer Befugnis zur Übermittlung personenbezogener Daten. Soweit es um Daten der Beschäftigten geht, kommt als Rechtsgrundlage § 29 Abs. 1 Satz 2 Brandenburgisches Datenschutzgesetz (BbgDSG), für die übrigen Daten § 16 BbgDSG in Betracht, da der Betriebsrat in einem in privater Rechtsform geführtem Krankenhaus als nicht-öffentliche Stelle anzusehen ist.

§ 29 Abs. 1 Satz 2 BbgDSG lässt eine Übermittlung von Personaldaten an nicht-öffentliche Stellen u. a. dann zu, wenn der Dienstverkehr es erfordert. Soweit der Betriebsrat die Daten für seine weitere Aufgabenerfüllung benötigt, ist diese Voraussetzung gegeben. Bei sonstigen personenbezogenen Daten ist die Übermittlung nach § 16 Abs. 1 Buchst. a) BbgDSG zulässig, weil die ordnungsgemäße Übergabe zu den Aufgaben des Personalrats gehört und diese Daten für den gleichen Zweck weitergenutzt werden sollen, zu dem sie erhoben wurden. Hier ist dem Umstand Rechnung zu tragen, dass trotz Änderung der Rechtsform des Arbeitgebers alle Arbeitsverhältnisse unverändert erhalten bleiben. Die Arbeitnehmervertretung folgt in ihrem Wandel der Rechtsform nur der des Arbeitgebers. Ein Verbot der Weiterverarbeitung der Daten wäre eine unbillige Schwächung der Rechtsposition der Arbeitnehmervertretung.

Welche Daten konkret nach § 94 Abs. 3 PersVG zu vernichten sind und welche Daten nach §§16, 29 BbgDSG dem neuen Betriebsrat übergeben werden können, muss der Personalrat unter Berücksichtigung seiner Aufgaben und derer des künftigen Betriebsrates kritisch prüfen.

Soweit Personalratsunterlagen mit personenbezogenen Daten für die weitere Aufgabenerfüllung des neu gewählten Betriebsrates erforderlich sind, dürfen sie diesem übergeben werden; im Übrigen sind sie zu vernichten.

## **4.6 Statistik und Wahlen**

### **4.6.1 Melderegisterabgleich per Videokamera?**

*Ein Bürger beschwerte sich darüber, dass im Rahmen der Vorbereitung einer melderegistergestützten Volkszählung die Briefkästen der Hausbewohner mit einer Videokamera gefilmt wurden.*

Im Rahmen des Zensusgesetzes sind Überprüfungen der Melderegister auf Über- und Untererfassungen vorgesehen. Hintergrund ist die Absicht, bei künftigen Volkszählungen auf die direkte Befragung der Bürgerinnen und Bürger zu verzichten und statt dessen auf bereits vorhandene Daten der Verwaltung zurückzugreifen, wenn der bundesweite Zensus zu einem positiven Ergebnis führt. Um Klarheit über die Aussagekraft dieser Daten zu erlangen, sieht das Zensusgesetz vor, dass die Einwohnermelderegister stichprobenweise sowohl bei den Meldebehörden als auch durch Erhebungsbeauftragte bei den Bürgerinnen und Bürgern überprüft werden. Dem Erhebungsbeauftragten werden nur die ausgewählten Gebäude, nicht aber die Daten der Bewohnerinnen und Bewohner mitgeteilt. Der Abgleich zwischen den vor-

handenen Registerdaten und den Informationen der Vor-Ort-Begehung erfolgt durch den Landesbetrieb für Datenverarbeitung und Statistik. Rückmeldungen an die Melderegister dürfen nicht stattfinden.

Das Zensusgesetz sieht in § 14 lediglich eine mündliche oder schriftliche Erhebung vor, nicht aber den Einsatz von Videokameras. Auch nach § 11a Bundesstatistikgesetz sind lediglich noch computergestützte Erhebungsverfahren, also beispielsweise die Verwendung von Laptops oder Notebooks, zulässig. Der Landesbetrieb für Datenverarbeitung und Statistik, den wir über diesen Vorfall informierten, hat daraufhin den Einsatz von Videokameras untersagt.

Der Einsatz von Videokameras bei der Datenerhebung für statistische Zwecke ist unzulässig.

#### 4.6.2 Briefwahanträge per Internet

*Seit der Änderung der Bundeswahlordnung im Februar 2002<sup>33</sup> ist es möglich, den Wahlschein zur Briefwahl elektronisch zu beantragen. Rechtzeitig zur Bundestagswahl am 22. September 2002 konnte dies über das Internetangebot des Landesbetriebes für Datenverarbeitung und Statistik realisiert werden.*

Wer einen Wahlschein elektronisch beantragen wollte, musste das entsprechende Formular herunterladen, um es dann ausgefüllt per E-Mail an die zuständige Gemeinde zu senden. Der Antragsteller wurde darauf hingewiesen, dass die angegebenen Daten über E-Mail unverschlüsselt übermittelt werden. Da die Briefwahl nach der Rechtsprechung des Bundesverfassungsgerichts und den entsprechenden gesetzlichen Vorgaben nur zulässig ist, wenn der Wahlberechtigte aus wichtigem Grund daran gehindert ist, persönlich im Wahllokal abzustimmen, stellt sich die Frage, ob der Wahlberechtigte den wichtigen (seine Privatsphäre, z. B. seinen Gesundheitszustand betreffenden) Grund unverschlüsselt über das Internet mitteilen soll. In Brandenburg ist darauf verzichtet worden. Das Formular war allerdings so gestaltet, dass keine sensitiven personenbezogenen Daten übermittelt wurden. Datenschutzfreundlich war auch der Hinweis auf die Freiwilligkeit der Angaben zu Geburtsdatum, Wahlbezirksnummer, Wählerverzeichnisnummer und E-Mail im Formular. Neben der elektronischen Versendung konnte der Wahlscheinantrag auch ausgedruckt und per Post verschickt werden.

In Anbetracht der stetig steigenden Anzahl von Briefwählern ist die Einführung der Wahlscheinbeantragung per Internet zu begrüßen und deren Umsetzung in Brandenburg als datenschutzgerecht einzustufen.

## 4.7 Kommunalrecht

### 4.7.1 Nicht-öffentliche Sitzungen von Gemeindevertretungen

*Wir stellen häufig Unsicherheiten beim Umgang mit personenbezogenen Daten im Zusammenhang mit nicht-öffentlichen Sitzungen von Gemeindevertretungen, Kreistagen oder Amtsausschüssen fest. In einem Fall beabsichtigte eine Gemeindevertretung die Behandlung persönlicher Themen einzelner Bürgerinnen und Bürger im nicht-öffentlichen Teil der Sitzung. Dabei wurden die Namen der Bürgerinnen und Bürger in der öffentlich bekannt gemachten Tagesordnung genannt. In anderen Fällen war zu klären, wie mit Niederschriften oder sonstigen Unterlagen aus nicht-öffentlichen Sitzungen umzugehen ist.*

Im ersten geschilderten Fall ist die Nennung der Namen in der öffentlichen Bekanntmachung der Tagesordnung nicht datenschutzgerecht. Die öffentliche Bekanntmachung führt zu einer Übermittlung personenbezogener Daten an Stellen oder Personen außerhalb des öffentlichen Bereichs im Sinne von § 16 Brandenburgisches Datenschutzgesetz (BbgDSG), da der Empfängerkreis potenziell unbegrenzt ist. Diese ist nur dann zulässig, wenn eine Rechtsvorschrift sie erlaubt oder eine Einwilligung vorliegt.

Als eine solche Rechtsvorschrift ist § 42 Abs. 4 der Gemeindeordnung (GO) anzusehen, wonach u. a. die Tagesordnung der Sitzung entsprechend den Festlegungen in der Hauptsatzung öffentlich bekannt zu machen ist.

Soweit der öffentliche Teil der Sitzung betroffen ist, können nach dieser Rechtsvorschrift auch personenbezogene Daten mit der Tagesordnung veröffentlicht werden. In diesen Fällen besteht in der Regel kein Interesse der betroffenen Personen, nicht genannt zu werden, da an der öffentlichen Sitzung ohnehin jeder teilnehmen kann und die Beschlüsse wiederum öffentlich bekannt gemacht werden.

Anders verhält sich dies beim nicht-öffentlichen Teil der Sitzung. Wird die Öffentlichkeit nach § 44 Satz 2 GO gerade deshalb ausgeschlossen, weil berechtigte Interessen Einzelner es erfordern, so würde es den Sinn dieser Vorschrift in das Gegenteil verkehren, wenn die personenbezo-

genen Daten dieser Einzelnen teilweise bereits bei der öffentlichen Bekanntmachung der Tagesordnung der Öffentlichkeit zur Kenntnis gelangen. Deshalb ist bei der Einladung zum nicht-öffentlichen Teil der Sitzung darauf zu achten, dass personenbezogene Daten nicht Bestandteil der öffentlichen Bekanntmachung werden. § 42 Abs. 4 GO verlangt lediglich, dass "die Tagesordnung" öffentlich bekannt gemacht wird. Dieses Erfordernis lässt sich in der Regel ohne konkreten Personenbezug erfüllen. Ausreichend sind Bezeichnungen der Tagesordnungspunkte wie z. B. "Personalangelegenheiten" oder "Grundstücksangelegenheiten".

Im zweiten Fall ist häufig unklar, ob Niederschriften oder andere Unterlagen aus dem nicht-öffentlichen Teil der Sitzung den Gemeindevertretern oder Mitgliedern des Amtsausschusses oder des Kreistages in Kopie zur Verfügung gestellt werden können.

Zum Umgang mit Niederschriften aus Sitzungen der Kommunalvertretungen enthält die Brandenburgische Kommunalverfassung nur sehr fragmentarische Regelungen. § 49 Abs. 3 Satz 2 GO und § 43 Abs. 3 Satz 2 Landkreisordnung (LKrO) bestimmen lediglich, dass die Niederschrift spätestens zur nächsten Sitzung vorliegen muss. Die Gemeindeordnung bzw. die Landkreisordnung treffen weder für öffentliche noch für nicht-öffentliche Sitzungen eine Aussage darüber, inwieweit die Gemeindevertreter bzw. Kreistagsabgeordneten einen Anspruch haben, eine Kopie der Niederschrift zu erhalten. Es spricht aus unserer Sicht jedoch nichts dagegen, jedem Gemeindevertreter bzw. Kreistagsabgeordneten eine Ausfertigung der Niederschrift zuzuleiten. Gerade in den Randgebieten Brandenburgs sind die räumlichen Entfernungen zum Verwaltungssitz sehr groß, sodass es kaum zuzumuten ist, die Kommunalvertreter auf eine Akteneinsicht zu beschränken, um die Niederschrift auf das Erfordernis von Einwänden hin zu überprüfen. Ebenso wenig ist es praktikabel, die Niederschriften aus nicht-öffentlichen Sitzungen erst in der nächsten Sitzung als Tischvorlage vorzulesen. Eine Abschrift bzw. Ausfertigung der Niederschrift sowohl des öffentlichen als auch des nicht-öffentlichen Teils kann den Vertretern daher kaum verwehrt werden.

Soweit in den Unterlagen auch personenbezogene Daten enthalten sind, bestehen dagegen auch keine datenschutzrechtlichen Bedenken. Es handelt sich dabei um personenbezogene Daten, die zur Erfüllung der Aufgaben der jeweiligen Kommunalvertretung erforderlich sind und zu diesem Zweck durch die Mitglieder der Kommunalvertretung auch weiter verarbeitet werden dürfen. Eine Zweckänderung ist hier nicht gegeben.

In Abhängigkeit von der Sensitivität der personenbezogenen Daten sind die jeweils angemessenen technischen und organisatorischen Maßnahmen zu treffen. Dabei sollten die Unterlagen entsprechend gekennzeichnet werden. Außerdem kann die Vertretung festlegen, dass sensitivere Informationen erst innerhalb einer bestimmten Frist vor der nächsten Sitzung versandt werden und nach der Sitzung wieder zu vernichten sind. Bei Unterlagen, die der Vorbereitung von Beschlüssen in nicht-öffentlicher Sitzung dienen, kann die Sensitivität der personenbezogenen Daten im Einzelfall so hoch sein, dass nur eine Einsichtnahme am Verwaltungssitz bzw. das Verteilen von Tischvorlagen in Frage kommt. Dies wäre etwa bei bestimmten Personaldaten denkbar.

Generell sind die Gemeindevertreter auf ihre Verschwiegenheitspflichten nach § 27 GO hinzuweisen, die nach § 16 Abs. 1 Amtsordnung und § 24 Abs. 1 Satz 3 LKrO auch für die Mitglieder des Amtsausschusses und für die Kreistagsabgeordneten gilt.

In diesem Zusammenhang bekräftigt der Landesbeauftragte seine Empfehlung, die Kommunalverfassung um bereichsspezifische Regelungen zum Datenschutz zu ergänzen, wie auch seine Bereitschaft, das Ministerium des Innern dabei zu beraten<sup>34</sup>. Dieses hatte zwar im Innenausschuss des Landtages bereits vor geraumer Zeit zugesichert, eine entsprechende Gesetzesnovelle vorzulegen, ohne dass dies bisher in die Tat umgesetzt worden wäre.

Die öffentliche Bekanntmachung der Tagesordnung muss für den nicht-öffentlichen Teil der Sitzung ohne Personenbezug erfolgen. Mitglieder der kommunalen Vertretungen haben grundsätzlich das Recht, auch Ausfertigungen oder Kopien von Niederschriften oder anderen Unterlagen aus nicht-öffentlichen Sitzungen zu erhalten. Die Kommunalverfassung sollte um spezifische Datenschutzregelungen ergänzt werden.

#### **4.7.2 Elektromog und Datenschutz – Kataster über Mobilfunkantennen**

*Immer mehr Gemeinden gehen dazu über, die Standorte von Mobilfunkantennen zu erheben und in einem Kataster festzulegen. In der Regel werden dabei Straße, Hausnummer, Netzbetreiber und Anbringungsart der Sendeanlage gespeichert. Dies wirft sowohl Fragen des Datenschutzes als auch des Informationszugangs auf.*

Die Gemeinden erhalten die genannten Daten aufgrund von Vereinbarungen mit den kommunalen Spitzenverbänden zum Teil von den Mobilfunknetzbetreibern selbst. Darüber hinaus besteht für die Gemeinden die Möglichkeit, diese Daten aus der Standortdatenbank der Regulierungsbehörde für Telekommunikation und Post abzurufen. Aus datenschutzrechtlicher Sicht war dabei zu klären, ob die Gemeinden befugt sind, diese Daten zu erheben und zu speichern. Daran schloss sich die zusätzliche Frage an, ob und in welchem Umfang ein Zugang zu den bei den Gemeinden gespeicherten Informationen besteht.

Die Angaben zu Straße und Hausnummer können ohne erheblichen Aufwand der Person des betroffenen Grundstückseigentümers zugeordnet werden. Soweit die Eigentümer natürliche Personen sind, handelt es sich deshalb um personenbezogene Daten im Sinne des Brandenburgischen Datenschutzgesetzes (BbgDSG). Die Gemeinden dürften diese Daten erheben und speichern, wenn sie zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich wären.

Eine solche Aufgabe der Gemeinden ist nicht ohne Weiteres erkennbar. Nach der 26. Bundesimmissionsschutzverordnung müssen die Mobilfunknetzbetreiber den Betrieb von Sendeanlagen bei den Ämtern für Immissionsschutz anzeigen. Eine Mitwirkung der Gemeinden ist im Immissionsschutzrecht nicht vorgesehen. Auch nach der Brandenburgischen Bauordnung sind nur Sendeanlagen genehmigungspflichtig, die eine bestimmte Höhe überschreiten, sodass zumindest ein flächendeckendes Kataster auch auf dieser Basis nicht angelegt werden kann. Schließlich können sich die Gemeinden auch nicht auf die o. g. Vereinbarung mit den Mobilfunknetzbetreibern stützen, da eine solche Vereinbarung weder eine kommunale Zuständigkeit begründen noch eine Befugnis zur Erhebung personenbezogener Daten schaffen kann.

Andererseits ist zu berücksichtigen, dass die Gemeinden angesichts der Diskussion um gesundheitliche Gefahren durch die Strahlenbelastung ein erhebliches Interesse gerade daran haben, die konkreten Standorte von Mobilfunkantennen zu kennen, um dies beispielsweise bei der eigenen Bauleitplanung zu berücksichtigen. Zudem ist der mit der Erhebung und Speicherung der Standortdaten verbundene Eingriff in das Recht auf informationelle Selbstbestimmung der Grundstückseigentümer vor allem bei offen sichtbaren Anlagen gering, zumal den Eigentümern die Umweltrelevanz der Anlagen bewusst ist und sie daraus wirtschaftliche Vorteile erzielen.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 64. Konferenz in Trier eine EntschlieÙung verabschiedet, in der sie den Bundesgesetzgeber auffordern, eine eindeutige Rechtsgrundlage zur

Erstellung von Mobilfunkkatastern im Immissionsschutzrecht zu schaffen.<sup>35</sup> Das Ministerium für Landwirtschaft, Umweltschutz und Raumordnung unterstützt diesen Vorschlag und hat sich damit an das Bundesumweltministerium gewandt.

Unabhängig davon muss die Frage nach dem Zugang zu diesen Informationen beurteilt werden. Soweit die Gemeinden diese Daten als Behörden speichern, die Aufgaben des Umweltschutzes wahrzunehmen haben, besteht ein Anspruch auf Zugang zu diesen Informationen nach dem Umweltinformationsgesetz (UIG). Soweit jemand den genauen Standort wissen will und der Grundstückseigentümer eine natürliche Person ist, muss das Informationsinteresse nach § 8 UIG mit den schutzwürdigen Interessen des Betroffenen abgewogen werden. Soweit die Anlagen offen sichtbar angebracht sind, bestehen keine schutzwürdigen Interessen des Eigentümers, da es sich um allgemein zugängliche Informationen handelt. Bei verdeckt angebrachten Anlagen wird das Interesse am Informationszugang wegen des nur geringen Eingriffs in die Persönlichkeitsrechte des Eigentümers in der Regel überwiegen; der Eigentümer ist dazu vorher anzuhören. Die Ämter für Immissionsschutz müssen den Zugang zu diesen Informationen in gleicher Weise gewähren wie die Gemeinden.

Der Anspruch auf Informationszugang nach dem Umweltinformationsgesetz bezieht sich auch auf den Namen des Netzbetreibers, da es sich hierbei nicht um Betriebs- und Geschäftsgeheimnisse handelt.

Für die Erstellung von Mobilfunkkatastern existiert derzeit keine eindeutige Rechtsgrundlage, während der Zugang zu diesen Informationen bereits nach geltendem Recht nach dem Umweltinformationsgesetz möglich ist. Wir bitten die Landesregierung, die Schaffung einer eindeutigen Rechtsgrundlage für die Erstellung von Mobilfunkkatastern weiterhin zu unterstützen.

#### **4.7.3 Videüberwachung auch von Mülltonnen?**

*Ein Landkreis ärgerte sich darüber, dass sich in den von ihm aufgestellten Wertstoffcontainern (Gelbe Tonne bzw. Papier- und Glascontainer) statt des vorgesehenen Inhalts größere Mengen gewöhnlichen Hausmülls befanden. Er entschloss sich deshalb dazu, die öffentlichen Stellplätze für die Wertstoffcontainer mit versteckt angebrachten Videokameras zu beobachten und aufzuzeichnen.*

Die Videoüberwachung durch öffentliche Stellen ist nur unter den Voraussetzungen von § 33c Brandenburgisches Datenschutzgesetz (BbgDSG) zulässig. Danach können öffentlich zugängliche Räume mit Videokameras überwacht werden, wenn dies zur Erfüllung ihrer Aufgaben oder zur Wahrung des Hausrechts erforderlich ist.

Die vom Landkreis überwachten Containerstellplätze befinden sich auf öffentlichem Straßenland. Dabei handelt es sich nicht um einen öffentlich zugänglichen Raum. Ein Raum im Sinne der Vorschrift ist ein von der Umwelt abgegrenzter Bereich, an dem der Landkreis ein Hausrecht haben müsste. Das heißt nicht unbedingt, dass ein Zaun oder ein Dach vorhanden sein müssen. Wichtig ist, dass die Abgrenzung für jedermann eindeutig erkennbar ist.<sup>36</sup>

In diesem Fall gerieten dagegen Bereiche ins Blickfeld der Kamera, die als öffentliche Straße dem Gemeingebrauch gewidmet sind, sodass von einem "Raum" keine Rede mehr sein konnte. Deshalb bestand hier auch kein Hausrecht des Landkreises. Die Videoüberwachung konnte daher nicht auf § 33c BbgDSG gestützt werden.

Öffentlich zugängliche Straßen und Plätze können nur unter den Voraussetzungen des § 31 Abs. 3 des Brandenburgischen Polizeigesetzes von der Polizei videoüberwacht werden. Diese Regelung geht als speziellere Vorschrift dem § 33c BbgDSG vor.

Eine Videoüberwachung von Wertstoffcontainern könnte nur dann auf § 33c BbgDSG gestützt werden, wenn die Container an Orten abgestellt würden, die kein öffentliches Straßenland sind. Der Landkreis hat aufgrund unseres Hinweises die Videoüberwachung der Containerstellplätze eingestellt.

Die Befugnis des Landkreises, zur Ermittlung von Ordnungswidrigkeiten nach dem Abfallrecht im Einzelfall Videokameras einzusetzen, bleibt unberührt.

Eine Videoüberwachung von auf öffentlichem Straßenland eingerichteten Stellplätzen für Wertstoffcontainer ist unzulässig.

## 4.8 Sonstiges/Verwaltungsrecht

### 4.8.1 Der unabhängige Datenschutzbeauftragte

*Die Funktion des behördlichen Datenschutzbeauftragten wird Bediensteten häufig als Zusatzaufgabe zu den normalen Dienstaufgaben aufgetragen. Neben dem Problem, welchen Personen man diese Aufgabe ohne Interessenkollisionen übertragen kann, stellt sich auch die Frage nach ihrer dienstrechtlichen Stellung. Eine kreisfreie Stadt erwog im Zuge der notwendigen Aufgabenkritik, die Stelle des behördlichen Datenschutzbeauftragten zu halbieren.*

Die Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten im Land Brandenburg ergibt sich aus § 7a Brandenburgisches Datenschutzgesetz (BbgDSG).

Die Person, die diese Funktion ausübt, sollte möglichst im Leitungsbereich angesiedelt sein. In jedem Fall muss sie sich jederzeit unmittelbar an die Leitung wenden können. Bei der Erfüllung ihrer Aufgabe unterliegt sie lediglich der Dienstaufsicht, im Übrigen ist sie weisungsfrei und unterliegt keinerlei Fachaufsicht. Eine Kontrolle ihrer Sachvorgänge durch Dienstvorgesetzte hat auch im Hinblick auf die Pflicht zur Verschwiegenheit über die Identität von Personen, die sich an den behördlichen Datenschutzbeauftragten wenden, in aller Regel zu unterbleiben. Das Verbot einer Benachteiligung wegen der Tätigkeit als behördlicher Datenschutzbeauftragter ist explizit in § 7a Abs. 2 BbgDSG festgeschrieben. Wendet sich jemand in seiner Funktion als behördlicher Datenschutzbeauftragter an den Brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, muss zudem kein interner Dienstweg eingehalten werden. Auch die Dienststellenleitung muss hierüber nicht ausdrücklich informiert werden. Vielmehr besteht das Recht auf direkten Zugang zum Landesbeauftragten, das im Übrigen nach § 21 BbgDSG auch allen anderen Landesbediensteten zusteht. Aus den gesetzlichen Grundlagen wird deutlich, dass die Ausübung der Funktion eines behördlichen Datenschutzbeauftragten nicht nur "nebenbei" erfolgen darf. Die hervorgehobene Stellung verlangt, dass die betreffende Person wirklich unabhängig und weisungsfrei handeln kann. Zumindest in größeren Verwaltungen sollte der behördliche Datenschutzbeauftragte deshalb, um mögliche Interessenkonflikte zu vermeiden, nur hauptamtlich tätig sein. Kleinere Verwaltungseinheiten – insbesondere Gemeinden – können nach § 7a Abs. 3 BbgDSG einen gemeinsamen behördlichen Datenschutzbeauftragten bestellen, dem seinerseits aber wiederum der unmittelbare Kontakt zu den jeweiligen Dienststellenleitungen und eine unabhängige Position eingeräumt werden muss.

Angesichts der schwierigen Finanzlage der Kommunen sind Überlegungen zur Aufgabenkritik unausweichlich. Sie dürfen aber nicht dazu führen, dass der Stellenumfang des behördlichen Datenschutzbeauftragten derart beschnitten wird, dass er nicht mehr wirksam zur Wahrung des Grundrechts auf Datenschutz in seiner Verwaltung beitragen kann.

Besonders ist darauf hinzuweisen, dass ausschließlich die Daten verarbeitende Stelle selbst – und damit deren Leitung – für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist und es auch dann bleibt, wenn sie einen behördlichen Datenschutzbeauftragten bestellt hat. Dieser soll lediglich innerhalb der Dienststelle auf die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und zur Datensicherheit hinwirken und die Dienststellenleitung auf Missstände hinweisen sowie auf deren Beseitigung dringen.

Die Funktion des behördlichen Datenschutzbeauftragten muss unabhängig ausgeübt werden können und unterliegt keinerlei fachlichen Weisungen der Dienststelle. Um Interessenkonflikte zu vermeiden, sollte sie jedenfalls in größeren Verwaltungen durch hauptamtlich mit dieser Aufgabe betraute Personen ausgeübt werden.

#### **4.8.2 Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz**

*Drei Jahre nach In-Kraft-Treten des novellierten Brandenburgischen Datenschutzgesetzes hat uns das Ministerium des Innern den Entwurf einer neuen Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz zur Stellungnahme vorgelegt.*

Die inzwischen in Kraft getretene Verwaltungsvorschrift<sup>37</sup> hat das Ziel, die oftmals sehr abstrakten Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) näher zu erläutern und das Gesetz damit für die Anwender in den öffentlichen Stellen des Landes in der Praxis leichter handhabbar zu machen. Sie erläutert insbesondere neu in das Gesetz aufgenommene Regelungen wie z. B. die Vorschriften zur Verarbeitung besonders sensibler Daten (§ 4a BbgDSG), zum behördlichen Datenschutzbeauftragten (§ 7a BbgDSG), zum Systemdatenschutz (§§ 11b, 11c BbgDSG), zur Übermittlung personenbezogener Daten an ausländische und internationale Stellen innerhalb oder außerhalb der Europäischen Union (§§ 17, 17a BbgDSG) und zur Videoüberwachung (§ 33c BbgDSG).

<sup>37</sup>

ABI. Nr. 7 vom 19.2.2003, S. 170

Bedauerlich ist aus unserer Sicht, dass die Verwaltungsvorschrift ihrem Anspruch, eine Anwendungshilfe gerade auch im nachgeordneten und kommunalen Bereich zu sein, nur zum Teil gerecht wird. An einigen Stellen finden sich lediglich Umformulierungen des Gesetzeswortlauts. Diesem Mangel konnte im Laufe der Beratungen an vielen Stellen abgeholfen werden.

Zwar hat das Ministerium des Innern unsere Anregung, in der Verwaltungsvorschrift auch die Rechte der Betroffenen sowie die besonderen Vorschriften zur Datenverarbeitung für wissenschaftliche Zwecke und bei Dienst- und Arbeitsverhältnissen zu erläutern, nicht aufgegriffen, unsere übrigen Empfehlungen jedoch überwiegend umgesetzt.

Die Verwaltung sollte sich allerdings in Zukunft nicht darauf beschränken, die Verwaltungsvorschrift anzuwenden, sondern immer auch den allein maßgeblichen Text des Datenschutzgesetzes berücksichtigen.

Eine Verwaltungsvorschrift kann die Umsetzung des Brandenburgischen Datenschutzgesetzes in der Praxis erleichtern. Maßgebend für Bürger und Verwaltung bleibt aber der Gesetzestext.
--

## **5 Justiz und Europaangelegenheiten**

### **5.1 Datenschutz im Strafvollzug**

*Immer wieder beschäftigen uns Einzelanfragen von Häftlingen, aber auch Bediensteten zum Datenschutz und dem Akteneinsichtsrecht in den Justizvollzugsanstalten. Wir nahmen dies zum Anlass, unabhängig von konkreten Anlässen verschiedene Justizvollzugsanstalten und den dortigen Umgang mit personenbezogenen Daten zu überprüfen. Die Prüfungen sind noch nicht abgeschlossen und werden auch im kommenden Jahr an verschiedenen Orten fortgeführt.*

#### **5.1.1 Rechtliche Grundlagen und ihre Umsetzung**

Wie bei allen öffentlichen Stellen des Landes Brandenburg gehören auch in einer Justizvollzugsanstalt Datenschutz und Akteneinsicht zu den alltäglichen Aufgaben.

Rechtsgrundlage für die Durchführung und Organisation der Haft ist das Strafvollzugsgesetz (StVollzG) des Bundes, dessen spezielle Regelungen zum Umgang mit personenbezogenen Daten dem Brandenburgi-

schen Datenschutzgesetz (BbgDSG) vorgehen. Die §§ 179 ff StVollzG regeln in einem besonderen Abschnitt des Gesetzes die Bedingungen, unter denen diese Daten verarbeitet werden dürfen. Ergänzt werden diese Bestimmungen beispielsweise durch Vorschriften zur Postkontrolle oder zur Vornahme erkennungsdienstlicher Maßnahmen.

Eine im Oktober 2002 in Kraft getretene Änderung des Strafvollzugsgesetzes<sup>38</sup> sieht erstmals vor, dass von allen Gefangenen Lichtbilder aufgenommen werden dürfen, die nur von Justizbediensteten genutzt und für die Fahndung nach entwichenen Gefangenen an Strafverfolgungsbehörden übermittelt werden dürfen. Sie sind nach der Entlassung oder Verlegung der Betroffenen in eine andere Anstalt zu vernichten oder zu löschen. Damit ist eine normenklare Rechtsgrundlage für eine Praxis geschaffen worden, die schon seit Jahren in den Justizvollzugsanstalten des Landes üblich war.<sup>39</sup>

Nach einer ersten stichprobenartigen Überprüfung einzelner Gefangenenpersonalakten und der aus den Geschäftsverteilungsplänen ersichtlichen Zugriffsrechte ist festzustellen, dass in den bisher überprüften Justizvollzugsanstalten ein durchaus verantwortungsbewusster Umgang mit den Akten zu beobachten ist.

Auch die im Strafvollzugsgesetz vorgeschriebene Belehrung, mit der die Gefangenen darüber aufgeklärt werden, wie mit ihren personenbezogenen Daten im Rahmen des Strafvollzugs umgegangen wird, ist in einer Vollzugsanstalt aufgrund unserer Empfehlungen in datenschutzgerechter Weise präzisiert worden.

Ein Ausdruck dafür, dass datenschutzrechtlichen Problemen zunehmend Beachtung geschenkt wird, ist in diesem Zusammenhang der Umstand, dass die meisten der Justizvollzugsanstalten nunmehr ihrer Pflicht, behördliche Datenschutzbeauftragte zu bestellen, nachkommen. Im Berichtszeitraum gab es auch die Gelegenheit zu einer ersten datenschutzrechtlichen Schulung, die von Mitarbeitern des Landesbeauftragten durch Vorträge unterstützt werden konnte. Es bleibt zu hoffen, dass es gelingt, durch die Zusammenarbeit der verschiedenen behördlichen Datenschutzbeauftragten zu einer für das ganze Land Brandenburg einheitlichen Verfahrensweise bei der Führung von Akten und der Behandlung von datenschutzrechtlichen Problemen zu gelangen, was insbesondere bei der Verlegung von Insassen in andere Vollzugsanstalten von Vorteil wäre. Problematisch ist wie bei anderen Stellen (s. o. Punkt A 4.8.1.), dass die hierarchische Einordnung der behördlichen Daten-

---

<sup>38</sup> 6. Gesetz zur Änderung des StVollzG vom 5.10.2002, BGBl. I S. 3954

<sup>39</sup> 3. Tätigkeitsbericht (1994/95), 4.3.2

schutzbeauftragten und ihre Befugnisse intern noch nicht überall klar geregelt sind.

Unsicherheiten zeigen sich auch bei der Behandlung von Fragen zur Akteneinsicht in die Gefangenenpersonalakten durch die Gefangenen selbst. § 185 StVollzG gewährt für den Regelfall lediglich ein Auskunftsrecht. Ein Einsichtsrecht besteht für die Betroffenen erst dann, wenn sie im Einzelfall darlegen, dass sie zur Wahrnehmung ihrer rechtlichen Interessen darauf angewiesen sind, neben der bloßen Auskunft auch die Einsicht in die Akte zu erhalten. Generell sollten allerdings an die Darlegungserfordernisse keine besonders hohen Ansprüche gestellt werden. Auch bei der Auslegung von Bundesrecht wie dem Strafvollzugsgesetz durch Landesbehörden ist nach der Rechtsprechung des Landesverfassungsgerichts<sup>40</sup> soweit wie möglich den Wertungen des Verfassungsgebers Rechnung zu tragen, der seinen Bürgerinnen und Bürgern ein voraussetzungsloses Grundrecht auf Akteneinsicht garantiert hat. Auch außerhalb des Bereichs des bundesrechtlichen Aktenauskunfts- und Einsichtsrechts, das die Gefangenenpersonen betrifft, bleibt durchaus noch Raum für das allgemeine Akteneinsichtsrecht nach dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz. Es gibt daher beispielsweise keinen Grund, Anfragen von Vollzugsinsassen nach Herausgabe von allgemeinen Richtlinien abzulehnen<sup>41</sup>. Allenfalls in Fällen, in denen beispielsweise Sicherheitsgesichtspunkte betroffen sind, darf eine Auskunft oder Einsicht verweigert werden.

### **5.1.2 Technisch-organisatorische Fragen**

Wird ein datenschutzrechtlicher Sachverhalt nicht durch das Strafvollzugsgesetz geregelt, kommen die allgemeinen Vorschriften des Brandenburgischen Datenschutzgesetzes zum Tragen. Erfolgt die Verarbeitung von Gefangenenpersonalakten nicht nur in Akten, sondern auch in elektronischer Form, ist für jedes eingesetzte automatisierte Verfahren zur Verarbeitung personenbezogener Daten nach § 8 BbgDSG ein Verfahrens- und Anlagenverzeichnis zu führen. Dies gilt sowohl für Daten der Inhaftierten als auch für die der Bediensteten, z. B. in Arbeitszeiterfassungssystemen. Solche Verzeichnisse lagen entweder gar nicht oder nur lückenhaft vor.

Die Führung des Anlagenverzeichnisses kann nach § 8 Abs. 4 BbgDSG entfallen, wenn ein Verzeichnis nach haushaltsrechtlichen Vorschriften geführt wird. Da Inventarlisten der Technikausstattung vorhanden waren, kamen wir überein, dass diese um die fehlenden Angaben nach der

<sup>40</sup> Beschluss vom 25.9.2002 – VfGBbg 79/02 – zur Vereinbarkeit einer Beschlagnahme mit dem Grundrecht auf Datenschutz

<sup>41</sup> Tätigkeitsbericht 2001, B 3.1

Verordnung zum Verfahrens- und Anlagenverzeichnis zu ergänzen sind, um mit möglichst geringem Aufwand den Anforderungen des Brandenburgischen Datenschutzgesetzes gerecht zu werden.

Im Land Brandenburg ist vorgesehen, alle Justizvollzugsanstalten mit dem **B**uchhaltungs- und **A**brechnungssystem im **S**trafvollzug (BASIS) auszustatten. Dies wird über die ADV-Leitstelle koordiniert, die für die Beschaffung von Informationstechnik und deren Betreuung in den Justizvollzugsanstalten eingesetzt wurde. In den von uns besuchten Anstalten wurde BASIS bereits genutzt. Probleme der Bediensteten beim Umgang mit dieser Software sind nach Aussagen der jeweiligen Systembetreuer nicht bekannt. BASIS bietet die Möglichkeit, die Zugriffsrechte der jeweiligen Nutzer, die sich über ihre jeweilige Kennung und ein Passwort in das System einloggen, auf das notwendige Maß einzuschränken. Die Vergabe dieser Berechtigungen war unterschiedlich geregelt; teilweise bedarf es noch schriftlicher Festlegungen für die Vergabe der Zugriffsrechte auf die Gefangenenendaten.

Für eine effektivere Kontrolle der Datenverarbeitungsanlagen ist es zudem erforderlich, aussagekräftige Organigramme und Netzpläne vorzuhalten und mit einer ausreichenden Dokumentation zu versehen. Letztlich muss diesen Erfordernissen auch aus Gründen des Datenschutzes, genauer der Ordnungsmäßigkeit des Datenschutzes, nachgekommen werden. Eine Dokumentation dient auch der Sicherung des technischen Betriebs und ist die unabdingbare Voraussetzung, eine EDV-Anlage unabhängig von konkreten Einzelpersonen pflegen zu können. Auf sie darf nicht mit dem Hinweis auf eine ADV-Leitstelle verzichtet werden, die den Einsatz der Anlagen koordiniert. Denn datenschutzrechtlich verantwortlich bleibt nach dem Gesetz die jeweilige Justizvollzugsanstalt.

Die Grundrechte auf Datenschutz und Akteneinsicht gelten auch im Strafvollzug. Sicherheitsbedürfnisse beim Betrieb einer Justizvollzugsanstalt müssen mit den Rechten der Betroffenen in Einklang gebracht werden. Technische Abläufe und personelle Verantwortlichkeiten sind ausreichend zu dokumentieren.

## 5.2 Rechtsgrundlage für den IMSI-Catcher

*Im Februar 2001 hat das brandenburgische Landeskriminalamt erstmals den sog. IMSI-Catcher im Rahmen einer Zielfahndung eingesetzt. Der Einsatz dieses Gerätes zur Lokalisierung von Handys wurde mit der Tatsache begründet, dass Verdächtige schwerer Straftaten ihre Mobiltelefone und Telefonkarten häufig wechseln, um auf Grund der ständig neuen Telefonnummern eine Überwachung ihrer Telefongespräche auszuschließen.*

In modernen Mobilfunknetzen spielt die Identitätsnummer des Handys, die "International Mobile Subscriber Identity" (IMSI) eine wichtige Rolle. Mit ihr bucht sich das Handy in die jeweils nächste Basisstation ein, um jederzeit erreichbar zu sein. Die IMSI ist nicht identisch mit der Rufnummer, sie wird ihr aber beim Verbindungsaufbau zugeordnet. Der IMSI-Catcher ist ein handliches Gerät, das sich im Netz gegenüber allen Handys, die in seiner Nähe benutzt werden, als Basisstation ausgibt und sie dazu veranlasst, ihm ihre Identifikationsnummer zuzusenden. Da auf diese Weise unmittelbar auch Handy-Rufnummern in Erfahrung gebracht werden können, die unter falschem Namen beantragt wurden, hat der IMSI-Catcher große praktische Bedeutung für die Strafverfolgungsbehörden. Er wird nicht nur dazu verwendet, alle Telefonate, die von einem eingebuchten Handy ausgehen, unbemerkt abzuhören, sondern auch um gesuchte Tatverdächtige zu lokalisieren. Da der IMSI-Catcher alle Mobiltelefone in seiner Umgebung erfasst, liegt es auf der Hand, dass durch seinen Einsatz in die Grundrechte zahlreicher unverdächtigter Personen eingegriffen wird.

Nach übereinstimmender Auffassung der Datenschutzbeauftragten und des Bundesjustizministeriums bestand bis zum Sommer 2002 keine Rechtsgrundlage für den Einsatz von IMSI-Catchern für die Strafverfolgung, da die Vorschriften der Strafprozessordnung hierfür nicht ausreichten. Erst durch das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002<sup>42</sup> ist eine begrenzte Rechtsgrundlage (§ 100i StPO) für den Einsatz dieser Technik geschaffen worden.

Seitdem darf zur Vorbereitung einer Telefonüberwachung nach § 100a StPO die Geräte- und Kartenummer sowie zur vorläufigen Festnahme oder zur Ergreifung eines Täters auf Grund eines Haftbefehles oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobiltelefons ermittelt werden. Die Feststellung der Geräte- und Kartenummer zur Vorbereitung einer Telefonüberwachung ist insbesondere nur zulässig, wenn dies zur Ermittlung einer im Katalog des § 100a StPO aufgeführten Straftat erforderlich ist. Der Einsatz des IMSI-Catchers steht unter Richtervorbehalt.

Zur vorläufigen Festnahme oder Ergreifung eines Tatverdächtigen auf Grund eines Haft- und Unterbringungsbefehls darf das Gerät nur verwendet werden, wenn er einer Straftat von erheblicher Bedeutung verdächtig wird und die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend wäre. Bei einer Straftat von erheblicher Bedeutung darf mittels IMSI-Catcher der Aufenthaltsort des mutmaßlichen Täters auch festgestellt werden, wenn es zur Eigensicherung der

zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich ist.

IMSI-Catcher können ausschließlich im Zusammenhang mit Strafverfolgungsmaßnahmen eingesetzt werden. Ihr Einsatz zum Abhören von Telefongesprächen ist ohne besondere richterliche Anordnung nicht nur unzulässig, sondern auch strafbar.

Der Bundesgesetzgeber hat es bei der Einfügung des § 100i in die Strafprozessordnung allerdings versäumt, entsprechend dem verfassungsrechtlichen Zitiergebot (Art. 19 Abs. 1 Satz 2 GG) die Einschränkung des grundrechtlichen Telekommunikationsgeheimnisses ausdrücklich im Gesetz festzustellen. Sinn des Zitiergebotes ist es nach der Rechtsprechung des Bundesverfassungsgerichts, die Volksvertretung dazu anzuhalten, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären<sup>43</sup>. Darauf hat der Landesbeauftragte gemeinsam mit den Datenschutzbeauftragten anderer Bundesländer den Bundespräsidenten in einem Schreiben vor der Ausfertigung des Gesetzes hingewiesen. Das Gesetz ist dennoch unverändert im Bundesgesetzblatt verkündet worden.

Seit August 2002 steht mit § 100i StPO eine Rechtsgrundlage für den Einsatz von IMSI-Catchern und vergleichbaren anderen technischen Mitteln zur Verfügung. IMSI-Catcher dürfen nur zur Strafverfolgung verwendet werden.

## 5.3 Fragen zum Grundbuch

### 5.3.1 Wie öffentlich ist das Grundbuch?

*Immer wieder erreichen uns Eingaben zur Einsicht in Grundbücher. Je nach Interessenlage beschweren sich Interessenten darüber, dass ihnen die Einsicht verwehrt, oder beklagen sich Betroffene darüber, dass sie Dritten ermöglicht wurde.*

In einer Entscheidung des Bundesverfassungsgerichts heißt es: "Das Grundbuch und die Grunddaten enthalten eine Fülle von personenbezogenen Daten aus dem persönlichen, familiären, sozialen und wirtschaftlichen Bereich. Wenn Dritten eine Grundbucheinsicht gewährt wird, liegt darin ein Eingriff in das auf diese Daten bezogene informationelle Selbstbestimmungsrecht."<sup>44</sup>

<sup>43</sup> BVerfGE 85, 386, 403 f.

<sup>44</sup> BVerfG, Kammerbeschluss vom 28.8.2000 – 1 BvR 1307/91 – NJW 2001, 503, 505

Die Voraussetzungen, unter denen ein solcher Eingriff berechtigt sein und jemand in das Grundbuch Einsicht nehmen oder Auskunft daraus erhalten kann, sind in § 12 der Grundbuchordnung festgelegt. Danach ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt. Ob ein solches vorliegt, muss jeweils für den konkreten Einzelfall festgestellt werden. Der Begriff des berechtigten Interesses ist dabei weit gefasst. Zweck dieser Regelung ist es, allen, die beabsichtigen, Verträge über ein Grundstück abzuschließen, Informationen über sämtliche Rechte, die mit diesem Grundstück zusammenhängen, zugänglich zu machen, um damit ihre wirtschaftlichen Interessen zu schützen. Nicht vorausgesetzt wird dagegen ein rechtliches Interesse des Einsicht Nehmenden (also seine Absicht, einen Anspruch gerichtlich durchzusetzen oder sich zur Verteidigung seiner Rechte auf Grundbuchinformationen zu berufen).

Vom Vorliegen eines berechtigten Interesses geht das Grundbuchamt bereits aus, wenn die Gründe für das Einsichtersuchen dargelegt werden und es ausgeschlossen erscheint, dass mit der Auskunft unzulässige Zwecke verfolgt werden. Die Vorlage von Nachweisen wie z. B. Kaufverträgen ist in der Regel nicht notwendig. Die Gewährung der Einsicht muss auf Teile des Grundbuchs beschränkt werden, wenn für die übrigen Teile kein berechtigtes Interesse festgestellt wird.

Zugang zu den Grundbüchern erhalten beispielsweise:

- Kreditgeber des Grundstückseigentümers,
- Gläubiger des Grundstückseigentümers, die beabsichtigen, dessen Grundbesitz in die Zwangsvollstreckung einzubringen,
- Wohnungseigentümer, die sich für die Wohnungsgrundbücher anderer Eigentümer derselben Gemeinschaft interessieren,
- Aktionäre, soweit deren Gesellschaft Grundstückseigentümer ist,
- Mieter, wenn der Vermieter wegen gestiegener Kapitalkosten die Miete erhöht,
- geschiedene Ehegatten des Grundstückseigentümers zur Durchsetzung eines Anspruchs auf Zugewinnausgleich.

Auch die Presse hat nach der Rechtsprechung des Bundesverfassungsgerichts ein grundsätzlich schutzwürdiges "berechtigtes" Interesse am Zugang zum Grundbuch. Allerdings muss das Grundbuchamt in die-

sem Fall zwischen dem Informationsinteresse der Öffentlichkeit und dem Persönlichkeitsrecht des Grundstückseigentümers abwägen<sup>45</sup>.

Die Einsicht ist durch das Grundbuchamt zu verweigern, wenn sie lediglich aus purer Neugier oder zu unbefugten Zwecken erfolgen soll. Als unbefugt gilt beispielsweise ein Kaufinteressent, der durch die Einsicht erst den Namen des Eigentümers erfahren möchte. Befindet er sich allerdings bereits in konkreten Vertragsverhandlungen, wird dies als berechtigtes Einsichtsinteresse anerkannt. Potenzielle künftige Ansprüche, wie die späterer Erben, sind hingegen grundsätzlich nicht ausreichend.

Zum Schutz der wirtschaftlichen Belange von Personen, die am Rechtsverkehr zu einem Grundstück beteiligt sind, besteht ein weit gefasstes Recht auf Einsicht in die Grundbücher. Ob deren dargelegtes Interesse berechtigt ist, haben die Grundbuchämter jeweils im Einzelfall zu prüfen.

### 5.3.2 Gehört ein Gerichtsurteil vollständig ins Grundbuch?

*Aufgrund eines Gerichtsurteils änderten sich die Eigentumsverhältnisse an einem Grundstück. Die begünstigte Prozesspartei beantragte daraufhin den entsprechenden Eintrag ins Grundbuch und reichte das Urteil samt Urteilsbegründung des Gerichts beim Grundbuchamt ein. Beides wurde vollständig zu den Grundbuchakten genommen. Die unterlegene Partei forderte jedoch, dass lediglich der Urteilstenor – ohne Urteilsgründe – zu den Akten genommen wird und wandte sich deshalb an den Landesbeauftragten.*

Ein rechtskräftiges Urteil ersetzt die für eine Übertragung des Eigentums an einem Grundstück notwendigen Erklärungen der unterliegenden Partei. Deren Mitwirkung ist daher – anders als bei einer normalen Eigentumsübertragung – nicht mehr nötig. Für die in einen Rechtsstreit gewinnende Partei genügt das Urteil als Nachweis der Berechtigung, eine Änderung des Grundbuchs zu erwirken.

Das Grundbuchamt muss nach § 10 Grundbuchordnung alle Unterlagen, aufgrund derer es eine Änderung einer Eintragung im Grundbuch vornimmt, vollständig zu den Akten nehmen, damit die Entwicklung der Rechtsverhältnisse an einem Grundstück lückenlos nachvollziehbar ist.

Gerichtsverhandlungen und damit auch die Urteile der Gerichte sowie deren Urteilsbegründungen sind grundsätzlich öffentlich. Alle, die Kenntnis von dem Urteil haben, können sich beim Gericht über die Be-

gründung informieren. Die Aufbewahrung der über die so genannte vollstreckbare Ausfertigung des Urteils hinausgehenden Begründung in den Grundbuchakten stellt somit keine unzumutbare Beeinträchtigung des Persönlichkeitsrechts des Schuldners dar und ist von diesem hinzunehmen.

Legt ein Gläubiger ein vollständiges Urteil vor, um eine Änderung der Eintragung der Eigentümerstellung im Grundbuch zu veranlassen, hat die Gegenseite keine Möglichkeit, zu erzwingen, dass nur eine um die Entscheidungsgründe gekürzte Fassung des Urteils zu den Grundbuchakten genommen wird.

## 5.4 Einführung des elektronischen Grundbuchs

*Im Rahmen der Einführung des elektronischen Grundbuchs wurde das Programm SOLUM-STAR ausgewählt. Das Oberlandesgericht Brandenburg bat uns in Vorbereitung eines Pilotbetriebes am Amtsgericht Frankfurt (Oder) um datenschutzrechtliche Beratung.*

Das Ziel des elektronischen Grundbuches besteht darin, alle herkömmlichen Akten auf elektronischen Medien zu speichern und die Eintragungen im Grundbuch künftig unmittelbar am Bildschirm vorzunehmen. Dazu müssen alle bisherigen Grundbücher eingescannt und in Bilddateien überführt werden. Bis zum Jahre 2006 wird dieses Vorhaben in einem sogenannten Umstellungszentrum im Landesbetrieb für Datenverarbeitung und Statistik, in dem auch das gesamte Grundbuchrechenzentrum angesiedelt werden soll, vollzogen. Bereits ab dem Jahre 2003 erhalten Notare, Banken und andere Behörden wie Finanzämter und Katasterämter in einem automatischen Abrufverfahren die Möglichkeit, über das Internet Einsicht in die Grundbücher zu nehmen.

Ein derartiges zentrales Grundbuchrechenzentrum und die mit dem Internet entstehenden Schnittstellen müssen höchsten Ansprüchen an Betriebssicherheit, Datensicherheit und Datenschutz genügen. Durch unsere rechtzeitige Einbeziehung hatten wir die Möglichkeit, bereits auf die Berücksichtigung der §§ 9 und 10 Brandenburgisches Datenschutzgesetz bezüglich automatisierter Abrufverfahren und technisch-organisatorischer Maßnahmen hinzuweisen.

Gemeinsam mit dem Oberlandesgericht und den beteiligten Unternehmen haben wir erörtert, durch welche technisch-organisatorischen Maßnahmen die hohen Anforderungen an den Datenschutz und die Datensicherheit gewährleistet werden können. Notwendig sind unter anderem folgende Vorkehrungen:

- Die Erstellung eines Sicherheitskonzeptes auf der Basis einer Risikoanalyse,
- die Auswahl geeigneter Verfahren zur digitalen Signatur,
- die Auswahl geeigneter Verfahren zur Verschlüsselung auf dem zentralen Grundbuchrechner, auf den Grundbuchclients und auf den Übertragungswegen,
- ein gesichertes automatisches Abrufverfahren, das den Zugriff auf berechnete Nutzerinnen und Nutzer beschränkt,
- die datenschutzgerechte Protokollierung der Veränderungen im Grundbuch sowie der Online-Abrufe.

Das eingesetzte Programm stammt z. T. bereits aus dem Jahre 1994. Viele Lösungen können daher nicht dem heutigen Stand der Technik entsprechen. Wir halten es für zwingend geboten, dass die Software im Rahmen der Einführung des elektronischen Grundbuchs überarbeitet und dem Stand der Technik angepasst wird.

Bei der Einführung des elektronischen Grundbuchs muss die eingesetzte Software den aktuellen Anforderungen an den Datenschutz und die Datensicherheit genügen.

## **5.5 Erprobung des elektronischen Rechtsverkehrs (ELREV)**

*Der bundesweite Geschäftsverkehr mit Gerichten und Staatsanwaltschaften soll künftig auch auf elektronischem Wege möglich werden. Die Landesregierung hatte dazu ein Konzept zur Erprobung des elektronischen Rechtsverkehrs (ELREV) vorgelegt; erste Erfahrungen dazu sollten im Rahmen eines Pilotprojektes am Finanzgericht Cottbus gesammelt werden.<sup>46</sup>*

Unverzichtbare Schwerpunkte waren dabei auch für das Ministerium der Justiz und für Europaangelegenheiten Fragen des Datenschutzes und der Wahrung des Steuergeheimnisses. Es bestand Einigkeit mit dem Landesbeauftragten darüber, dass Authentizität, Vertraulichkeit, Integrität und Verbindlichkeit der ausgetauschten Daten durch geeignete digitale Signaturlösungen gesichert werden müssen. Das Ministerium hat betont, dass eine auf Brandenburg beschränkte Lösung nicht realistisch ist, da

<sup>46</sup>

siehe Tätigkeitsbericht 2001, A 1.6.1

die gesamte öffentliche Verwaltung aller Bundesländer und des Bundes und im Rahmen der EU möglichst nach einheitlichen Standards vorgehen sollten. Als Ergebnis der Zusammenarbeit der einzelnen Bundesländer im Rahmen der Arbeitsgruppe "Elektronischer Rechtsverkehr" verabschiedete die Konferenz der Justizministerinnen und -minister im Juni 2002 die "Organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften".

Auch wenn Details noch der Erörterung bedürfen, bieten diese Leitlinien eine gute Grundlage für die künftige Datensicherheit im Justizbereich, wenn sie konsequent umgesetzt werden.

Die Einführung des elektronischen Rechtsverkehrs verlangt letztlich eine Verständigung in der Europäischen Union auf einheitliche technische und datenschutzrechtliche Standards.

## **6 Bildung, Jugend und Sport**

### **6.1 Was dürfen Eltern volljähriger Schüler erfahren?**

*Das Ministerium für Bildung, Jugend und Sport des Landes Brandenburg hatte uns unter dem Eindruck des Amoklaufs eines ehemaligen Schülers an einem Erfurter Gymnasium den Entwurf eines Rundschreibens zur Information der Schule an Eltern volljähriger Schülerinnen und Schüler vorgelegt. Darin war vorgesehen, dass das Einverständnis der Betroffenen mit der Information der Eltern über wichtige schulische Angelegenheiten bis zu einem schriftlichen Widerspruch unterstellt werden könne. Im Falle eines Widerspruchs sollte die Schule die Eltern schriftlich darüber informieren.*

Die Übermittlung wichtiger Informationen an die Eltern volljähriger Schülerinnen und Schüler ist als Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen anzusehen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur auf Grund einer Einwilligung der volljährigen Schülerinnen und Schüler oder im überwiegenden Allgemeininteresse auf einer verfassungsgemäßen gesetzlichen Grundlage zulässig.

An die Stelle der Einwilligung der Betroffenen sollte nach dem Entwurf des Ministeriums ein Widerspruchsrecht treten. Schweigen als Zustimmung zu werten, ist allerdings mit dem Erfordernis einer ausdrücklichen Einwilligung der Schülerinnen und Schüler nach § 65 Abs. 6 Satz 2 Brandenburgisches Schulgesetz nicht zu vereinbaren. Darüber hinaus

würden der Schule im Falle des schriftlichen Widerspruchs der volljährigen Schülerin bzw. des volljährigen Schülers auch persönliche Familienverhältnisse (z. B. familiäre Konfliktsituationen) offenbart. Für eine solche Datenübermittlung muss deshalb eine klare gesetzliche Regelung geschaffen werden, die Ausnahmefälle für die Unterrichtung der Eltern eng festlegt. Auch sind die betroffenen Schülerinnen und Schüler über die beabsichtigte Datenübermittlung zu informieren. Aber auch eine gesetzliche Regelung dürfte nur solche Eingriffe in das Grundrecht der volljährigen Schülerinnen und Schüler vorsehen, die dem Verhältnismäßigkeitsgrundsatz genügen.

Insbesondere ist fraglich, ob die Unterrichtung der Eltern geeignet ist, den angestrebten Zweck (tatsächliche Verhinderung solcher Vorfälle wie jüngst in Erfurt geschehen) erreichen zu können. Es müsste geprüft werden, ob nicht wirkungsvollere Lösungen für die Handhabung zur Konfliktlösung mit volljährigen Schülerinnen und Schülern zur Verfügung stehen (z. B. Beteiligung spezieller Beratungsstellen). Das überwiegende öffentliche Interesse kann jedenfalls nicht mit dem in Artikel 6 Abs. 2 Satz 1 Grundgesetz normierten Elternrecht begründet werden. Denn dieses ist mit der Volljährigkeit erloschen.

Das Ministerium für Bildung, Jugend und Sport plant eine Novellierung des Brandenburgischen Schulgesetzes, wobei noch nicht feststeht, ob eine Einwilligungs- oder Widerspruchslösung bevorzugt wird.

Volljährige Schülerinnen und Schüler verfügen über ein eigenes, von den Eltern unabhängiges Recht auf Datenschutz. Sollten die Eltern über wichtige schulische Angelegenheiten dieser Kinder informiert werden, ist zuvor deren Einwilligung einzuholen.

## 6.2 Müssen Lehrkräfte alles offenbaren?

*Ein staatliches Schulamt forderte 500 potenziell von einer Versetzung betroffene Lehrkräfte auf, alle erdenklichen Gründe zu benennen, die aus ihrer Sicht einer möglichen Versetzung in einen anderen Schulamtsbezirk entgegenstehen könnten. Der Personalüberhang machte jedoch nicht 500, sondern nur 20 bis 30 Versetzungen notwendig.*

Das entsprechende Aufforderungsschreiben an die Lehrkräfte enthielt u. a. den Hinweis, dass unter Umständen nicht alle persönlichen Gründe im Rahmen einer Abwägungsentscheidung rechtlich bedeutsam sein werden, sowie die Bitte, alle aus der Sicht der Lehrkräfte in Betracht kommenden persönlichen Gründe anzugeben.

Die pauschale Abfrage personenbezogener Daten führte dazu, dass die Lehrkräfte sich veranlasst sahen, sämtliche Lebensumstände anzugeben, die ihrer Versetzung entgegenstehen. Es ist daher in einer solchen Situation zu erwarten, dass dem staatlichen Schulamt personenbezogene Daten bekannt werden, die für die Auswahl der für eine Versetzung in Betracht kommenden Lehrkräfte weder geeignet noch erforderlich sind. Das an die betroffenen Lehrkräfte gerichtete Schreiben enthielt keinerlei Anhaltspunkte, welche Kriterien letztlich bedeutsam sind und worauf das staatliche Schulamt seine Auswahlentscheidung stützen wollte. Tatsächlich sahen sich Betroffene gehalten, gesundheitliche Beeinträchtigungen und intimste Lebensumstände mitzuteilen. Dafür, dass nur ca. 20 bis 30 Lehrkräfte versetzt werden sollten, war die Abfrage von nicht näher konkretisierten personenbezogenen Daten bei ca. 500 Lehrkräften zudem unverhältnismäßig. Wir sind jedoch davon ausgegangen, dass hierfür entsprechend einer Sozialauswahl bei einer Kündigung objektive Kriterien herangezogen werden und die persönlichen Umstände erst im Rahmen einer konkreten Anhörung als Hilfskriterien Verwendung finden.

Wir haben das staatliche Schulamt darauf hingewiesen, dass diese Form der Personaldatenerhebung unzulässig ist, da sie ohne ausreichende Rechtsgrundlage erfolgt. Nach § 29 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) sowie § 57 Abs. 4 Landesbeamtengesetz (LBG) dürfen Beschäftigtendaten nur verarbeitet werden, wenn dies u. a. zur Durchführung des Arbeitsverhältnisses erforderlich ist.

In Anbetracht des bestehenden arbeits- bzw. dienstrechtlichen Abhängigkeitsverhältnisses und der drohenden Versetzung werden die Lehrkräfte zu dem quasi gezwungen, z. T. sehr persönliche Angaben schon weit im Vorfeld einer konkreten Entscheidung darzulegen. Von einer Freiwilligkeit im Sinne des Brandenburgischen Datenschutzgesetzes ist daher nicht auszugehen.

Unserer Bitte, diese Art der Personaldatenerhebung sofort einzustellen und bereits rückgesandte Erhebungsbögen zu vernichten, ist das staatliche Schulamt nicht nachgekommen. Allerdings wurden die Lehrkräfte mit einem neuerlichen Schreiben darüber informiert, dass die erbetenen zusätzlichen Personaldaten ausschließlich freiwillig abzugeben sind und keine Pflicht der Behörden gegenüber besteht, der Bitte um Angabe von einer Versetzung entgegenstehenden Gründe zu folgen. Ein Katalog von Auswahlkriterien wurde nicht erstellt. Darüber hinaus wurde nicht verdeutlicht, dass derjenige, der sich nicht an der Befragung beteiligt, seine Einwände auch im persönlichen Gespräch vorbringen kann.

Für den Fall, dass es im nächsten Schuljahr erneut zu Versetzungsmaßnahmen kommen sollte, wird das betroffene staatliche Schulamt unsere Bedenken erneut prüfen und berücksichtigen. Von einer Beanstandung wurde aus diesem Grunde vorerst abgesehen.

Um eine sachgerechte Entscheidung bei einer Versetzungsauswahl zu treffen, kann es erforderlich sein, im Vorfeld dazu personenbezogene Daten zu erheben. Allerdings ist der Kreis der Betroffenen anhand eines zu erstellenden Kriterienkatalogs möglichst frühzeitig einzugrenzen. Dieser ist den Bediensteten, die möglicherweise versetzt werden, mitzuteilen, damit sie ihre Angaben dementsprechend machen können. Pauschale Abfragen persönlicher Informationen sind dagegen unzulässig. Wer das persönliche Gespräch der Ausfüllung eines Formulars vorzieht, darf nicht benachteiligt werden.

## **7 Wissenschaft, Forschung und Kultur**

### **7.1 Gesundheitsdaten von Kindern in einem Forschungsvorhaben**

*Eine Universität plante ein Projekt zur Erforschung der These, dass Bewegung im Kindesalter die Hirnreifung fördert. Hierzu sollten kinderärztliche Untersuchungen ausgewertet und Kindergärten befragt werden. Mit den Ergebnissen sollten pädagogische Konzepte für die Arbeit in Kindertagesstätten und Schulen erstellt werden. Bereits im Rahmen der Vorbereitung des Projekts wurden wir gebeten, zu klären, wie mit den erfragten personenbezogenen Daten der Kinder umzugehen ist.*

Im Zusammenhang mit den Untersuchungen ist an erster Stelle die Frage zu klären, ob es möglich ist, auf einen Personenbezug der im Forschungsprojekt verarbeiteten Daten zu verzichten.

Es wurde vereinbart, die bei Kinderärzten erhobenen Daten soweit wie möglich nur nach Altersgruppen sowie Geschlecht und unter Rubriken wie beispielsweise "Motorikfähigkeiten 7-jähriger Mädchen" zusammengefasst weiterzugeben. Die Daten sind insoweit als anonym zu betrachten und können daher datenschutzrechtlich unproblematisch weiterverarbeitet werden. Dort, wo in bestimmten zeitlichen Abständen Wiederholungsuntersuchungen erforderlich sind, wird mit Pseudonymen gearbeitet. Den einzelnen Kindern wird zu diesem Zweck eine Kennung zugewiesen, die es für einen außenstehenden Dritten ohne Zusatzwissen unmöglich macht, einen Bezug zu einer konkreten Person herzustellen.

Hier sind besondere Sicherheitsvorkehrungen bei der Verwahrung der Unterlagen zu treffen, mit deren Hilfe die hinter den Pseudonymen verborgenen Personen aufgefunden werden können.

Allerdings ist auch bei Pseudonymen noch immer ein Personenbezug herstellbar. Es handelt sich insofern um datenschutzrechtlich geschützte Informationen, die nur aufgrund einer gesetzlichen Bestimmung bzw. der Einwilligung der Betroffenen verarbeitet werden dürfen. Von der Nutzung der Forschungsklausel des Brandenburgischen Datenschutzgesetzes, die es unter eng umrissenen Voraussetzungen erlaubt, personenbezogene Daten ohne Einwilligung zu nutzen, wurde abgesehen, da es sich auch um besonders sensitive Gesundheitsdaten handelt. Daher ist es erforderlich, eine Einwilligung der Betroffenen einzuholen. Diese werden aufgrund ihres kindlichen Alters von den Sorgeberechtigten, i. d. R. ihren Eltern, vertreten, die an ihrer Stelle entscheiden müssen, ob sie einwilligen.

Eine Weitergabe personenbezogener Daten ist auch in pseudonymisierter Form nicht vorgesehen. Vielmehr sollen die Daten in einem weiteren Schritt aufbereitet und losgelöst von Einzelpersonen zu Gruppen zusammengefasst werden. Erst dann erfolgt die Weitergabe an die Forschungspartner. Sie ist, da es ihnen nunmehr am Personenbezug mangelt, aus datenschutzrechtlicher Sicht unbedenklich.

Für das Einholen der erforderlichen Einverständniserklärungen wird auf das Adressmittlungsverfahren zurückgegriffen. Das Forschungsinstitut erstellt hierzu eine schriftliche Beschreibung des Projekts und bittet die Eltern durch eine beigefügte Einwilligungserklärung, der Teilnahme ihrer Kinder zuzustimmen. Die vorbereiteten Unterlagen werden dann von den Kindertagesstätten und Kinderärzten an die Betroffenen weitergereicht, sodass das Institut selbst zu diesem Zeitpunkt keine Namen und Adressen erhält. Damit haben es die Eltern in der Hand, in die Preisgabe persönlicher Daten ihrer Kinder einzuwilligen.

Für Forschungsvorhaben, die den Umgang mit personenbezogenen Daten einschließen, ist es in aller Regel nötig, eine Einwilligungserklärung der Betroffenen einzuholen. Die Verwendung personenbezogener Daten ist so weit wie möglich zu beschränken, sie sollen frühzeitig anonymisiert werden. Die Verwendung von Pseudonymen gewinnt in Forschungsprojekten immer mehr an Bedeutung, wobei pseudonymisierte Daten – im Gegensatz zu anonymisierten – einen Personenbezug aufweisen und nur unter Beachtung des Datenschutzrechts verarbeitet werden dürfen.

## 7.2 Begleitforschung zum neuen Grundsicherungsgesetz

*Zur Beurteilung der Auswirkungen des Grundsicherungsgesetz und zu seiner Fortentwicklung wird eine Bundesstatistik mit verschiedenen Erhebungsmerkmalen (u. a. Alter, Geschlecht, Staatsangehörigkeit, Größe der Bedarfsgemeinschaft, Ursachen und Beginn der Leistung, (Netto-) Bedarf je Monat) geführt. Die Grundsicherungsämter sind zur Auskunft an die Statistikämter verpflichtet. Zugleich hat das Bundesministerium für Arbeit und Sozialordnung das Institut für angewandte Sozialwissenschaft (infas) mit einer begleitenden Forschung beauftragt, um Fragen der Inanspruchnahme, der "verschämten Armut", der Überschneidung von Grundsicherung und Sozialhilfe, der Mehrausgaben sowie der Administration zu klären.*

Seit dem 1. Januar 2003 gilt das neue Gesetz über eine bedarfsorientierte Grundsicherung im Alter und bei Erwerbsminderung (Grundsicherungsgesetz, GSiG)<sup>47</sup>. Danach hat jeder über 65-Jährige sowie jeder im Sinne des § 43 Abs. 2 Sechstes Buch Sozialgesetzbuch erwerbsgeminderte Volljährige statt des Sozialhilfeanspruches einen Anspruch auf eine bedarfsorientierte Grundsicherung, soweit er seinen Lebensunterhalt nicht aus seinem Einkommen und Vermögen beschaffen kann. Die Berechnung von Einkommen und Vermögen richtet sich wiederum nach den einschlägigen Vorschriften des Bundessozialhilfegesetzes (BSHG). Im Unterschied zur Sozialhilfe wird die Grundsicherung jährlich bewilligt; unterhaltspflichtige Kinder und Eltern werden nicht in die Pflicht genommen, sofern deren Einkommen 100.000 Euro nicht übersteigt. Der Kreis der Anspruchsberechtigten wird aus diesem Grunde steigen, aber auch, weil Neuantragsteller aus dem Bereich der verdeckten Altersarmut erwartet werden. Zuständig sind die neu eingerichteten Grundsicherungsämter der Kreis-, Stadt- oder Gemeindeverwaltungen.

Hierbei wird u. a. ein Abgleich der (neu einzurichtenden) Grundsicherungsstatistik mit der (schon existenten) Sozialhilfestatistik geführt, um Veränderungen und Verschiebungen abzubilden. Sämtliche Individualdatensätze werden anonymisiert übermittelt, d. h. Einzelangaben sind nicht mehr oder nur durch einen unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren Person zuzuordnen. Kennnummern der Sozialhilfe-Datensätze sind zu löschen und Kommunen mit unter 1.000 Einwohnern sowie über 90-jährige Leistungsbezieher nicht mit in die Forschung einzubeziehen, um eine Identifizierung vollständig auszuschließen. Aus datenschutzrechtlicher Sicht ist daher eine Genehmigung zu Forschungszwecken nicht erforderlich.

---

<sup>47</sup> BGBl. 2001 I S. 1310, 1335 in der Fassung der Änderung vom 27.4.2002 in BGBl. I S. 1462

Weiterhin ist eine stichprobenartige, telefonische Einzelbefragung von Leistungsbeziehern u. a. zu Ursachen der unterlassenen Antragstellung vor Einführung des Grundsicherungsgesetzes zur Bewertung desselben, aber auch zu zusätzlichen Unterhaltsleistungen beabsichtigt. Hierzu begehrt infas von den Grundsicherungsämtern die Adressen von Leistungsbeziehern ohne deren vorherige Zustimmung. Auch bei Forschungsvorhaben gilt gem. § 75 Zehntes Buch Sozialgesetzbuch für die Übermittlung von Sozialdaten grundsätzlich der Einwilligungsvorrang. Nur wenn der Zweck der Forschung nicht mehr erreichbar ist, kann eine Übermittlung ausnahmsweise ohne Zustimmung erforderlich sein.

Da nur eine geringe Anzahl von Leistungsempfängern auf eine nachträgliche Anfrage mit der Bitte um die Gewährung des schriftlichen Einverständnisses reagieren würde, ist von einer Gefährdung eines aussagekräftigen Forschungsergebnisses auszugehen. Die Weitergabe der Adressen durch die Grundsicherungsämter ist daher zulässig. Zum Ausgleich für diese Beeinträchtigung müssen die Betroffenen vorher bei Antragstellung über die beabsichtigte Übermittlung ihrer Daten und den Zweck der Forschung unterrichtet werden. Dabei soll ihnen die Möglichkeit eingeräumt werden, innerhalb eines Monats nach der Unterrichtung der Datenweitergabe zu widersprechen. Diese Widerspruchslösung entspricht den parallelen gesetzlichen Vorschriften zur Forschung im Bereich des Bundessozialhilfegesetzes und stellt eine sachgerechte Abwägung zwischen den Persönlichkeitsrechten einerseits und der Forschungsfreiheit sowie der Evaluation von Leistungsgesetzen andererseits dar.

Eine Offenbarung von Adressen zu Forschungszwecken darf nur erfolgen, wenn der Betroffene zuvor von der möglichen Übermittlung und dem Forschungszweck unterrichtet und ihm ein Widerspruchsrecht eingeräumt wird.

### **7.3. Abi 1942 – Ein Klassentreffen**

*Zur Vorbereitung eines Klassentreffens des Abiturjahrgangs 1942 wurde Einsicht in ein Stadtarchiv begehrt. Anhand der dort liegenden Zeugnisse sollten die Personen des Abiturjahrgangs festgestellt werden.*

Die Benutzung von Archivgut richtet sich nach dem Brandenburgischen Archivgesetz (BbgArchivG). Nach dessen § 10 Abs. 3 darf in Archivgut, das wie z. B. Schulzeugnisse personenbezogene Daten enthält, nicht ohne Weiteres Einsicht genommen werden.

Es gelten hier verschiedene Sperrfristen: Eine Einsicht in Archivgut darf danach erst zehn Jahre nach dem Tod der betroffenen Personen erfolgen. Ist das Todesjahr nicht bekannt, endet die Frist neunzig Jahre nach der Geburt. Ist auch das Geburtsjahr nicht bekannt, endet die Schutzfrist sechzig Jahre nach der Entstehung der Unterlagen. Geht man davon aus, dass i.d.R das Abitur im Alter von achtzehn Jahren erworben wird, sind im vorliegenden Fall erst achtundsiebzig Jahre der Sperrfrist von neunzig Jahren verstrichen.

Allerdings ist eine Verkürzung der Schutzfristen denkbar: Nach § 10 Abs. 5 BbgArchivG können die Fristen im Einzelfall nämlich verkürzt werden, sofern nicht besondere in den § 11 und 12 BbgArchivG genannte Gründe die Einsicht in die Unterlagen ausschließen. Als möglicher Ausschlussgrund kämen hier lediglich die in § 11 Abs. 1 Nr. 2 BbgArchivG genannten "schutzwürdigen Belange Dritter" in Betracht. Angesichts des langen zurückliegenden Zeitraums ist eine ernsthafte Gefährdung der Rechte der Betroffenen nicht mehr zu befürchten: Nach so vielen Jahren bedeutet die Einsichtnahme in Zeugnisse zum Zwecke der Zuordnung der Personen zu einem bestimmten Schulabschlussjahrgang und die damit verbundene Möglichkeit, zugleich auch deren Schulnoten wahrzunehmen, keinen allzu schweren Eingriff in die Persönlichkeitsrechte. Der Einsichtnehmende könnte zudem nach § 10 Abs. 5 Satz 2 BbgArchivG verpflichtet werden, Namen und Geburtsdaten ausschließlich für die Organisation des geplanten Klassentreffens zu verwenden und über weitere Daten – die Schulnoten der Betroffenen – Stillschweigen zu bewahren. Eine Verletzung datenschutzrechtlicher Bestimmungen wäre bei einem solchen Vorgehen nicht zu befürchten. Die Entscheidung über eine Verkürzung der Sperrfristen sowie die Gewährung der Einsicht in die Unterlagen liegt ausschließlich im Ermessen des Archivs.

Sechzig Jahre nach dem Ablegen der Abiturprüfung bedeutet es keinen erheblichen Eingriff in die Persönlichkeitsrechte, wenn zum Zwecke der Organisation eines Jahrgangstreffens einem ehemaligen Mitschüler die Einsicht in die bei einem Stadtarchiv aufbewahrten Abiturzeugnisse erlaubt wird.

## **8 Arbeit, Soziales, Gesundheit und Frauen**

### **8.1 Soziales**

#### **8.1.1 Verhaltensprofile Behinderter im Sozialamt**

*Werden sozialhilfeberechtigte Behinderte in Einrichtungen betreut, sind die Sozialhilfeträger nach dem Bundessozialhilfegesetz (BSHG) gehalten, sich bei der Vergütung am Betreuungsbedarf der behinderten Menschen zu orientieren. Die Sozialämter müssen die behinderten Menschen dazu in Gruppen mit einem vergleichbaren Hilfebedarf einordnen. Gegen diese Datenverarbeitung wandte sich der Träger eines betroffenen Heimes.*

Damit die Sozialämter in der Lage sind, die Hilfeempfänger den Gruppen mit vergleichbarem Hilfebedarf zuzuordnen, wird landesweit nach einem einheitlichen Verfahren vorgegangen, das die Brandenburger Kommission nach § 93 BSHG entwickelt hat. Die Träger der Einrichtungen sind gehalten, einen umfangreichen Fragebogen auszufüllen, in dem zunächst für den Lebensbereich "Wohnen" die Fähigkeiten des behinderten Menschen in einzelnen Bereichen der täglichen Lebensführung in einem Aktivitätsprofil ermittelt werden. Für jede dieser Fähigkeiten formuliert die Einrichtung dann einen nach vier Gruppen unterteilten Hilfebedarf.

Obwohl den Sozialämtern damit eine Fülle sehr sensibler Informationen über die behinderten Menschen vorliegen, ist dieser Teil des Verfahrens datenschutzrechtlich nicht zu beanstanden.

Mit der Aufforderung an die Einrichtungen, die ausgefüllten Fragebögen an die Sozialämter zu übersenden, werden Sozialdaten der betroffenen Bewohner erhoben. Da die Fragebögen in der Regel nicht durch die Bewohner selbst, sondern durch die Einrichtungen ausgefüllt werden, handelt es sich um eine Datenerhebung bei Dritten, die nur unter engen Voraussetzungen zulässig ist. Da die Einrichtungen nicht selbst dem Sozialgeheimnis unterliegen, ist eine solche Datenerhebung u. a. dann erlaubt, wenn die Aufgaben, zu deren Erfüllung die Daten erhoben werden, ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Hilfebedürftigen beeinträchtigt werden.

Diese Voraussetzung war aus unserer Sicht erfüllt. Die Art der abgefragten Angaben schließt ein Ausfüllen der Fragebögen durch die Hilfebedürftigen selbst aus. Die Hilfeempfänger dürften in der Regel nicht

selbst in der Lage sein, ihre eigenen Fähigkeiten und den daraus abzuleitenden Hilfebedarf einzuschätzen, sodass nur eine Befragung der Einrichtung in Betracht kam. Zusätzlich ist es aus unserer Sicht notwendig, dass die Hilfebedürftigen bzw. ihre gesetzlichen Vertreter in die Beantwortung des Fragebogens einbezogen werden. Dies ist nach Angaben der Sozialhilfeträger der Fall.

Da die Daten zur Erfüllung der Aufgaben der Träger der Sozialhilfe erforderlich sind, sind die Hilfebedürftigen gemäß § 60 SGB I zur Mitwirkung verpflichtet, wozu ggf. auch eine Entbindung schweigepflichtiger Personen von ihrer Schweigepflicht gehört.

Die mit den Fragebögen erhobenen Daten sind auch für die Erfüllung der Aufgaben der Sozialämter erforderlich. Die Datenerhebung durch die örtlichen Träger der Sozialhilfe soll dazu dienen, die Hilfeempfänger in Gruppen mit vergleichbarem Hilfebedarf einzuordnen. Nur anhand der Informationen aus dem Fragebogen kann das Sozialamt feststellen, ob die von der Einrichtung ausgefüllten Angaben zu einer der vier Hilfebedarfsgruppen plausibel sind. Die Prüfung auf Plausibilität kann nur durchgeführt werden, wenn der örtliche Träger der Sozialhilfe sowohl über die Angaben zum Aktivitätsprofil als auch zum geltend gemachten Hilfebedarf verfügt. Die Ergebnisse der Plausibilitätsprüfung wirken sich wiederum unmittelbar auf die Zuordnung zu den Hilfebedarfsgruppen aus. Die Erforderlichkeit für die Erfüllung der Aufgaben des örtlichen Trägers der Sozialhilfe ist damit gegeben.

Die Sozialämter dürfen eine Reihe sensibler Sozialdaten erheben, um für die in Einrichtungen betreuten sozialhilfebedürftigen Behinderten den Betreuungsbedarf und damit die Leistungen nach dem Bundessozialhilfegesetz zu ermitteln.

### **8.1.2 Unzulässige Datensammlung beim Sozialamt**

*Bei der Bearbeitung der Beschwerde einer Sozialhilfeempfängerin haben wir uns erneut mit der Vorlage von Kontoauszügen und deren Ablage in der Sozialhilfeakte befasst.<sup>48</sup> Außerdem war der zulässige Umfang von Halteranfragen bei der Kfz-Zulassungsstelle durch das Sozialamt Gegenstand dieser Eingabe.*

Das Sozialamt hatte die Sozialhilfeempfängerin bei der erstmaligen Antragstellung aufgefordert, die Kontoauszüge der letzten drei Monate vorzulegen. Im Anschluss daran ergingen z. T. mehrmals innerhalb eines Jahres weitere Anforderungen zur Vorlage von Kontoauszügen, ohne

<sup>48</sup>

vgl. Tätigkeitsbericht 2001, A 8.1.1.3

dass dafür ein konkreter Anlass in der Sozialhilfeakte dokumentiert war. Zudem waren in der Akte die Kopien von über 100 Kontoauszügen ungeschwärzt abgeheftet.

Nach § 67a des Zehnten Buches des Sozialgesetzbuches (SGB X) darf das Sozialamt von Personen, die Sozialhilfe beziehen oder beantragen, die erforderlichen Daten erheben. Die Sozialhilfeempfänger sind dabei nach § 60 SGB I verpflichtet, die notwendigen Auskünfte zu erteilen und die erforderlichen Unterlagen vorzulegen.

Hilfe zum Lebensunterhalt wird nur Personen gewährt, die ihren notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften und Mitteln, vor allem aus ihrem Einkommen und Vermögen beschaffen können. Deshalb müssen die Sozialämter prüfen, ob der Antragsteller über Einkommen oder Vermögen verfügt. Um dies festzustellen, sind dem Sozialamt Originalkontoauszüge vorzulegen.

Wir sehen es als erforderlich an, wenn sich das Sozialamt bei der ersten Antragstellung die Kontoauszüge der letzten drei Monate vorlegen lässt. In der Regel ist es dann ausreichend, wenn dem Sozialamt erst wieder nach einem oder zwei Jahren die Kontoauszüge der letzten drei Monate vorgelegt werden. Besteht allerdings ein konkreter Anlass (z. B. ständig wechselndes Einkommen oder Anhaltspunkte für zusätzliches Einkommen), kann sich das Sozialamt die Kontoauszüge auch in kürzeren Abständen oder sogar lückenlos vorlegen lassen. Eine solche intensivere Kontrolle muss vom Sozialamt aber begründet und in der Akte dokumentiert werden.

Das betroffene Sozialamt hat eingeräumt, in einigen Fällen ohne Anlass Kontoauszüge angefordert bzw. den besonderen Anlass weder gegenüber der Sozialhilfeempfängerin begründet noch in der Akte dokumentiert zu haben und uns zugesichert, die Vorgaben des Sozialdatenschutzes in Zukunft zu beachten.

Das Sozialamt darf auch Kopien von Kontoauszügen anfertigen und diese in der Sozialhilfeakte abheften. Dies ist aber nur dann erlaubt, wenn sich auf dem Kontoauszug überhaupt Buchungen befinden, die das Sozialamt für die Prüfung des Einkommens und Vermögens benötigt. Alle übrigen Buchungen sind vom Sozialamt zu schwärzen, wenn es Kopien zur Akte nehmen will. Auch hier hat das betroffene Sozialamt zugesagt, die nicht erforderlichen Kontoauszüge zu entfernen bzw. nicht erforderliche Buchungen zu schwärzen.

Das Sozialamt hatte in dem vorliegenden Fall außerdem bei der Kfz-Zulassungsstelle angefragt, ob ein bestimmter, konkret benannter PKW auf

die Sozialhilfeempfängerin oder einen vom Sozialamt vermuteten Lebenspartner der Hilfeempfängerin zugelassen sei. Anfragen in dieser Form sind unzulässig.

Nach § 117 Abs. 3 Satz 1 Bundessozialhilfegesetz (BSHG) darf das Sozialamt u. a. bei der Kfz-Zulassungsstelle Daten von Personen überprüfen, die Leistungen nach dem Bundessozialhilfegesetz beziehen. Damit ist zunächst der zu überprüfende Personenkreis auf den Sozialhilfeempfänger selbst beschränkt. Daten von Dritten – etwa eines Lebenspartners – dürfen nicht überprüft werden.

§ 117 Abs. 3 Satz 2 BSHG schreibt weiterhin vor, dass das Sozialamt im Rahmen der Anfrage seinerseits nur bestimmte Daten an die Kfz-Zulassungsstelle übermitteln darf. Zu den dort genannten Daten gehört z. B. nicht das amtliche Kennzeichen eines Fahrzeugs. Unzulässig ist daher beispielsweise eine Frage, auf wen ein bestimmtes Fahrzeug zugelassen ist.

Sozialämter dürfen sich bei erstmaliger Antragstellung und in Abständen von mindestens einem Jahr die Kontoauszüge der letzten drei Monate ohne konkreten Anlass vorlegen lassen. Darüber hinaus ist eine Vorlage nur bei konkretem Anlass zulässig, der gegenüber dem Hilfeempfänger zu begründen und in der Akte zu dokumentieren ist. Kopien von Kontoauszügen dürfen nur im erforderlichen Umfang zur Akte genommen werden; nicht erforderliche Angaben sind zu schwärzen.

Sozialämter dürfen bei der Kfz-Zulassungsstelle ausschließlich danach fragen, ob ein bestimmter Sozialhilfeempfänger Halter eines Fahrzeugs ist. Daten zum Fahrzeug selbst dürfen nicht übermittelt werden.

### **8.1.3 Befragungen von Patienten in der gesetzlichen Krankenversicherung**

#### **8.1.3.1 "Wie war es denn im Krankenhaus?"**

*Patienten, die sich in stationärer Behandlung befanden, wurden von ihrer Krankenkasse nach Abschluss der Behandlung zu ihrem Krankenhausaufenthalt befragt. So wollte die Krankenkasse nicht nur wissen, ob die Versicherten mit der Behandlung zufrieden waren. Die Versicherten wurden auch gebeten, sich dazu zu äußern, ob sie regelmäßig ärztlich behandelt worden sind und ob bzw. wann sie operiert wurden.*

Die Krankenkasse verwendete dabei einen personenbezogenen Fragebogen, der weder eine Begründung oder eine Rechtsgrundlage für die Befragung noch einen Hinweis auf die Freiwilligkeit der Beantwortung der Fragen enthielt. Dieses Vorgehen war nicht datenschutzgerecht.

Die Krankenkasse erhält von den Krankenhäusern zum Zwecke der Abrechnung eine Reihe von versichertenbezogenen Daten nach § 301 Fünftes Buch Sozialgesetzbuch (SGB V). Mit dem Fragebogen erhob die Krankenkasse daneben zum Teil Daten, die sie nach dieser Vorschrift vom Krankenhaus nicht bekommen würde und die zur Erfüllung Ihrer Aufgaben nicht erforderlich sind. Teilweise handelte es sich um Daten, die die Krankenkasse nach § 301 SGB V ohnehin erhält, so dass für eine doppelte Erhebung keine Notwendigkeit ersichtlich war.

Es entstand der Eindruck, dass die Krankenkasse mit den Angaben aus dem Fragebogen beabsichtigt, Notwendigkeit, Dauer, Qualität und Wirtschaftlichkeit von Krankenhausaufenthalten zu überprüfen.

Für die Prüfung von Notwendigkeit und Dauer eines Krankenhausaufenthaltes ist in den §§ 275 ff. SGB V allerdings ein eigenes gesetzlich geregeltes Verfahren vorgesehen, welches ausschließlich vom Medizinischen Dienst der Krankenversicherung im Auftrag einer Krankenkasse durchzuführen ist.

Soweit die Qualität und Wirtschaftlichkeit der stationären Behandlung überprüft werden soll, gibt es dafür in § 113 SGB V eine spezielle Vorschrift. Derartige Qualitäts- und Wirtschaftlichkeitsprüfungen können nur gemeinsam von den Landesverbänden der Krankenkassen, den Verbänden der Ersatzkassen und dem Landesausschuss des Verbandes der privaten Krankenversicherung durch einvernehmlich mit dem Krankenhausträger bestellte Prüfer vorgenommen werden. Einzelne Krankenkassen sind dazu nicht befugt.

In beiden Fällen ist eine Beteiligung der Patienten nicht vorgesehen. Sie kann auch nicht durch eine Einwilligung des Patienten herbeigeführt werden. Öffentliche Stellen wie die Krankenkasse können die Verarbeitung personenbezogener Daten dann nicht auf eine Einwilligung stützen, wenn sie damit über den ihr gesetzlich zugewiesenen Aufgabenbereich hinausgehen würden. Diese Aufgabenzuweisung steht nicht zur Disposition des betroffenen Bürgers, oder der beteiligten öffentlichen Stelle.

Selbstverständlich steht es der Krankenkasse frei, ihre Versicherten allgemein nach der Zufriedenheit mit der medizinischen Behandlung zu befragen. Ein Personenbezug ist dabei allerdings nicht erforderlich, so dass für diese Zwecke anonyme Fragebögen verwendet werden sollten.

Krankenkassen dürfen bei Versicherten auch mit deren Einwilligung dann keine Informationen über einen Krankenhausaufenthalt erheben, wenn damit die gesetzlichen Vorschriften des SGB V zur Prüfung von Notwendigkeit, Dauer, Qualität und Wirtschaftlichkeit des Aufenthaltes umgangen werden.

### 8.1.3.2 "Wer hat Sie eigentlich behandelt?"

*Die Kassenärztliche Vereinigung Brandenburg (KVBB) hatte erhebliche Zweifel, ob ein zur ambulanten Behandlung ermächtigter Krankenhausarzt die von ihm abgerechneten Leistungen tatsächlich persönlich erbracht hat oder unerlaubterweise durch ihm unterstelltes Krankenhauspersonal hat erbringen lassen. Um dies festzustellen, befragte sie die Patienten.*

In dem von der KVBB verwendeten erläuternden Anschreiben zum Fragebogen wies sie die Patienten einerseits darauf hin, dass eine Verpflichtung zur Beantwortung der Fragen nicht bestehe. Andererseits wurden die Patienten darauf aufmerksam gemacht, dass es sich um eine Zeugenbefragung nach § 21 des Zehnten Buches des Sozialgesetzbuchs (SGB X) handelte und die Beantwortung der Fragen eine staatsbürgerliche Pflicht sei.

Nach § 285 Abs. 1 Nr. 2 SGB V darf die KVBB zur Überprüfung der Zulässigkeit und Richtigkeit der Abrechnungen personenbezogene Daten der Ärzte erheben und speichern, soweit dies zur Erfüllung dieser Aufgabe erforderlich ist. Ergeben sich aus den der KVBB übermittelten Abrechnungsunterlagen Anhaltspunkte, die an der Zulässigkeit und Richtigkeit der Abrechnung Zweifel lassen, so kann die KVBB auch Daten erheben, die über die eigentlichen Abrechnungsdaten hinausgehen. Im vorliegenden Fall bestanden solche Zweifel, sodass gegen eine weitergehende Erhebung personenbezogener Daten des Arztes keine grundsätzlichen Bedenken bestanden.

Die Datenerhebung bei den Versicherten setzt zusätzlich voraus, dass eine Erhebung personenbezogener Daten bei anderen Personen oder Stellen erlaubt ist. Angesichts der Interessenlage bei der Überprüfung der Abrechnungen wäre eine vorrangig zu prüfende Datenerhebung beim Arzt selbst nicht Erfolg versprechend, sodass wir davon ausgegangen sind, dass die Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht. Darüber hinaus bestanden angesichts des hohen öffentlichen Interesses an der Richtigkeit vertragsärztlicher Abrechnungen und vor dem Hintergrund der Vorgeschichte des konkreten Falles auch keine Anhaltspunkte für überwiegende schutzwürdige Interessen des Arztes.

Die Erhebung von Daten der Versicherten hielten wir im vorliegenden Fall nach § 285 Abs. 2 in Verbindung mit § 83 Abs. 2 SGB V für zulässig. Danach darf die KVBB personenbezogene Daten der Versicherten dann erheben und speichern, wenn dies u. a. zur Überprüfung der Abrechnungen auf Rechtmäßigkeit durch Plausibilitätskontrollen erforderlich ist.

Die Frage, ob ein zur ambulanten Versorgung ermächtigter Krankenhausarzt die Leistungen tatsächlich persönlich erbracht hat, kann letztlich nur vom sonstigen Krankenhauspersonal oder den Versicherten hinreichend beantwortet werden. Da es angesichts der Stellung des Arztes und der Interessenlage im vorliegenden Fall wenig wahrscheinlich war, dass die Befragung des ihm unterstellten Krankenhauspersonals weitere Erkenntnisse bringt, bestanden gegen die Erforderlichkeit, versichertenbezogene Daten zu erheben, keine grundsätzlichen datenschutzrechtlichen Bedenken.

Irreführend war allerdings das von der KVBB verwendete Anschreiben. Die Befragung von Versicherten ist zwar verwaltungsverfahrensmäßig als Zeugenvernehmung anzusehen. Die damit verbundene Erhebung versichertenbezogener Daten kann allerdings nicht auf die entsprechende Vorschrift (§ 21 SGB X) gestützt werden, da sie keine Befugnis zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten enthält.

Die KVBB hat das Anschreiben aufgrund unserer Hinweise verändert. Die Versicherten werden nunmehr darüber unterrichtet, dass und warum die KVBB ihre Daten verarbeiten darf. Außerdem werden die Versicherten nunmehr deutlich darauf hingewiesen, dass die Angabe ihrer personenbezogenen Daten im vorliegenden Fall freiwillig ist. Die Aussage, dass die Versicherten eine "wichtige staatsbürgerliche Pflicht" erfüllen, wurde gestrichen. Schließlich weist die KVBB nunmehr darauf hin, dass den Versicherten auch im Falle der Nicht-Beantwortung keine Nachteile bei der medizinischen Behandlung oder finanzieller Art entstehen.

Die Kassenärztliche Vereinigung darf bei Zweifeln an der Plausibilität von Abrechnungen auf freiwilliger Basis Versicherte befragen. Die Befragung der Patienten muss die Ausnahme sein und darf erst dann durchgeführt werden, wenn andere Formen der Sachverhaltsermittlung ausscheiden.

## 8.2 **Gesundheit**

### **Neun Gebote der Telemedizin**

*Durch elektronische Kommunikation und den dadurch einfacher möglichen Austausch von Patientendaten sollen künftig einerseits die Qualität im Gesundheitswesen gefördert, andererseits Kosten gesenkt werden. Hierzu wurden bereits unterschiedliche Projekte realisiert: Die Patienten begleitende Dokumentation (PaDok) enthält den Arztbefund, die Überweisung, die Einweisung, die Quartalsrechnung, das Rezept sowie die Fallakte jeweils in elektronischer Form. Die elektronische Patientenakte (EPA) gibt Auskunft über alle relevanten Daten einer Krankengeschichte.*

Die ärztliche Schweigepflicht zwischen den einzelnen Ärzten gilt auch in der Telemedizin. Eine Befugnis zur elektronischen Übermittlung personenbezogener Patientendaten kann sich nur aus Spezialgesetzen (z. B. Krebsregistergesetz, Infektionsschutzgesetz, Fünftes Sozialgesetzbuch, Landeskrankenhausgesetz), dem Behandlungsvertrag oder einer konkreten, schriftlichen Einwilligung des Patienten ergeben.

Hingegen kann die beim Arztbesuch aus Abrechnungsgründen erforderliche Vorlage der Krankenversichertenkarte nicht den Abruf von Patientendaten rechtfertigen. Diese Chipkarte enthält ausschließlich Daten zur Krankenversicherung und keine Informationen über Arztbesuche, Behandlungen oder Krankheiten eines Patienten.

Die Telemedizin basiert auf Verfahren, die entweder mittels einer dezentralen Datenhaltung zwischen einzelnen Ärzten, von einer zentralen, gemeinsamen Daten verarbeitenden Stelle oder durch eine Mischform realisiert werden. Sie bedürfen aufgrund der hohen Sensibilität der Gesundheitsdaten eines besonderen Schutzes.

Die dabei auftretenden komplexen Fragen sind von einer Arbeitsgruppe "Telemedizin" der Datenschutzbeauftragten des Bundes und der Länder untersucht worden, an der auch eine Mitarbeiterin des Landesbeauftragten teilgenommen hat. Die Ergebnisse dieser Untersuchung sind in einem Arbeitspapier "Datenschutz und Telemedizin – Anforderungen an Medizinetze" zusammengefasst, das die Konferenz der Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.<sup>49</sup>

Danach müssen Medizinetze folgende Anforderungen erfüllen:

1. Vertraulichkeit: Nur durch eine Verschlüsselung mittels kryptografischer Verfahren ist gewährleistet, dass ausschließlich Befugte patientenbezogene Daten zur Kenntnis nehmen können.
2. Authentizität: Eine elektronische Signatur und ein Zeitstempel gewährleisten, dass das Dokument einem Urheber bzw. Verantwortlichen zurechenbar ist.
3. Integrität: Die elektronische Signatur bescheinigt gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokuments.
4. Verfügbarkeit: Bei der zentralen Datenhaltung ist ein schneller Zugriff auf Daten gegeben. Bei der dezentralen Datenhaltung hängt die Verfügbarkeit von den beteiligten (Sub-) Systemen ab, insbesondere den Praxiszeiten und der technischen Kompatibilität.
5. Revisionsfähigkeit: Die elektronische Signatur gewährleistet, dass die Verarbeitungsprozesse lückenlos nachvollzogen werden können. Denn der Inhalt eines signierten Dokuments kann nicht ohne Verletzung der Signatur nachträglich verändert werden. Die Übermittlungs- und Lesvorgänge sind durch eine manipulationssichere Protokollierung zu dokumentieren.
6. Validität: Die Sicherstellung einer angemessenen Qualität der Daten (z. B. der Bildauflösung) hängt von Hard- und Softwarekomponenten ab.
7. Rechtssicherheit: Die beweiskräftige, nachweisbare Verursachung eines Datenverarbeitungsvorganges wird durch eine qualifizierte elektronische Signatur bewiesen.
8. Die Nicht-Abstreitbarkeit des Sendens und Empfangens – v. a. in der dezentralen Datenhaltung – muss durch ein Quittungsverfahren gewährleistet werden. Empfänger und Sender bestätigen sich jeweils, dass das Dokument vom Sender stammt und der Empfänger genau dieses Dokument erhalten hat.
9. Nutzungsfestlegung: Ein systemweites oder definiertes Berechtigungskonzept muss den Nutzerkreis und die abgestuften Nutzerrechte hinsichtlich der übermittelten Daten festlegen.

Datenflüsse in der Telemedizin unterliegen der ärztlichen Schweigepflicht und bedürfen – ohne Einwilligung des Patienten – einer Rechtsgrundlage. Sie müssen u. a. den Grundsätzen der Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit, Revisionsfähigkeit und Rechtssicherheit gerecht werden.

## 9 Wirtschaft

### 9.1 Gewerbedaten im Internet

*Eine Gemeinde beabsichtigte, den Namen, die betriebliche Anschrift und die angezeigte Tätigkeit aller in einem Ort gemeldeten Gewerbetreibenden im Internet zu veröffentlichen. Statt deren Einwilligung einzuholen, wollte die Gemeinde, das Vorhaben im Amtsblatt bekannt geben und dort den Betroffenen die Möglichkeit einräumen, innerhalb einer festgelegten Frist zu widersprechen.*

Die Gewerbeordnung erlaubt in § 14 Abs. 8 die Weitergabe von Grunddaten der Gewerbetreibenden nur, wenn der Auskunftsbegehrende ein berechtigtes Interesse glaubhaft macht. Insofern ist die Rechtslage ähnlich wie beim Grundbuch.<sup>50</sup>

Da aus dem Internet jeder Daten abrufen kann, ohne hierfür Gründe darlegen zu müssen, hat die Behörde keine Möglichkeit festzustellen, ob diese rechtlichen Voraussetzungen tatsächlich erfüllt sind. Auch die von der Gemeinde vorgeschlagene Einräumung eines Widerspruchsrechts im Rahmen der Veröffentlichung des Vorhabens ist von der Vorschrift nicht gedeckt. Dem Recht des Gewerbetreibenden wird nur durch eine informierte Einwilligung ausreichend Rechnung getragen. Die Betroffenen müssen vorher über die mit dem Internet verbundenen Risiken aufgeklärt werden (z. B. mögliche Veränderung, Fälschung und Manipulation der Daten).

Eine Veröffentlichung der Grunddaten aus der Gewerbeanzeige im Internet ist nur mit einer informierten Einwilligung der Gewerbetreibenden zulässig.

## 9.2 Veröffentlichung von Mitgliederdaten der Industrie- und Handelskammer im Internet

*Eine Industrie- und Handelskammer unterrichtete uns über ihr Vorhaben, Mitgliederdaten der Unternehmen, die im Handelsregister eingetragen sind, im Internet zu veröffentlichen.*

Die Veröffentlichung z. B. von Stammkapital, dem Unternehmensgegenstand sowie Name und Anschrift der Unternehmen stellt eine Datenübermittlung an nicht-öffentliche Stellen dar. Das Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern lässt zwar eine Datenübermittlung in diesem Umfang nicht zu. Da aber sämtliche zu veröffentlichenden Daten der Mitglieder der Industrie- und Handelskammer den in Zeitungsinserten üblichen amtlichen Bekanntmachungen der Handelsregistereintragungen entsprechen und Ende 2001 die rechtlichen Voraussetzungen dafür geschaffen worden sind, dass eine "Online-Einsicht" in die entsprechenden staatlichen Register für jedermann möglich ist, bestehen auch gegen ein von der Industrie- und Handelskammer betriebenes Online-Abfrageverfahren keine Bedenken.

Eine Befugnis zur Veröffentlichung der Mitgliederdaten besteht nach den §§ 16 Abs. 1 Buchst. b, 13 Abs. 2 Satz 1 Buchst. f Brandenburgisches Datenschutzgesetz i. V. m. § 9a Handelsgesetzbuch. Der Online-Abfrage für jedermann ist nur "zu Informationszwecken" zulässig. Auf diese Weise soll verhindert werden, dass gewerbliche Unternehmen massenhaft Handelsregisterdaten abrufen, um private Parallelregister aufzubauen.

Die Industrie- und Handelskammer muss sicherstellen und durch Stichproben überprüfen, dass die Recherche nach den Namen handelnder Personen ausgeschlossen bleibt, da das Register nur Unternehmensdaten, nicht jedoch die Unternehmensbeteiligung einzelner natürlicher Personen abbilden soll. Dazu sind die Abfrage zu protokollieren.

Die Industrie- und Handelskammer darf die Mitgliederdaten, die mit den Handelsregistereintragungen identisch sind, im Internet veröffentlichen. Durch technisch-organisatorische Maßnahmen ist sicherzustellen, dass aus einem reinen Unternehmens- kein Personenregister wird.

## 10 Finanzen

### Beharrlichkeit führt zum Erfolg

*Im letzten Tätigkeitsbericht schilderten wir einen Fall, in dem die Finanzbehörde einem Steuerpflichtigen die Einsicht in seine eigene Steuerakte mit Verweis auf die Abgabenordnung verweigerte<sup>51</sup>. Wir wiesen darauf hin, dass eine Offenlegung zu erfolgen hat und forderten das Finanzamt auf, die Einsicht zu gewähren. Zur Klärung des Sachverhalts hatten wir weitere Einzelheiten aus der Steuerakte des Petenten angefordert. Die Behörde entgegnete, das Steuergeheimnis stehe einer solchen Auskunft an den Landesbeauftragten entgegen.*

Diese Rechtsauffassung war unzutreffend. Der Landesbeauftragte hat nach § 24 Abs. 2 Satz 1 Nr. 2 i. V. m. Abs. 6 Bundesdatenschutzgesetz auch ein Kontrollrecht in Bezug auf die dem Steuergeheimnis nach § 30 Abgabenordnung unterliegenden Daten.

Die hier anwendbaren materiell-rechtlichen Bestimmungen des Brandenburgischen Datenschutzgesetzes gewähren den Betroffenen ein Auskunfts- bzw. Einsichtsrecht über die zu ihrer Person von öffentlichen Stellen gespeicherten Daten. Das Finanzamt ist dazu verpflichtet, dem Landesbeauftragten Einzelheiten zum Sachverhalt mitzuteilen, da dieser die Einhaltung des Brandenburgischen Datenschutzgesetzes ansonsten nicht zu kontrollieren in der Lage ist.

Nach erneuter Prüfung des Sachverhalts hat das Finanzamt dem Steuerpflichtigen mittlerweile die gewünschte Akteneinsicht gewährt. Das Grundsatzproblem bleibt allerdings ungelöst. In vergleichbaren Fällen hat das Ministerium der Finanzen seine Auffassung bekräftigt, dass dem Steuerschuldner kein Recht auf Einsicht in die eigene Akte zustehe. Diese Auffassung steht im Gegensatz zum Grundrecht auf Einsicht in seine persönlichen Daten nach der Landesverfassung, das auch bei der Anwendung von Bundesrecht zu berücksichtigen ist.<sup>52</sup>

Das Steuergeheimnis steht der Kontrolle des Umgangs der Finanzämter mit Steuerdaten durch den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht nicht entgegen. Der Bundesgesetzgeber bleibt aufgefordert, das Recht des Steuerbürgers auf Einsicht in die eigene Steuerakte zur Klarstellung auch in der Abgabenordnung zu verankern.

<sup>51</sup> Tätigkeitsbericht 2001, A 10.1

<sup>52</sup> vgl. Verfassungsgericht des Landes Brandenburg, Beschl. vom 25.9.2002 – VfGBbg 79/02

## Teil B

### **Akteneinsicht und Informationszugang**

Die Verfassung des Landes Brandenburg beschränkt sich nicht darauf, dem Einzelnen ein Grundrecht auf Schutz seiner personenbezogenen Daten zu garantieren, sondern sieht darüber hinaus auch ein Grundrecht auf Akteneinsicht und Informationszugang vor. Auch wenn der Tätigkeitsbericht des Landesbeauftragten bisher seinen Schwerpunkt immer noch im Datenschutzbereich hat, nimmt die Bedeutung des Informationszugangsrechts ständig zu. Dabei ist das Land Brandenburg, das ursprünglich Vorreiter der deutschen Informationszugangsgesetzgebung war, stark abhängig von Entwicklungen auf europäischer und bundesstaatlicher Ebene, sodass es sinnvoll erscheint, auch Entwicklungen auf diesen Ebenen in den Blick zu nehmen.

## **1 Entwicklung des Informationszugangsrechts**

### **1.1 Europa**

Im Anschluss an ihr Grünbuch "Informationen des öffentlichen Sektors – eine Schlüsselressource für Europa", zu dem der Landesbeauftragte 1999 Stellung genommen hatte<sup>53</sup>, hat die Europäische Kommission im Berichtszeitraum den Entwurf einer Richtlinie über die Weiterverwendung und kommerzielle Verwertung von Dokumenten des öffentlichen Sektors vorgelegt<sup>54</sup>. Dieser Vorschlag soll die Bedingungen für den Zugang zu Dokumenten des öffentlichen Sektors harmonisieren, um gleiche Wettbewerbsbedingungen für Informationsanbieter auf dem europäischen Binnenmarkt zu gewährleisten. Der Richtlinienvorschlag nimmt ausdrücklich solche Dokumente von seinem Anwendungsbereich aus, die personenbezogene Daten enthalten, es sei denn, dass deren Weiterverwendung nach dem Gemeinschaftsrecht über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre und in entsprechenden nationalen Gesetzen zulässig ist. Hinsichtlich der Dokumente und Informationen des öffentlichen Sektors, die keinen Personenbezug aufweisen (z. B. Geoinformationen), ergibt sich eine mögliche Kollision mit dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz.

---

<sup>53</sup> Tätigkeitsbericht 1999, B 1.1

<sup>54</sup> KOM (2002) 207 endg.; BR-Drs. 664/02

Der Richtlinienvorschlag eröffnet den öffentlichen Stellen die Möglichkeit, durch die Erhebung von Gebühren für den Zugang zu Dokumenten für kommerzielle Zwecke einen "angemessenen Gewinn" zu erzielen. An dieser Stelle wird deutlich, dass die Europäische Kommission mit ihrem Vorschlag einen grundlegend anderen Ansatz verfolgt als die Verfassung des Landes Brandenburg und das auf ihrer Grundlage beschlossene Akteneinsichtsgesetz. Während in Brandenburg der Zugang zu Informationen des öffentlichen Sektors eine grundrechtlich gesicherte Voraussetzung zur politischen Mitgestaltung ist, deren Ausübung die Verwaltung durch die Erhebung von Gewinn orientierten oder prohibitiven Gebühren nicht behindern darf, ließe die geplante Europäische Richtlinie den Behörden der Mitgliedstaaten einen größeren Spielraum bei der Bemessung der Gebühren. Unzulässig wären nur solche Gebühren, die der Verwaltung zu einem unangemessenen Gewinn verhelfen würden.

Hier zeichnet sich ein Konflikt ab, der zu Gunsten des grundrechtsfreundlichen Verständnisses von Informationsfreiheit, wie es in Brandenburg von der Verfassung vorgegeben ist, gelöst werden sollte. Das nachvollziehbare Bestreben der öffentlichen Verwaltung, ihren erheblichen Finanzbedarf durch gewinnbringende Vermarktung von Informationen ohne Personenbezug zu decken, darf das Grundrecht auf allgemeinen Informationszugang nicht durch eine prohibitive Gebührengestaltung ad absurdum führen. Zwar könnte erwogen werden, für den Fall höhere Gebühren zuzulassen, in dem die Informationen für kommerzielle Zwecke weiter verwendet werden sollen. Dann allerdings geriete der Grundsatz des voraussetzungslosen und nicht begründungsbedürftigen Informationszugangs in Gefahr.

Auch im Bereich des Zugangs zu Umweltinformationen stehen Änderungen des Gemeinschaftsrechts bevor, die Auswirkungen auf Brandenburg haben werden. So ist vor kurzem die Richtlinie des Europäischen Parlaments und des Rates über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der ersten Umweltinformationsrichtlinie (90/313/EWG) in Kraft getreten<sup>55</sup>. Damit wird die Europäische Umweltinformationsrichtlinie an die Vorgaben der Konvention von Aarhus<sup>56</sup> angepasst. Insbesondere soll die neue Umweltinformationsrichtlinie die Voraussetzungen dafür schaffen, dass Umweltinformationen möglichst umfassend und systematisch in der Öffentlichkeit z. B. über das Internet verbreitet werden.

---

<sup>55</sup> Richtlinie 2003/4/EG, ABIEU L 41/26 vom 14.2.2003

<sup>56</sup> dazu siehe Tätigkeitsbericht 1998, B 1.1

Der europäische Gesetzgeber beschleunigt damit in diesem Bereich die Entwicklung von der lediglich passiven Transparenz, bei der die Bürgerinnen und Bürger jeweils auf die Offenlegung von Informationen dringen müssen, hin zu einer aktiven Transparenz, die die Verwaltung zur Veröffentlichung von Umweltinformationen von "Amts wegen" verpflichtet. Zu den Umweltinformationen, die unter die Richtlinie fallen, gehören auch Angaben über Kontaminierungen der Nahrungskette. Die neue Umweltinformationsrichtlinie geht vom Grundsatz des kostenlosen Zugangs zu Umweltinformationen aus. Insbesondere müssen die Nutzung öffentlicher Listen und Verzeichnisse und die Einsichtnahme in die gewünschten Informationen an Ort und Stelle gebührenfrei sein. Kosten dürfen nur für das Reproduzieren des beantragten Materials (Herstellen von Fotokopien) verlangt werden und dürfen die tatsächlichen Kosten der Reproduktion nicht übersteigen. Auch müssen die Mitgliedstaaten gewährleisten, dass die Umweltinformation aktuell, vollständig und vergleichbar sind. Vor dem Hintergrund, dass der Begriff "Umweltinformation" nach Gemeinschaftsrecht weit auszulegen ist, wird nach einer Umsetzung dieser Richtlinie in deutsches Recht, die innerhalb von zwei Jahren zu erfolgen hat, auch in Brandenburg der Zugang zu manchen Verwaltungsvorgängen erleichtert werden, selbst wenn sie nicht von einem Umweltamt geführt werden.

## **1.2 Bundesrepublik Deutschland**

Auf Bundesebene scheiterte im Berichtszeitraum das Vorhaben eines Informationsfreiheitsgesetzes für die Bundesverwaltung am Widerstand einzelner Bundesministerien, die für ihren Bereich Blankettausnahmen verlangten, und einzelner Wirtschaftsverbände, die eine Aushöhlung von Betriebs- und Geschäftsgeheimnissen befürchteten. Es bleibt sehr zu hoffen, dass die Absichtserklärung der Koalitionsparteien nach der Bundestagswahl erneut ein Informationsfreiheitsgesetz für die Bundesbehörden in den Gesetzgebungsprozess einzubringen, bald in die Tat umgesetzt wird. Das gilt auch für das vor der Bundestagswahl am Widerstand des Bundesrates gescheiterte Verbraucherinformationsgesetz, das mehr Transparenz auch im Bereich der Privatwirtschaft sicherstellen soll. Die wiederholten Skandale im Bereich der Futtermittelherstellung haben deutlich gemacht, dass der Mangel an gezielten Informationen über die Verursacher von gesundheitsgefährdenden Belastungen in der Nahrungsmittelkette dazu führt, dass letztlich alle – und damit auch unbeteiligte Landwirte – unter dem wachsenden Misstrauen der Verbraucher zu leiden haben.

Wir haben bereits im vergangenen Jahr darüber berichtet, welche rechtlichen Schwierigkeiten bestehen, wenn die Öffentlichkeit über den Ausbruch von Tierseuchen informiert werden soll.<sup>57</sup> Es ist wünschenswert, dass die Befugnis der zuständigen Stellen, bei konkreter Gesundheitsgefährdung herstellerbezogene Warnungen zu veröffentlichen, eindeutig gesetzlich geregelt wird.

### 1.3 Brandenburg

Der Landesbeauftragte für das Recht auf Akteneinsicht hatte bereits Anfang 2001 detaillierte Vorschläge zur Weiterentwicklung und Vereinfachung des Akteneinsichts- und Informationszugangsgesetzes gemacht<sup>58</sup>. Nach Erörterung dieser Vorschläge im Innenausschuss hat der Landtag in seinem Beschluss vom 18. April 2002<sup>59</sup> die Landesregierung aufgefordert, bis zum 31. August 2002 einen Gesetzentwurf zur Änderung des Akteneinsichts- und Informationszugangsgesetzes mit folgender Maßgabe vorzulegen:

- "Für die Bearbeitung des Antrages auf Akteneinsicht ist eine Frist zu bestimmen. Dabei soll die Möglichkeit der Erteilung eines Zwischenbescheides bestehen. Für die Fristbestimmung ist eine Orientierung an der Frist für die Bearbeitung von Petitionen gemäß § 21 der Gemeindeordnung anzustreben."
- "Für den Fall der Ablehnung des Antrages auf Akteneinsicht soll der Antragsteller in dem Ablehnungsbescheid auf das Recht, den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht anzurufen, hingewiesen werden."

Zwar hat das Ministerium des Innern uns einen Gesetzentwurf zur Umsetzung des Landtagsbeschlusses im Juni 2002 zur Stellungnahme zugeleitet und vor Beginn der Ressortabstimmung einen Teil unserer Änderungsvorschläge berücksichtigt. Zu einem Beschluss der Landesregierung ist es jedoch bisher nicht gekommen, so dass auch die vom Landtag gesetzte Frist inzwischen deutlich überschritten worden ist.

Stattdessen erwägt das Innenministerium Presseberichten zufolge, das "bundesweit als besonders weit gehend"<sup>60</sup> geltende Akteneinsichtsgesetz einzuschränken. In Wirklichkeit ist das Brandenburgische Akteneinsichts- und Informationszugangsgesetz im Vergleich zu der entspre-

---

<sup>57</sup> Tätigkeitsbericht 2001, A 9.2

<sup>58</sup> Tätigkeitsbericht 2000, B 4

<sup>59</sup> Drs. 3/4034-B

<sup>60</sup> Potsdamer Neueste Nachrichten vom 24.1.2003

chenden Gesetzgebung anderer Bundesländer inzwischen das restriktivste seiner Art. Die vom Innenministerium angestrebte Entlastung der Verwaltungsbehörden kann am besten durch die Umsetzung der Vorschläge erreicht werden, die der Landesbeauftragte zur Novellierung gemacht hat.

Neue Impulse für das Informationszugangsrecht kommen gegenwärtig insbesondere aus Europa. Die Harmonisierung der Verwertungsbedingungen für Dokumente der öffentlichen Verwaltung und die weitere Stärkung der Rechte der Öffentlichkeit auf Zugang zu Umweltinformationen kann auch in Deutschland den Zugang zu Verwaltungsinformationen erleichtern.

Es ist zu hoffen, dass in absehbarer Zeit der Bundesgesetzgeber ein Informationsfreiheitsgesetz für die Bundesbehörden verabschiedet. Die Landesregierung ist bisher der Aufforderung des Landtages nicht nachgekommen, das Akteneinsichts- und Informationszugangsgesetz in einem wesentlichen Punkt zu Gunsten der Bürgerinnen und Bürger zu verändern.

## 1.4 Korruptionsbekämpfung durch Informationsfreiheit

*Immer wieder erkundigen sich Bürgerinnen und Bürger, wie sie mit Hilfe des Akteneinsichts- und Informationszugangsgesetzes Informationen über öffentliche Auftragsvergaben erhalten können. Von Interesse sind dabei sowohl kleinere Beschaffungen einer Gemeinde, als auch größere Aufträge an Baufirmen.*

Die Rechtsgrundlage für die Durchführung eines Vergabeverfahrens richtet sich nach der Auftragssumme. Werden bestimmte Schwellenwerte erreicht, gilt das Bundesgesetz gegen Wettbewerbsbeschränkungen bzw. die Vergabeverordnung, in denen auch nach dem Abschluss des Verfahrens strenge Geheimhaltungsvorschriften vorgesehen sind. Sie gehen dem Akteneinsichts- und Informationszugangsgesetz vor und schließen einen Informationszugang aus. Unterhalb der Schwellenwerte kommen die Verdingungsordnungen zum Tragen, deren Geheimhaltungsvorschriften die Zugangsrechte aus dem Akteneinsichts- und Informationszugangsgesetz zwar nicht außer Kraft setzen. Dennoch scheitern Anträge auf Informationszugang hier häufig daran, dass das Akteneinsichts- und Informationszugangsgesetz unternehmensbezogene Daten derart weit gehend schützt, dass nach einer Anonymisierung kaum brauchbare Informationen übrig bleiben. Für eine Bürgerin, die beispielsweise nachvollziehen möchte, wie es kommt, dass ein und dieselbe Firma sämtliche Aufträge zur Straßensanierung in einer Region erhält,

bleiben die Aktendeckel also faktisch geschlossen.

Ziel des Akteneinsichts- und Informationszugangsgesetzes ist die Stärkung der politischen Mitgestaltung durch die Bürgerinnen und Bürger. Dazu gehört für sie auch die Notwendigkeit, Entscheidungen der Behörden über öffentliche Aufträge und damit über die Verwendung von Steuergeldern nachvollziehen zu können. Die zuständigen Gesetzgeber haben mit den strengen Geheimhaltungsvorschriften aber das Ziel, laufende Vergabeverfahren sowie Betriebs- und Geschäftsgeheimnisse von Unternehmen zu schützen, bei weitem übertroffen. Die aktuellen Korruptions- und Spendenskandale belegen hingegen die Notwendigkeit transparenter Strukturen.

Die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland hat daher gefordert, die Informationsfreiheitsgesetze und die Vergabevorschriften so zu gestalten, dass die öffentliche Auftragsvergabe transparent und für die Allgemeinheit kontrollierbar wird<sup>61</sup>:

- Informationsfreiheit muss grundlegender Bestandteil der Vergaberegungen sein.
- Im Hinblick auf das öffentliche Interesse sind die Gründe für die Vergabeentscheidung so weit wie möglich offen zu legen. Unterlagen, die keine Betriebs- oder Geschäftsgeheimnisse enthalten und deren Offenlegung den Entscheidungsprozess nicht beeinträchtigt, zum Beispiel die Niederschrift über die Angebotseröffnung oder die Dokumentation der Auftragsvergabe selbst, sind zugänglich zu machen.
- Das öffentliche Interesse an einer transparenten Auftragsvergabe ist gegenüber dem Interesse der bietenden Unternehmen am Schutz ihrer Betriebs- und Geschäftsgeheimnisse stärker zu gewichten.

Informationsfreiheitsgesetze und die Vergabevorschriften sind dringend so zu gestalten, dass die öffentliche Auftragsvergabe transparent und für die Allgemeinheit kontrollierbar wird.

## 2 Umsetzung des AIG

### 2.1 Eingaben und Anfragen beim Landesbeauftragten

*Beschwerden von Bürgerinnen und Bürgern sowie Anfragen von Verwaltungen beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht spiegeln zumindest teilweise wider, wie sich die Nutzung des Rechts auf Informationszugang in Brandenburg entwickelt hat. Welche Erkenntnisse lassen sich aus den Fällen, die im abgelaufenen Berichtsjahr an uns herangetragen wurden, ableiten?*

Während die Nachfrage brandenburgischer Behörden nach Beratung im Jahre 2002 konstant blieb, war quantitativ eine leichte Rückläufigkeit der bei uns eingelegten Beschwerden von Bürgerinnen und Bürgern zu verzeichnen. Gleichzeitig lagen den Eingaben zunehmend komplizierte Fallkonstellationen zu Grunde, die im Vergleich zu den Vorjahren eine deutlich aufwändigere Ermittlung des Sachverhalts sowie eine ausführlichere rechtliche Prüfung notwendig machten. Dies könnte ein Indiz dafür sein, dass sich die Verwaltung in den meisten Fällen eine gewisse Routine im Umgang mit dem Akteneinsichts- und Informationszugangsgesetz angeeignet hat und Konflikte vorwiegend dort auftreten, wo dessen Anwendung – auch in Abgrenzung zu anderen Rechtsgrundlagen für den Informationszugang – tatsächlich und rechtlich schwierig ist.

Wie bereits in den Vorjahren lagen die Schwerpunkte der Anträge im Baubereich sowie im Kommunalrecht. Auffallend war eine Häufung der Anfragen und Eingaben zu Einsichtsbegehren, die zum Ziel hatten, die Erfolgsaussichten für Schadensersatzforderungen gegenüber der öffentlichen Hand zu beurteilen.

Die Mehrzahl der Anträge auf Akteneinsicht, mit denen wir befasst waren, wurde im vergangenen Berichtszeitraum wieder bei den brandenburgischen Gemeinden, Ämtern und Städten gestellt. Auch Zweckverbände waren Adressaten von Einsichtsbegehren, allerdings waren Anträge, die dort gestellt wurden, zumeist nach dem Umweltinformationsgesetz zu bearbeiten.

In über der Hälfte aller von uns bearbeiteten Fälle wurde nach Intervention durch den Landesbeauftragten der zuvor abgelehnte Informationszugang gewährt. Weniger als einem Fünftel der Petentinnen und Petenten mussten wir nach der rechtlichen Prüfung des Sachverhalts mitteilen, dass gesetzliche Ausschlussgründe einer Akteneinsicht entgegenstehen. Dabei handelte es sich zumeist um einen überwiegenden öffentlichen

Schutzbedarf oder um Unternehmensdaten. Nur in einem einzigen Fall standen personenbezogene Daten dem Informationszugang entgegen. In einem Fall wurde der Informationszugang zu Unrecht abgelehnt. Dies haben wir der Akten führenden Stelle gegenüber beanstandet (siehe B 2.2).

Nachdem im Vorjahr die Akteneinsichts- und Informationsgebührenordnung in Kraft getreten war und bereits erste Beschwerden über die Kostenerhebung für den Informationszugang eingegangen sind, hat sich diese Entwicklung im Jahre 2002 nicht fortgesetzt. Wir gehen daher davon aus, dass die Verwaltungen in der Kostenfrage überwiegend angemessene Lösungen finden und keine überhöhten Kosten für die Akteneinsicht verlangen.

Während die Anwendung des Akteneinsichts- und Informationszugangsgesetzes für die brandenburgische Verwaltung in der Regel zum Alltag geworden ist, sind in Einzelfällen zunehmend komplizierte Sachverhalte zu entscheiden. Insgesamt ist jedoch ein pragmatischer Umgang mit dem Recht auf Informationszugang festzustellen.

## **2.2 Akteneinsicht auch bei Schadensersatzforderungen**

*Nachdem eine Überschwemmung Schäden auf einem Grundstück verursacht hatte, vermutete der Grundstückseigentümer die mangelnde Reinigung der Regenentwässerungsanlagen durch die Stadt als Ursache. Er wollte prüfen, ob Schadensersatzforderungen realistische Erfolgsaussichten hätten und beantragte Einsicht in die entsprechenden Unterlagen. Die Stadt lehnte den Antrag unter anderem mit der Begründung ab, dass aufgrund der Schadensersatzforderungen kein Einsichtsanspruch bestehe. Da es bei den Reinigungsarbeiten nicht um eine hoheitliche Aufgabe gehe und es keinen Anspruch auf die Reinigung der Entwässerungsanlagen gebe, bestehe, so die Stadt, auch kein Anspruch auf Akteneinsicht. Außerdem sei die Behörde nicht verpflichtet, Beweise für die gegnerische Seite vorzulegen.*

Das Akteneinsichts- und Informationszugangsgesetz gewährt den Anspruch auf Akteneinsicht grundsätzlich ohne Voraussetzung. Dies bedeutet, dass der Grund, aus dem Einsicht beantragt wird, unerheblich ist und der Antragsteller nicht danach gefragt werden darf. Sollte der Antragsteller den Antrag von sich aus begründen, hat die Akten führende Stelle dies außer Acht zu lassen. Ausnahmen von der Voraussetzungslosigkeit gelten nur in den eng begrenzten Fällen des § 4 Abs. 2 und § 5

Abs. 2 Nr. 3 Akteneinsichts- und Informationszugangsgesetz, in denen die Behörde zwischen dem Geheimhaltungs- und Offenbarungsinteresse abzuwägen hat. Davon war hier aber nicht auszugehen. Die Tatsache, dass der Grundstückseigentümer prüfen möchte, ob er von der Stadt Schadensersatz fordern kann, darf also bei der Bearbeitung des Antrags auf Akteneinsicht keine Rolle spielen. Somit ist es auch irrelevant, ob der Grundstückseigentümer einen Anspruch auf die Reinigung der Anlagen hat.

Das Akteneinsichts- und Informationszugangsgesetz gilt für alle brandenburgischen Städte und Gemeinden und unterscheidet nicht zwischen hoheitlichen und nicht-hoheitlichen Aufgaben. Die Unterlagen zur Reinigung der Regenentwässerungsanlagen sind lediglich daraufhin zu prüfen, ob sie einem überwiegenden privaten oder öffentlichen Interesse an der Geheimhaltung unterliegen. Sollten beispielsweise personenbezogene Daten von Nachbarn oder schutzbedürftige Informationen über Unternehmen, die mit der Reinigung beauftragt wurden, darin enthalten sein, sind die Betroffenen auf Verlangen des Antragstellers nach der Zustimmung zur Akteneinsicht zu fragen oder die schutzbedürftigen Daten auszusondern und der Rest der Akte offen zu legen.

Die Annahme der Stadt, dass sie nicht verpflichtet sei, dem künftigen Prozessgegner Beweise zu verschaffen, die ihr schaden können, geht ebenfalls fehl. Selbst in Fällen, in denen das Akteneinsichts- und Informationszugangsgesetz nicht zum Tragen kommt, ist schon allein aus rechtsstaatlichen Gründen von einem Recht auf Akteneinsicht auszugehen, wenn ein rechtliches Interesse vorliegt und die Kenntnis des Akteneinhalts Voraussetzung für die wirksame Rechtsverfolgung ist. Unabhängig davon, ob es sich bei der zu Grunde liegenden Aufgabe der Behörde um eine zivil- oder öffentlich-rechtliche Tätigkeit handelt, ist sie in besonderer Weise zur Öffentlichkeit und Rechenschaft für ihre Handlungen verpflichtet.

Da die Stadt an ihrer Verweigerung des Informationszugangs festhielt, stellte der Landesbeauftragte einen Verstoß gegen das Akteneinsichts- und Informationszugangsgesetz fest und beanstandete das Vorgehen der Behörde. Der Landkreis als Kommunalaufsichtsbehörde hat sich unserer Auffassung angeschlossen.

Das Einsichtsinteresse eines Antragstellers ist nach dem Akteneinsichts- und Informationszugangsgesetz grundsätzlich unerheblich und darf von der Behörde nicht erfragt werden. Auch die Absicht, Schadensersatzforderungen gegenüber der Akten führenden Stelle geltend zu machen, steht dem Informationszugang nicht entgegen.

## 2.3 Hinreichende Bestimmtheit eines Antrags auf Akteneinsicht

*Mit der Absicht, einen möglichen Anspruch auf Schadensersatz aufgrund eines Wasserschadens zu prüfen, beantragte die Rechtsanwältin der Anwohnerin einer Ortsdurchfahrt Akteneinsicht in die Unterlagen zu einer Baumaßnahme an der Straße. Die Behörde lehnte die Akteneinsicht unter anderem mit der Begründung ab, der Antrag sei nicht hinreichend bestimmt und die Zusammenstellung der umfangreichen Akten erfordere einen "unbotmäßigen personellen Aufwand", durch den die Behörde in der ordnungsgemäßen Erfüllung ihrer "eigentlichen" öffentlichen Aufgaben beeinträchtigt werden würde. Die Pflicht der Behörde zur Beratung bei der Benennung der für die Einsicht in Frage kommenden Akten entfalle, da es sich um eine offensichtlich rechtskundige Antragstellerin handelt.*

Das Recht auf Akteneinsicht ist in Artikel 21 der Landesverfassung als Grundrecht verankert und wird durch das Akteneinsichts- und Informationszugangsgesetz konkretisiert. Die Anwendung dieses Gesetzes gehört genau wie beispielsweise die Beachtung der Landeshaushaltsordnung oder des Verwaltungsverfahrensgesetzes zu den Aufgaben der öffentlichen Verwaltung in Brandenburg – unabhängig davon, für welche weiteren Fachaufgaben sie zuständig ist. Baubehörden oder Fachämter haben sich daher mit Anträgen auf Informationszugang in derselben Intensität zu befassen wie allgemeine Verwaltungsbehörden.

Die Unterstützungspflicht des § 6 Abs. 1 Akteneinsichts- und Informationszugangsgesetz hat zum Ziel, im Vorfeld der Prüfung eines Antrags auf Akteneinsicht zu klären, um welche Unterlagen es dem Antragsteller geht. Dadurch soll der Behörde die Arbeit und gleichzeitig dem Antragsteller die Eingrenzung der Informationen erleichtert werden. Häufig ist es für Außenstehende aber nur schwer nachzuvollziehen, welche Akten in der Behörde überhaupt geführt werden und welche Ämter über welche Unterlagen verfügen. Die Rechtskundigkeit einer Antragstellerin oder ihre Qualifikation als Rechtsanwältin bedeutet nicht, dass diese sich auch mit der konkreten Aktenführung und internen Arbeitsteilung eines Amtes auskennt. Daher gilt die gesetzliche Unterstützungspflicht ausnahmslos für alle Antragsteller.

Dass ein Antrag auf Akteneinsicht hinreichend bestimmt zu stellen ist, bedeutet aber nicht immer, dass darin die einzelnen Akten genau bezeichnet werden müssen. Verfügt ein Antragsteller – wie im vorliegenden Fall – nur über vage Anhaltspunkte, die es nicht erlauben, die Unterlagen

genauer einzugrenzen, so gilt der Antrag ebenfalls als ausreichend bestimmt. Die Akten führende Stelle sollte aber in jedem Fall im Rahmen der Beratung des Antragstellers über Art und Inhalt der Akten sowie über die internen Zuständigkeiten eventuell beteiligter Ämter informieren.

Das Akteneinsichts- und Informationszugangsgesetz gehört zu den Kernaufgaben aller Behörden. Zwecks hinreichender Bestimmung des Antrags auf Akteneinsicht hat die Behörde den Antragsteller – ohne Ansehen seiner Qualifikation – bereits im Vorfeld zu beraten.

## 2.4 Daten für einen Mietspiegel

*Eine Vereinigung von Mieterinnen und Mietern, die zusammen mit der Stadt und den Vermietern am Zustandekommen eines Mietspiegels beteiligt war, interessierte sich für die konkreten Mietdaten, die der Berechnung der Vergleichsmiete zu Grunde lagen. Die Stadt lehnte den Antrag auf Akteneinsicht mit der Begründung ab, dass die betroffenen Wohnungsgesellschaften einer Einsichtnahme in die unternehmensbezogenen Daten nicht zugestimmt hätten.*

Auf der Grundlage des Bürgerlichen Gesetzbuchs wird ein Mietspiegel als Übersicht über die ortsübliche Vergleichsmiete von der Gemeinde und von Interessenvertretungen der Mieter und Vermieter gemeinsam erstellt. Der hierzu eingerichtete Arbeitskreis Mietspiegel war allerdings nur an der Konzeption des Erhebungsformulars beteiligt, bestimmte also darüber, welche Arten von Informationen erhoben werden. Die anonymisierte Erhebung der konkreten Daten oblag der Vermieterseite und deren Auswertung dem Gutachterausschuss für Grundstückswerte.

Fraglich war, ob es sich, wie von der Stadt angenommen wurde, um schutzbedürftige unternehmensbezogene Daten im Sinne des § 5 Abs. 1 Nr. 3 Akteneinsichts- und Informationszugangsgesetz (AIG) handelte. Danach ist es erforderlich, dass diese nur einem eng begrenzten Personenkreis bekannt sind, zu einem bestimmten Geschäftsbetrieb in Beziehung stehen und nach dem Willen des Unternehmens geheim zu halten sind oder an der Geheimhaltung ein schutzwürdiges Interesse besteht. Wir konnten zunächst nicht erkennen, dass die Daten nur einem eng begrenzten Personenkreis bekannt waren – schließlich handelte es sich um Daten aus Mietverträgen, die keineswegs nur wenigen Mitarbeitern der Wohnungsgesellschaften bekannt waren, sondern zumindest auch den Mieterinnen und Mietern sowie deren persönlichem Umfeld. Somit wären die Voraussetzungen für einen Schutzbedarf nicht gegeben und die Akteneinsicht dürfte nicht von der Zustimmung der betroffenen Unternehmen abhängig gemacht werden. Die Stadt überzeugte uns je-

doch davon, dass durch die Aggregation dieser Daten sozusagen "neue" Informationen entstehen, die über die den einzelnen Mietern bekannten Angaben zu deren eigenen Mietverhältnissen hinausgehen und die somit nur wenigen (nämlich den erhebenden und auswertenden) Personen bekannt sein können. Dies gilt insbesondere, wenn sich der Antrag auf Informationen zu Mietobjekten einer einzigen Wohnungsgesellschaft bezieht.

Im Ergebnis stellten wir fest, dass die Voraussetzungen des § 5 Abs. 1 Nr. 3 AIG vorlagen und die Verweigerung der Einsichtnahme mangels Zustimmung der betroffenen Unternehmen zulässig war.

Werden mehrere Einzelinformationen mit Unternehmensbezug, die jeweils für sich betrachtet nicht schutzbedürftig sind, weiterverarbeitet, kann dadurch ein Mehrwert entstehen, der einen stärkeren Schutzbedarf aufweist als die Grunddaten. Diese aufbereiteten Informationen können dann nur mit Zustimmung der betroffenen Unternehmen offen gelegt werden.

## **2.5 Gehört eine handschriftliche Notiz zur Akte?**

*Während der Einsichtnahme in die Unterlagen zu einem Sportstadion wurden auch handschriftliche Notizen, die in der Akte abgeheftet waren, offen gelegt. Dem Wunsch des Antragstellers, Fotokopien der Dokumente zu erhalten, wurde nur im Hinblick auf die übrigen Informationen entsprochen. Bei den handschriftlichen Notizen handele es sich – so die Behörde – um rein interne Vermerke, die nur versehentlich der Akte beigefügt worden seien und daher nicht fotokopiert werden könnten.*

Das Recht auf Informationszugang bedeutet, dass Informationen – soweit keine gesetzlichen Ausnahmegründe hierfür vorliegen – vollständig zur Verfügung zu stellen sind. Ein Antragsteller kann aber nur dann über sie verfügen, wenn er sie nicht lediglich während der Einsicht in die Akte lesen, sondern zum Beispiel in Form einer Kopie mitnehmen und in Ruhe selbst oder mit Sachverständigen seiner Wahl auswerten kann. Auch bieten Kopien eine sichere Möglichkeit, Informationen, die zur Verteidigung einer Rechtsposition erforderlich sind, vollständig zu erlangen und dauerhaft über sie zu verfügen. Ihre Verweigerung stellt prinzipiell eine Schwächung dieser Rechtsposition dar. Grundsätzlich hat ein Antragsteller also ein Recht, Fotokopien von Unterlagen, die ihm im Rahmen der Akteneinsicht zugänglich gemacht wurden, zu erhalten. Beantragt er die Herausgabe von Fotokopien, hat die Akten führende Stelle – abgesehen von Ausnahmen aufgrund des Urheberrechts – nicht erneut zu

prüfen, ob der Informationszugang möglich ist. Diese Prüfung ist bereits abschließend bei der Bearbeitung des ursprünglichen Antrags auf Akteneinsicht erfolgt.

Bei der Frage, welche Dokumente Aktenbestandteil sind, handelt es sich um eine grundsätzliche Frage der Aktenführung. Handschriftliche Notizen oder Vorentwürfe, die nicht Aktenbestandteil werden sollen, sind unverzüglich zu vernichten und gar nicht erst zur Akte zu nehmen. Sofern aus ihnen jedoch Informationen hervorgehen, die für den Vorgang von Bedeutung sind, gehören sie automatisch zur Akte. Im vorliegenden Fall stellte die Behörde fest, dass ein handschriftliches Dokument versehentlich der Akte beigefügt war und eigentlich nicht deren Bestandteil hätte werden sollen. Sie vernichtete die Notiz, ohne dem Antragsteller eine Kopie zu fertigen. Zwar ist der Akten führenden Stelle grundsätzlich nicht das Recht abzusprechen, eine fehlerhafte Entscheidung zu revidieren, allerdings sollte gerade auf dem Gebiet der Informationsfreiheit auf ein transparentes Verwaltungshandeln geachtet werden. Eine Bearbeitung abgeschlossener Verwaltungsvorgänge zwischen Einsichtnahme und Herausgabe von Fotokopien schürt – unabhängig davon, ob sie ausnahmsweise gerechtfertigt sein kann – unwillkürlich Misstrauen auf Seiten des Antragstellers.

Durch eine ordentliche Aktenführung und eine gründliche Prüfung des Antrags auf Informationszugang wird vermieden, dass sich erst bei der Herausgabe von Fotokopien herausstellt, dass die Informationen gar nicht zur Akte gehören und nicht hätten zugänglich gemacht werden dürfen.

## **2.6 Zugang zu Informationen über privatrechtlich organisierte Aufgaben**

*Um sich über die finanziellen Aspekte beim Betrieb einer Abwasseranlage zu informieren, beantragte ein Bürger Akteneinsicht beim Zweckverband. Dieser lehnte den Antrag u. a. mit der Begründung ab, dass der privatrechtlich organisierte Betrieb nicht Gegenstand des Informationszugangs sein könne.*

Verfügt eine Behörde über Unterlagen, die unternehmensbezogene Daten enthalten, hat sie deren Schutzbedarf auf der Grundlage von § 5 Abs. 1 Nr. 3 Akteneinsichts- und Informationszugangsgesetz zu prüfen. Ausführliche Hinweise zum Umgang mit unternehmensbezogenen Informationen können dem Tätigkeitsbericht 2001 (Teil B, Punkt 2.5) entnommen werden. Allerdings ist zu beachten, dass es sich bei Unterlagen zu einer Abwasseranlage – auch, wenn es um deren Finanzierung geht – um

Umweltinformationen handeln kann, sodass vorrangig das Umweltinformationsgesetz anzuwenden sein dürfte. Die Vorschriften des § 8 Umweltinformationsgesetz zum Schutz von Betriebs- und Geschäftsgeheimnissen sind weniger weit gehend als die des Akteneinsichts- und Informationszugangsgesetzes.

Befinden sich Unterlagen ausschließlich bei dem privaten Betreiber einer Abwasseranlage, kann auch diesem gegenüber ein Anspruch auf Akteneinsicht bestehen. Das Akteneinsichts- und Informationszugangsgesetz verlangt hierfür eine Übertragung hoheitlicher Aufgaben (§ 2 Abs. 4) durch Gesetz oder Beleihungsakt, während nach § 2 Nr. 2 Umweltinformationsgesetz lediglich die Wahrnehmung öffentlich-rechtlicher Aufgaben im Bereich des Umweltschutzes unter behördlicher Aufsicht erforderlich ist. In beiden Fällen ist die Behörde verpflichtet, den Antragsteller darauf hinzuweisen, dass nicht sie selbst, sondern der private Betreiber über die Akten verfügt und den Antrag gegebenenfalls weiterzuleiten.

Die Darstellung des Zweckverbands, nach der ein Zugang zu Informationen über privatrechtlich organisierte Aufgaben nicht möglich sei, trifft somit in keinem Fall zu.

Auch gegenüber privaten Betreiberfirmen besteht nach dem Umweltinformationsgesetz ein Recht auf Akteneinsicht, wenn diese öffentlich-rechtliche Aufgaben wahrnehmen. Nach dem Akteneinsichts- und Informationszugangsgesetz müssen private Firmen nur dann Akteneinsicht gewähren, wenn sie Beliehene sind.

## **2.7 Haben eingetragene Vereine Geschäftsgeheimnisse?**

*Um die Finanzierung der Betriebskosten einer von einem eingetragenen Verein geführten Kindertagesstätte zu überprüfen, beantragte ein Vater Akteneinsicht in die entsprechenden Abrechnungen. Insbesondere interessierte er sich für die Höhe und Verwendung der gemeindlichen Zuschüsse. Die Behörde verweigerte den Informationszugang und machte geltend, dass es sich bei den Informationen um Geschäftsgeheimnisse des Vereins handele.*

§ 5 Abs. 3 Nr. 1 Akteneinsichts- und Informationszugangsgesetz nimmt unternehmensbezogene Daten von dem Recht auf Akteneinsicht unter bestimmten Voraussetzungen aus. Zweck dieser Regelung ist der Schutz des Geschäftsbetriebes eines auf wirtschaftliche Betätigung ausgerichteten Unternehmens. Auf eingetragene Vereine, die als Träger für eine

Kindertagesstätte handeln, ist diese Vorschrift nicht anzuwenden. Bei ihnen handelt es sich um nicht-wirtschaftliche Vereine. Sie verfolgen vorrangig keine wirtschaftlichen Interessen und bieten ihre Leistungen nicht im marktwirtschaftlichen Wettbewerb an. Daher können sie sich als juristische Personen weder auf Betriebs- und Geschäftsgeheimnisse, noch auf das Grundrecht auf Datenschutz berufen, das lediglich natürlichen Personen zusteht. Verfügt die Behörde also über Informationen zu einem solchen Verein, so ist ein überwiegendes privates Interesse, das einer Akteneinsicht entgegenstehen könnte, nicht zu erkennen. Das Amt hat die Unterlagen aufgrund unseres Hinweises offen gelegt.

Betriebs- und Geschäftsgeheimnisse können nur von wirtschaftlich tätigen Unternehmen geltend gemacht werden. Für eingetragene, nicht-wirtschaftliche Vereine gilt dies nicht.

## **2.8 Herausgabe von Kopien eines ausländerrechtlichen Erlasses**

*Es war unklar, wie mit einem Erlass zum Bleiberecht für Asylbewerber sowie mit der Weitergabe der darin enthaltenen Informationen an Außenstehende verfahren werden sollte. Das Ministerium des Innern regelte deshalb in einem ergänzenden Runderlass, dass der ursprüngliche Erlass zwar eingesehen werden durfte, die Aushändigung von Kopien jedoch ausgeschlossen war.*

Zu Recht vermutete eine Ausländerbehörde, dass die Verweigerung von Fotokopien mit dem Recht auf Informationszugang nicht zu vereinbaren war. Nach § 7 Akteneinsichts- und Informationszugangsgesetz ist der Informationszugang nicht ausschließlich durch die Einsicht in Originaldokumente zu gewähren. Vielmehr können – mit Zustimmung des Antragstellers – auch Fotokopien der Unterlagen gefertigt werden. Die Verwaltung kann dies beispielsweise aus organisatorischen Gründen vorschlagen. Unabhängig von dieser Regelung kann auch der Antragsteller Kopien verlangen. Insbesondere sind Kopien eine sichere Möglichkeit, Informationen, die zur Untermauerung der eigenen Rechtsposition erforderlich sind, zu erlangen und dauerhaft über sie zu verfügen. Dies ist auch für Antragsteller bedeutsam, die auf der Grundlage des Verwaltungsverfahrensgesetzes am laufenden Verwaltungsverfahren beteiligt sind.

Ein Grund dafür, dass der ausländerrechtliche Erlass zwar eingesehen, nicht aber kopiert werden durfte, ist nicht ersichtlich. Dieser Auffassung hat sich das Ministerium des Innern angeschlossen. Es hat den entgegenstehenden Runderlass teilweise aufgehoben und klargestellt, dass

die Herausgabe von Fotokopien sowohl an Verfahrensbeteiligte als auch an Außenstehende zulässig ist.

Unterlagen, deren Einsichtnahme keine privaten oder öffentlichen Schutzinteressen entgegenstehen, sind auf Wunsch des Antragstellers zu fotokopieren. Etwas Gegenteiliges darf auch in Verwaltungsvorschriften nicht geregelt werden.

## **2.9 Anwendungshinweise zum Akteneinsichts- und Informationszugangsgesetz**

Seit 1998 gilt in Brandenburg das Akteneinsichts- und Informationszugangsgesetz. Es ermöglicht allen Interessierten ohne Voraussetzungen den Zugang zu Informationen bei öffentlichen Stellen. Um die Nutzung des Gesetzes zu erleichtern, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht seine bisherigen Erfahrungen mit der Anwendung des Gesetzes zusammengetragen und auf ihrer Grundlage Anwendungshinweise veröffentlicht. Sie stellen eine Zusammenfassung der Empfehlungen des Landesbeauftragten aus zahlreichen Einzelfällen dar.

Das Recht auf Akteneinsicht kann u. a. dann eingeschränkt sein, wenn private Schutzinteressen Dritter überwiegen. Dies ist insbesondere der Fall, wenn die zur Einsicht beantragten Unterlagen personen- oder unternehmensbezogene Daten enthalten. Das Akteneinsichts- und Informationszugangsgesetz sieht hierfür zwei unterschiedliche Verfahren zur Prüfung eines Antrages auf Akteneinsicht vor, die wir jeweils sowohl in Textform als auch grafisch aufbereitet haben.

Die im Jahre 2001 in Kraft getretene Akteneinsichts- und Informationszugangsgebührenordnung ermöglicht es den Akten führenden Stellen, Kosten für den Informationszugang zu erheben. In jedem Fall stellt sich aber die Frage, ob überhaupt und wenn ja, in welcher Höhe Gebühren und Auslagen verlangt werden können. Zur Frage der Kostenerhebung hat der Landesbeauftragte gesonderte Hinweise veröffentlicht.

Die Anwendungshinweise werden ständig aktualisiert. Auf eine Druckversion haben wir daher zunächst verzichtet. Anregungen und Kritik von Bürgerinnen und Bürgern sowie Rückmeldungen aus der Verwaltungspraxis, die dazu beitragen, unsere Hinweise weiterzuentwickeln, sind jederzeit willkommen.

Die Anwendungshinweise zum Akteneinsichts- und Informationszugangsgesetz im Internet: <http://www.lda.brandenburg.de>

### **3 Technisch-organisatorische Voraussetzungen der Akteneinsicht**

#### **Elektronische Akteneinsicht Rathenow**

*Bereits in unserem Tätigkeitsbericht 1999 haben wir darüber berichtet, dass die Stadt Rathenow im Rahmen des Städtewettbewerbs Media@Komm einen Förderpreis für das Projekt "Elektronische Akteneinsicht" erhalten hat<sup>62</sup>. Seitdem setzt die Stadt das Projekt in enger Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie dem Landesbetrieb für Datenverarbeitung und Statistik schrittweise um.*

Ziel des Projektes ist es, den nach dem brandenburgischen Akteneinsichts- und Informationszugangsgesetz (AIG) grundsätzlich voraussetzungslosen Zugang zu den von der Verwaltung vorgehaltenen Informationen auch elektronisch über das Internet zu ermöglichen.

Die Stadt wird das so genannte City-Informationssystem auf einem Webserver zum Abruf über das Internet bereitstellen. Dort werden Dokumente vorgehalten, zu denen ein voraussetzungsloser Zugang besteht und die nach unterschiedlichen Rechtsvorschriften ohnehin öffentlich gemacht werden können oder müssen, wie z. B. Satzungen oder Unterlagen aus öffentlichen Sitzungen der Stadtverordnetenversammlung. Insofern besteht kein wesentlicher Unterschied zu vielen anderen Kommunen.

Darüber hinaus wird die Stadt Rathenow aber auch Akten und Dokumente aus dem gewöhnlichen Verwaltungsvollzug für einen elektronischen Zugang bereitstellen. Zur Umsetzung des Projektes hat die Stadt zunächst ihren Aktenplan sowie das Dokumentenaufkommen analysiert, einen transparenten Aktenplan geschaffen und ein Dokumentenmanagement-System (DMS) ausgewählt. Derzeit wird das DMS sowie das elektronische Archivsystem zunächst für einige Ämter implementiert und die Internet-Schnittstelle entwickelt, bevor die elektronische Akte als Voraussetzung für eine elektronische Akteneinsicht zunächst in einer Pilotphase eingeführt wird.

Will ein Bürger in eine elektronische Akte einsehen, wird er in der Regel zunächst per E-Mail bei der Stadt anfragen. Der zuständige Bearbeiter wird dann zunächst die relevanten Akten bzw. Dokumente identifizieren. Ist die Akte noch nicht in elektronischer Form vorhanden, ist ad hoc eine Digitalisierung der Dokumente möglich. Der Bearbeiter prüft anschließend, ob und in welchem Umfang die Dokumente für eine Akteneinsicht

<sup>62</sup>

Vgl. Tätigkeitsbericht 1999, B 4.2

zur Verfügung stehen. Bestehen keine Geheimhaltungsgründe aus überwiegendem öffentlichen oder privaten Interesse nach §§ 4, 5 AIG, so werden die Dokumente ohne Weiteres dem Anfragenden per E-Mail zur Verfügung gestellt. Ebenso wird verfahren, wenn die nicht ohne Weiteres zugänglichen Teile entsprechend § 6 Abs. 2 AIG ausgesondert werden können.

Muss die Akteneinsicht abgelehnt werden oder ist der Inhalt nach §§ 4, 5 AIG geheim zu halten, erhält der Antragsteller eine entsprechende Nachricht. In diesen Fällen wird eine Identifizierung des Antragstellers mit qualifizierter elektronischer Signatur verlangt, weil die Ablehnung ein Verwaltungsakt ist und der Antragsteller dagegen Rechtsmittel einlegen kann.

Enthalten die Dokumente personenbezogene Daten oder geheim zu haltende unternehmensbezogene Daten, und soll die Zustimmung des Betroffenen eingeholt werden, ist ebenfalls eine Identifizierung des Antragstellers erforderlich.

Durch ein Serverzertifikat, das durch den Landesbetrieb für Datenverarbeitung und Statistik bereitgestellt wird, können die Empfänger nachvollziehen, dass die übermittelten Dokumente auch wirklich von der Stadt Rathenow stammen.

Die elektronische Akteneinsicht in Rathenow wird einen bürgerfreundlichen und datenschutzgerechten elektronischen Zugang zu den in der Verwaltung vorgehaltenen Informationen realisieren.

## **Teil C**

### **Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht**

#### **1 Die Dienststelle**

Die Anforderungen an eine effektive Datenschutzkontrolle und die zuverlässige Behandlung von Bürgerbeschwerden in den Bereichen Datenschutz und Informationszugang sind auch im Berichtszeitraum nicht geringer geworden. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht und seine 17 Mitarbeiterinnen und Mitarbeiter müssen sich mit einer wachsenden Zahl von Verfahren auseinandersetzen, bei der zum Teil sehr sensitive Daten (etwa im Krankenhausbereich) verarbeitet werden. Auch die Beratung und Kontrolle der Kreise und Gemeinden nimmt immer mehr Zeit in Anspruch.

Im Berichtszeitraum sind zwei bewährte Dienstkräfte, Diplom-Bibliothekarin Christel Kern, und der stellvertretende Leiter des Bereichs Technik und Organisation, Ulrich Wiener, in den Ruhestand getreten. Beiden ist es zu einem erheblichen Teil zu verdanken, dass die Dienststelle des Landesbeauftragten in den zurückliegenden 10 Jahren den Ansprüchen an eine Bürgerbehörde gerecht werden konnte. Erfreulicherweise konnten bis zum Ablauf des Berichtszeitraums die frei gewordenen Stellen erneut besetzt werden, was bei einer derart knappen Personalausstattung unabdingbar war, um die Prüf- und Beratungstätigkeit uneingeschränkt aufrechtzuerhalten. Mit der Besetzung einer weiteren Stelle im Bereich Technik und Organisation konnte die im Haushaltsplan vorgesehene Zahl von Mitarbeitern wieder erreicht werden.

Zu Beginn des Berichtszeitraums hatte der Landesbeauftragte gemeinsam mit dem Präsidenten des Landtages und dem ersten Landesbeauftragten für den Datenschutz bei einer Veranstaltung in Kleinmachnow an die Einrichtung der Dienststelle vor 10 Jahren erinnert und anschließend mit Schülerinnen und Schülern aus Teltow und Kleinmachnow über Fragen des Datenschutzes im Internet diskutiert. Der Schutz von Persönlichkeitsrechten bei der Unterrichtsgestaltung stand auch im Mittelpunkt eines Gesprächs, das der Landesbeauftragte mit den Leiterinnen und Leitern der für die Lehrerfortbildung verantwortlichen Studienseminare im Oktober 2002 führte. Dabei bot er an, hierzu auch in den einzelnen Studienseminaren nach Möglichkeit für Gespräche und Veranstaltungen zur Verfügung zu stehen. Der Landesbeauftragte misst der Berücksichtigung des Datenschutzes und der Informationsfreiheit bei der Unterrichtsgestaltung eine hohe Bedeutung bei.

## **2 Zusammenarbeit mit Parlamenten**

Im Berichtszeitraum wurden sowohl der Tätigkeitsbericht für das Jahr 2000 als auch der 10. Tätigkeitsbericht (2001) mit den Stellungnahmen der Landesregierung abschließend im Innenausschuss und im Plenum des Landtages behandelt. Allerdings verzichtete der Ausschuss für Inneres – anders als beim Tätigkeitsbericht 2000 – auf eine inhaltliche Beschlussempfehlung.

Der Landesbeauftragte hat im Rahmen einer Anhörung vor dem Innenausschuss zum Entwurf der Landesregierung für ein Gesetz zur Umsetzung des Terrorismusbekämpfungsgesetzes und zur Stärkung der parlamentarischen Kontrolle Stellung genommen.

Bei einem gemeinsamen Treffen des Ausschusses für Inneres mit dem Datenschutzausschuss der Bremischen Bürgerschaft im Landtag Brandenburg berichtete der Landesbeauftragte über die praktischen Erfahrungen mit der Umsetzung des Akteneinsichts- und Informationszugangsgesetzes.

Auf Einladung des Innenausschusses des Deutschen Bundestages hat der Landesbeauftragte als Sachverständiger an zwei öffentlichen Anhörungen teilgenommen, die dieser Ausschuss bei der Beratung des Entwurfs für ein Fünftes Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes am 25. April und 24. Juni 2002 durchgeführt hat<sup>63</sup>.

## **3 Kooperation mit Datenschutzbehörden und Informationszugangsbeauftragten**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im vergangenen Jahr unter dem Vorsitz des rheinland-pfälzischen Landesbeauftragten für den Datenschutz, Prof. Dr. Walter Rudolf, in Mainz und Trier stattgefunden. Die dabei gefassten Entschlüsse können in dem Band "Dokumente zu Datenschutz und Informationsfreiheit 2002" nachgelesen werden, den wir wieder gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit veröffentlicht haben. Im begonnenen Jahr 2003 hat der Sächsische Datenschutzbeauftragte, Dr. Thomas Giesen, den Vorsitz der Datenschutzkonferenz übernommen.

Die Entschließungen der Datenschutzkonferenz mit medienrechtlichem Bezug sind vom Arbeitskreis Medien der Konferenz vorbereitet worden, den der Landesbeauftragte als Vorsitzender zu zwei Sitzungen nach Potsdam eingeladen hatte.

Für die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation hat der Landesbeauftragte ein Arbeitspapier zur Überwachung der Telekommunikation im internationalen Rahmen vorbereitet, das die Arbeitsgruppe im Berichtszeitraum verabschiedet hat<sup>64</sup>. Bei der 24. Internationalen Konferenz der Datenschutzbeauftragten hat der Landesbeauftragte im September 2002 über die positiven Erfahrungen berichtet, die in Brandenburg mit einer gemeinsamen Instanz für Datenschutz und Informationszugang gesammelt werden konnten. Auch im vergangenen Jahr hat der Landesbeauftragte die Bundesländer in der Gruppe der Europäischen Datenschutzbeauftragten nach Art. 29 der EG-Datenschutzrichtlinie in Brüssel vertreten.

Die früher üblichen Koordinationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Ministerium des Innern konnten im Berichtszeitraum nicht wieder aufgenommen werden, sie sollen aber nach längerer Unterbrechung im jetzt begonnenen Jahr wieder stattfinden.

Die Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ist nach wie vor intensiv. Bei regelmäßigen Treffen der Dienststellenleitungen werden Fragen der Verarbeitung personenbezogener Daten, die immer stärker auch die gesamte Region betreffen, mit dem Ziel erörtert, einheitliche Prüfstandards zu entwickeln.

## **4 Anschluss unserer Dienststelle an das Internet**

Der Anschluss des Landesverwaltungsnetzes (LVN) an das Internet und der Aufbau eines Kommunikationsverbundes im Land ermöglicht schon seit einigen Jahren neue Formen der Zusammenarbeit der Dienststellen. Dies wird auch für uns immer wichtiger. Sei es die Überprüfung der Internetangebote öffentlicher Stellen, der elektronische Austausch von Dokumenten oder die Suche nach Informationen zum Thema Datenschutz – das Internet ist zu einem wesentlichen Bestandteil unserer Arbeit geworden.

---

64

Wir haben deshalb damit begonnen, unser lokales Netz an das LVN anzuschließen und damit allen Mitarbeiterinnen und Mitarbeitern die Nutzung des Internets am Arbeitsplatz zu ermöglichen. Der Anschluss wäre mit einer Reihe von Risiken verbunden gewesen. Die lokale Infrastruktur und die Daten hätten unter Umständen Angriffen aus dem Internet oder aus anderen am LVN angeschlossenen Einrichtungen ausgesetzt sein können. Obwohl das LVN schon durch eine zentrale Firewall vom Internet abgeschottet wird, werden dadurch nicht alle Gefährdungen ausgeschlossen. Nach einer eingehenden Kommunikationsanalyse wurde das bestehende IT-Sicherheitskonzept unserer Dienststelle entsprechend erweitert. U. a. schützt nun eine zusätzliche Firewall unser lokales Netz vor dem LVN. Eventuell auftretende Angriffe werden umgehend dem Systemadministrator elektronisch gemeldet und zusätzlich werden alle personenbezogenen Daten unseres Vorgangsverwaltungssystems mit Hilfe eines Chipkartensystems verschlüsselt auf dem Server gespeichert. Die im IT-Sicherheitskonzept festgelegten Maßnahmen werden in regelmäßigen Abständen dem Stand der Technik angepasst.

## **5 Öffentlichkeitsarbeit**

### **5.1 Aktuelle Publikationen des Landesbeauftragten**

Die Verabschiedung des brandenburgischen Datenschutzgesetzes vor zehn Jahren nahm der Landesbeauftragte zum Anlass, eine CD-ROM mit dem Titel "Zehn Jahre Datenschutz in Brandenburg 1992 – 2002" herauszugeben. Sie umfasst sämtliche Dokumente, die auf unserer Website vorhanden sind, so z. B. alle von uns veröffentlichten Broschüren, Gesetzestexte zu Datenschutz und Informationszugang, sämtliche Tätigkeitsberichte sowie Hinweise zu technisch-organisatorischen Aspekten des Datenschutzes. Dabei wurden z. T. auch allgemein interessante Veröffentlichungen von Datenschutzbeauftragten anderer Bundesländer übernommen. Darüber hinaus wird das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in den Informationstechnik angeboten. Die CD-ROM wird künftig jährlich aktualisiert und neu herausgegeben.

Die Broschüre "Datenscheckheft", die seit Jahresbeginn vergriffen war, haben wir aktualisiert und neu aufgelegt. Sie enthält abtrennbare Musterbriefe ("Schecks"), mit denen Datenschutzrechte auf einfachem Wege eingefordert werden können. Die Vordrucke richten sich an unterschiedlichste Behörden, die möglicherweise personenbezogene Daten der Absender speichern. Interessenten brauchen diese nur auszufüllen und in einem Briefumschlag zu versenden, um zu erfahren, ob und welche

Daten über die eigene Person dort vorhanden sind. Neben dieser Auskunft dient das Datenscheckheft auch der Berichtigung falscher Daten.

Außerdem stellen wir Interessenten drei weitere Faltblätter zur Verfügung: Mit den "Tipps zur datenschutzgerechten Gestaltung der Websites von Schulen" möchten wir Lehrkräften, Eltern sowie Schülerinnen und Schülern Hinweise geben, wie schulische Websites gestaltet werden können, ohne das Datenschutzrecht der Beteiligten zu gefährden. Im Faltblatt "Ins Internet? Aber sicher!" geben wir Hinweise, wie sicherheitsbewusste Nutzer ihren PC beim Surfen im Internet durch technisch-organisatorische Maßnahmen vor dem Missbrauch durch Dritte schützen können. Das Faltblatt "Keine Chance den Computer-Viren" informiert über die Möglichkeiten, den Computer gegen das Eindringen von Viren, Würmern und Trojanern zu schützen.

Zusammen mit anderen Datenschutzbeauftragten hat der Landesbeauftragte die Informationsbroschüre "Bitte keine Werbung – Tipps und Informationen zu Adressenhandel und unerwünschter Werbung" herausgegeben. Darin wird erläutert, wie man sich vor unerwünschter Werbung per Post, Telefon, Fax, E-Mail oder SMS schützen und die Weitergabe der eigenen Adresse zu Werbezwecken unterbinden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die "Handlungsempfehlungen datenschutzgerechtes eGovernment" veröffentlicht, die wir in Form einer Broschüre ebenfalls zur Verfügung stellen.

Alle Veröffentlichungen können kostenlos beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht angefordert werden. Sie sind auch im Internet unter <http://www.lda.brandenburg.de> abrufbar.

## **5.2 Der Landesbeauftragte auf dem Brandenburg-Tag**

Unter dem Motto "Zehn Jahre Datenschutz in Brandenburg" präsentierte sich der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht auf dem Brandenburg-Tag in Neuruppin. Zahlreiche Besucherinnen und Besucher, die den sonnigen Spätsommertag für einen Ausflug in die Prignitz nutzten, besuchten unseren Informationsstand, um sich über ihre Rechte auf Datenschutz und Akteneinsicht zu informieren.

Im Mittelpunkt des Interesses stand – wie schon in den Vorjahren – der Wunsch, sich gegen die Werbeflut zu schützen. Sorgen um die Sicherheit im Internet und Skepsis gegenüber der Videoüberwachung im öffentlichen Raum waren weitere Schwerpunkte der Beratungsgespräche. Auch

das Interesse, zu erfahren, welche öffentliche Stelle Informationen zur eigenen Person speichert, zu welchen Zwecken diese verarbeitet werden und vor allem, wie man dies als Betroffener erfahren kann, prägte zahlreiche Fragen.

Der nächste Brandenburg–Tag findet am 6. September 2003 in der Landeshauptstadt Potsdam statt. Auch dort wird der Landesbeauftragte wieder mit einem Informationsstand vertreten sein. Wir freuen uns bereits jetzt auf das Gespräch mit den Besucherinnen und Besuchern des Landesfestes.

### **5.3 Internationales Symposium "Informationsfreiheit und Datenschutz" wieder in Potsdam**

Vor vier Jahren hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht das erste Internationale Symposium "Informationsfreiheit in Datenschutz" in Potsdam durchgeführt. Es war die bundesweit erste Veranstaltung, die sich gleichzeitig mit den beiden Grundrechten auf Information und Datenschutz befasste. Zwei Jahre später organisierte der Landesbeauftragte erneut ein Symposium, das dieses Mal thematisch unter dem Zeichen der bevorstehenden Erweiterung der Europäischen Union stand. Datenschutzbeauftragte sowie viele andere interessierte Fachleute aus Brandenburg nahmen an diesem Erfahrungsaustausch zwischen West-, Mittel- und Osteuropa zu Fragen der Informationsgesellschaft ebenso teil wie Gäste aus der Bundesrepublik und Europa. Dabei wurde die Brückenfunktion Brandenburgs als Verbindungsland zwischen der gegenwärtigen Europäischen Union und den Beitrittsländern deutlich.

Das große Interesse an dem Internationalen Symposium sowie die vielen positiven Rückmeldungen haben uns in der Absicht bestärkt, solche Veranstaltungen regelmäßig durchzuführen. Die Vorbereitungen für das nächste Internationale Symposium sind mittlerweile angelaufen: Am 10. und 11. November 2003 lädt der Landesbeauftragte erneut zu einer Tagung ein. Schwerpunktthemen werden Fragen der Transparenz und des eGovernment in Mittel- und Osteuropa sein. Hierfür konnten wir bereits interessante und namhafte Referenten aus dem In- und Ausland gewinnen.

Einzelheiten zum diesjährigen Internationalen Symposium in Potsdam sowie das genaue Veranstaltungsprogramm können demnächst auf unserer Website abgerufen werden.

Kleinmachnow, den 12. März 2003

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz  
und für das Recht auf Akteneinsicht

# **Anlagen**



## **Allgemeine datenschutzrechtliche Anforderungen an zentrale Telekommunikations-Anlagen bei Behörden im Land Brandenburg**

Die folgenden Forderungen ergeben sich aus dem Brandenburgischen Datenschutzgesetz (BbgDSG), dem Telekommunikationsgesetz (TKG), der Telekommunikations-Datenschutzverordnung (TDSV), der Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg (DAV) und der Musterdienstvereinbarung:

### **1 Technisch-organisatorische Maßnahmen**

- 1.1 Die zur TK-Anlage gehörenden Kabel und Leitungen sind möglichst zugriffssicher zu verlegen. Alle Haupt- und Zwischenverteilerkästen sind in geeigneter Form zu schützen.
- 1.2 Dauerhaft nicht benötigte Leistungsmerkmale sind aus der Anlagensoftware zu entfernen oder so zu sperren, dass sie nicht reaktiviert werden können.
- 1.3 Alle Änderungen an den Leistungsmerkmalen und alle übrigen Administrationsarbeiten an der TK-Anlage sind revisionssicher zu protokollieren.
- 1.4 Die Zugriffsrechte auf die Software der TK-Anlage sind so zu gestalten, dass jeder nur die von ihm unbedingt benötigten Komponenten nutzen kann. Dauerhaft nicht benötigte Softwarekomponenten sind aus der Anlage zu entfernen.
- 1.5 Es ist zu sichern, dass der Zugriff auf Protokolldateien nur durch zwei Personen gleichzeitig (Vier-Augen-Prinzip) erfolgen kann.
- 1.6 Bei der Wartung von TK-Anlagen bzw. Gebührendatenverarbeitungsanlagen sind die Bestimmungen von § 11a BbgDSG konsequent einzuhalten.
- 1.7 Die Übertragung von Verbindungsdaten innerhalb von Netzen und der Versand von Einzelverbindungsdaten als E-Mail darf nur in verschlüsselter Form erfolgen.

### **2 Gebührendatenverarbeitung**

- 2.1 Eine Speicherung aller Verbindungsdatensätze über das Gesprächsende hinaus für Zwecke der Gebührenabrechnung und Kostenkontrolle ist grundsätzlich nicht zulässig.
- 2.2 Verbindungsdaten sind während ihrer Übernahme in den Gebührencomputer, die unmittelbar am Gesprächsende jedoch mindestens täglich erfolgen soll, weitestgehend zu selektieren und zu verdichten. So sind im Gebührencomputer im Regelfall nur noch die Gebühreneinheiten, ggf. fortlaufend addiert, zu speichern und Verbindungsdatensätze nur dann, wenn sie später auch tatsächlich für Kontrollzwecke oder zum Nachweis von Privatgesprächen ausgewertet werden.

- 2.3 Die Speicherung vollständiger Verbindungsdaten mit ungekürzter Zielrufnummer für Kontrollzwecke ist nur zulässig, wenn diese stichprobenartig bereits vor Beginn des Abrechnungszeitraumes oder durch ein automatisches Zufallsverfahren ausgewählt wurden. Es gilt der Grundsatz, nur solche Verbindungsdaten zu speichern, deren Auswertung konkret vorgesehen ist.
- 2.4 Für die Abrechnung von Privatgesprächen ist jedem Nutzer ein Wahlrecht einzuräumen, ob alle Verbindungsdaten mit verkürzter Zielrufnummer oder nur die kumulativen Gesamtgebühren gespeichert werden.

Arbeitsgruppe "Telemedizin" der Datenschutzbeauftragten des Bundes und der Länder<sup>65</sup>

### **Datenschutz und Telemedizin**

#### **– Anforderungen an Medizinetze –**

Stand 10/02

---

<sup>65</sup> Die Arbeitsgruppe wurde von der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen geleitet. Die Ausarbeitung ist von der 64. Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen worden und soll kontinuierlich weiterentwickelt werden.

## Inhaltsverzeichnis

	Seite
I. Einleitung.....	133
II. Allgemeine datenschutzrechtliche Anforderungen.....	133
III. Grundlegende Sicherheitsanforderungen.....	137
IV. Formen der Datenhaltung.....	139
V. Spezielle Datensicherheitsmaßnahmen.....	142
VI. Beispiele für Ansätze/Projekte zur Kommunikation im Gesundheitswesen....	148

## **I. Einleitung**

Zur Steigerung von Qualität und Effizienz in der Gesundheitsversorgung sowie zur Kosteneinsparung spielt die einrichtungsübergreifende elektronische Kommunikation eine immer größere Rolle. Kommunikationsnetze und Kommunikationsdienste sollen dazu beitragen, die Kommunikation zwischen den Institutionen zu verbessern und die Leistungsprozesse zu optimieren. Wegen der hohen Sensibilität der im Gesundheitswesen verarbeiteten Daten kommt dem Datenschutz und der Datensicherheit eine besondere Bedeutung zu.

Die folgenden Ausführungen sollen eine Hilfestellung zur Formulierung und Umsetzung einer datenschutzgerechten Sicherheitspolitik für die elektronische Kommunikation und Datenverarbeitung im Gesundheitswesen bieten. In Kapitel II werden zunächst die allgemeinen datenschutzrechtlichen Anforderungen aufgezeigt. Diese bilden den rechtlichen Rahmen, an dem sich medizinische Datenverarbeitung zu orientieren hat. Darauf aufbauend werden in Kapitel III grundlegende Sicherheitsanforderungen für Systeme definiert, die patientenbezogene Daten verarbeiten. Kapitel IV diskutiert basierend auf der Form der Datenhaltung vier Architekturszenarien für Systeme zur einrichtungsübergreifenden Kommunikation. Damit verbunden ist die Erwartung, dass sich alle Systeme zur einrichtungsübergreifenden Kommunikation nach diesen Architekturansätzen kategorisieren lassen bzw. eine Kombination aus diesen Architekturen darstellen. Insofern sind die zu den Szenarien gemachten Aussagen auf andere Kommunikationsarchitekturen entsprechend übertragbar. In Kapitel V werden für die in Kapitel IV dargestellten Szenarien spezielle Maßnahmen zur Datensicherheit erläutert, die erforderlich sind zur Realisierung der in Kapitel III formulierten Sicherheitsziele und die die hohen Anforderungen an die medizinische Datenverarbeitung berücksichtigen. In Kapitel VI werden schließlich exemplarisch zwei konkrete Ansätze zur Kommunikation im Gesundheitswesen beschrieben.

## **II. Allgemeine datenschutzrechtliche Anforderungen**

Für die Verarbeitung personenbezogener Patientendaten im Rahmen telemedizinischer Anwendungen gelten grundsätzlich die allgemeinen rechtlichen Rahmenbedingungen, die für die Verarbeitung personenbezogener Patientendaten außerhalb telemedizinischer Anwendungen gelten. Die Einführung telemedizinischer Anwendungen darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen. Die Durchsetzung bzw. Konkretisierung der Patientenrechte unter den veränderten technischen Bedingungen bedarf teilweise neuer datenschutzrechtlicher Konzepte.

### **Rechtsgrundlagen**

Für die Verarbeitung von Patientendaten durch niedergelassene Ärzte gelten die Vorschriften des BDSG. Für die Verarbeitung von Patientendaten durch die Krankenhäuser gelten in Bund und Ländern unterschiedliche Rechtsvorschriften. In einzelnen Ländern liegen sog. bereichsspezifische Regelungen der Verarbeitung personenbezogener Daten in Krankenhäusern (Landeskrankengesetze, Gesundheitsdatenschutzgesetze etc.) vor. Soweit keine bereichsspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Vorschriften. Die Religionsgesellschaften treffen für ihren Bereich zum Teil Regelungen in eigener

Zuständigkeit. Darüber hinaus sind die Regelungen der Berufsordnung und des Strafgesetzbuchs zu beachten.

Auf der Grundlage des Behandlungsvertrages in Verbindung mit den jeweils maßgeblichen datenschutzrechtlichen Vorschriften darf der Arzt die für die Durchführung der Behandlung erforderlichen Daten verarbeiten. Soweit die Verarbeitung der Daten nicht für die Durchführung der Behandlung erforderlich ist (z. B. zusätzliche Datenerhebungen für ein Forschungsvorhaben), bedarf es einer besonderen Einwilligung des Patienten.

Unabhängig vom verwendeten Datenträger muss der Arzt parallel zu den datenschutzrechtlichen Vorschriften die in der Berufsordnung und in § 203 StGB normierte Schweigepflicht beachten, ferner das in § 5 BDSG und den entsprechenden landesrechtlichen Bestimmungen geregelte Datengeheimnis. Gehilfen des Arztes unterliegen ebenfalls der ärztlichen Schweigepflicht.

### **Dokumentationspflicht**

Nach der Berufsordnung ist der Arzt verpflichtet, die erforderlichen Aufzeichnungen über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Es handelt sich um eine unselbstständige vertragliche Nebenpflicht aus dem Behandlungsvertrag. Ist die Dokumentation lückenhaft, kann dies im Haftungsprozess eine Umkehr der Beweislast zugunsten des Patienten nach sich ziehen, wenn die Aufklärung des Sachverhalts für den Patienten insgesamt erschwert wird.

### **Befugnis zur Übermittlung bzw. Weitergabe von Patientendaten**

Der Arzt darf personenbezogene Patientendaten nur im Rahmen der datenschutzrechtlichen Vorschriften und befugt i. S. v. § 203 StGB offenbaren. Eine Befugnis zur Offenbarung kann sich insbesondere aus einer gesetzlichen Regelung (z. B. Krebsregistergesetz, Infektionsschutzgesetz, Sozialgesetzbuch V), aus dem Behandlungsvertrag oder der speziellen Einwilligung des Patienten ergeben. Die ärztliche Schweigepflicht gilt grundsätzlich auch zwischen Ärzten. Eine Übermittlung personenbezogener Daten an einen vor-, mit- oder nachbehandelnden Arzt bedarf daher der Einwilligung des Patienten.

Nach den datenschutzrechtlichen Regelungen müssen Einwilligungen bestimmte Anforderungen erfüllen, um rechtswirksam zu sein. Insbesondere muss die Freiwilligkeit der Einwilligung gewährleistet sein und der Betroffene muss zuvor über Umfang und Zweck der geplanten Verarbeitung seiner Daten, die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung informiert werden (vgl. z. B. § 4a Abs. 1 Satz 1 und 2 BDSG). Pauschale Einwilligungserklärungen, deren Tragweite der Betroffene nicht übersehen kann, sind daher unzulässig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände im Einzelfall eine andere Form angemessen ist (vgl. z. B. § 4a Abs. 1 Satz 3, Abs. 2 BDSG). Die Landeskrankenhausgesetze enthalten bez. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte und an Angehörige zum Teil hiervon abweichende Regelungen (z. B. Widerspruchsrecht des Patienten nach Information über die geplante Datenübermittlung).

Spezialregelungen zur Einwilligung des Versicherten sind insbesondere im SGB V enthalten. Durch das GKV– Gesundheitsreformgesetz 2000 wurden Regelungen zur verstärkten Kooperation und Kommunikation zwischen den Leistungserbringern in das SGB V aufgenommen:

- § 73 Abs. 1b SGB V enthält eine Spezialregelung zur zentralen Dokumentation beim Hausarzt. Ein Hausarzt darf mit schriftlicher (widerruflicher) Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die behandelnden Leistungserbringer sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten die Behandlungsdaten und Befunde zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher (widerruflicher) Einwilligung des Versicherten, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu beschaffen und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen.
- In § 140a ff. SGB V sind Regelungen zur sog. integrierten Versorgung enthalten. Die Teilnahme der Versicherten an den integrierten Versorgungsformen ist freiwillig. Die Vertragspartner müssen u.a. die Gewähr dafür übernehmen, dass sie eine an dem Versorgungsbedarf orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten sicherstellen, einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und einer ausreichenden Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss. Der Leistungserbringer darf aus der gemeinsamen Dokumentation die den Versicherten betreffenden Behandlungsdaten und Befunde nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist.

Das Vorzeigen der Krankenversichertenkarte durch den Patienten beim behandelnden Arzt kann nicht als Einwilligung in die Anforderung bzw. den Abruf von medizinischen Daten bei anderen Ärzten qualifiziert werden, da der Patient in jedem Fall beim behandelnden Arzt seine Krankenversichertenkarte zum Nachweis der Leistungsberechtigung vorlegen muss. Eine pauschale Einwilligung des Patienten, eine Krankenversichertenkarte mit medizinischen Daten zu verwenden, die bei jedem Arztbesuch vorgezeigt werden muss, ist nach den dargelegten rechtlichen Anforderungen an Einwilligungen unzulässig. Entsprechendes gilt für eine pauschale Einwilligung des Patienten, dass ein Teil seiner Krankheitsdaten in einem zentralen Datenbestand zum Abruf durch andere Ärzte bereitgehalten werden darf.

### **Informationsrechte des Patienten**

Nach der Rechtsprechung des BGH hat der Patient grundsätzlich ein Recht auf Einsicht in seine Krankenunterlagen, soweit sie sog. objektive Daten betreffen. Es handelt sich um einen Nebenanspruch aus dem Behandlungsvertrag. Für den Bereich der Psychiatrie hat die Rechtsprechung Ausnahmen formuliert. Die – gegenüber der Rechtsprechung vorrangigen – datenschutzrechtlichen Regelungen (Lan–

deskrankenhausgesetze, Gesundheitsdatenschutzgesetze, allgemeine datenschutzrechtliche Regelungen) legen zum Teil weitergehende Rechte der Patienten auf Information, Auskunft und Einsicht fest.

Im Bereich der Telemedizin ist es besonders wichtig, dass der Patient in allen Verarbeitungsphasen ausreichend informiert ist über die Verarbeitung seiner personenbezogenen Daten. Dies setzt voraus, dass das ihn informierende Personal ebenfalls ausreichend informiert ist. Es muss insbesondere auch gewährleistet sein, dass dem Patienten bei Vertragsabschluss bzw. Einwilligung Umfang, Zweck und Rechtsgrundlage der Verarbeitung seiner Daten sowie ggf. die Grundzüge des technischen Verfahrens der Verarbeitung (z. B. bei Chipkartenverfahren) bekannt gegeben worden sind.

### **Datenverarbeitung im Auftrag durch externe Dritte**

In zunehmendem Ausmaß werden personenbezogene medizinische Patientendaten durch externe Dritte verarbeitet. Wenn ein Arzt personenbezogene Patientendaten für eine Auftragsdatenverarbeitung (z. B. Mikroverfilmung, Schreifarbeiten, externe Archivierung) an einen externen Dritten weitergibt, so ist dies keine Datenübermittlung im Sinne der datenschutzrechtlichen Regelungen, da der Arzt als Auftraggeber datenverarbeitende Stelle bleibt. Da die Weitergabe der personenbezogenen Patientendaten an einen externen Dritten jedoch eine Durchbrechung der ärztlichen Schweigepflicht darstellt, benötigt der Arzt für diese Datenweitergabe eine rechtliche Befugnis i. S. v. § 203 StGB. Einige Landeskrankenhausgesetze sehen z. B. die Möglichkeit einer Auftragsdatenverarbeitung für die Krankenhäuser vor. Sofern keine Rechtsvorschrift als Rechtsgrundlage für eine befugte Offenbarung der Patientendaten an einen externen Dritten vorhanden ist, kommt grundsätzlich nur eine Einwilligung der Betroffenen als Rechtsgrundlage für die Datenweitergabe in Betracht.

Wenn sichergestellt werden kann, dass der externe Dritte (Auftragnehmer) keine personenbezogenen medizinischen Daten zur Kenntnis nehmen kann (z. B. bei Konzepten zur digitalen externen Archivierung, bei denen eine Verschlüsselung aller Informationen vorgesehen ist), liegt keine Durchbrechung der ärztlichen Schweigepflicht vor.

Auch wenn eine Rechtsgrundlage für eine Datenweitergabe zur Auftragsdatenverarbeitung vorliegt, müssen die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit getroffen werden. Dies bedeutet insbesondere auch, dass der Kreis derjenigen Personen, die personenbezogene Patientendaten zur Kenntnis erhalten, soweit wie möglich begrenzt werden bzw. u. U. sogar eine Kenntnisnahme der personenbezogenen Patientendaten ausgeschlossen werden muss.

Die beim Arzt gespeicherten Patientendaten unterliegen dem Beschlagnahmeverbot i. S. v. § 97 Abs. 1 StPO. Das Beschlagnahmeverbot schützt das Vertrauensverhältnis zwischen dem zeugnisverweigerungsberechtigten Arzt und dem Betroffenen. Das Beschlagnahmeverbot erstreckt sich nur auf Gegenstände, die sich im Gewahrsam des Zeugnisverweigerungsberechtigten befinden. Wenn sich die Patientendaten nicht im Gewahrsam des Zeugnisverweigerungsberechtigten befinden, sondern im Gewahrsam eines externen Dritten, findet das Beschlagnahmeverbot des § 97 StPO keine Anwendung, d. h. der Schutz der Patientenrechte verschlech-

tert sich. Fraglich ist, ob das Beschlagnahmeverbot ausnahmsweise auch bei Gewahrsam eines externen Dritten Anwendung findet, wenn der externe Dritte (Auftragnehmer) ein Arzt ist. Mangels einer gerichtlichen Entscheidung kann dies nicht als gesichert angesehen werden, denn der Arzt wird hier nicht als behandelnder Arzt tätig, sondern übernimmt eine kommerzielle Tätigkeit.

### **Abruf von Patientendaten über ein Datennetz**

Patientendaten können nach Erteilung einer Einwilligung des Patienten im Einzelfall für einen Zugriff durch den Berechtigten freigegeben werden. Ein Zum – Abruf – Bereitstellen (vgl. z. B. § 10 BDSG) von Patientendaten durch einen Arzt über ein Datennetz ist nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig. Ein Arzt ist verpflichtet, vor einer Übermittlung zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt. Würde ein Arzt die Patientendaten für einen Abruf durch andere Behandlungseinrichtungen bereithalten und käme es dann zu einem Abruf, der rechtlich nicht (z. B. durch eine Einwilligung des Patienten) legitimiert ist, so hätte sich der speichernde Arzt nach § 203 StGB strafbar gemacht. Eine Offenbarung von Patientendaten kann auch dadurch vorgenommen werden, dass nicht verhindert wird, dass die Daten durch externe Dritte abgerufen werden können.

## **III. Grundlegende Sicherheitsanforderungen**

Das Bundesdatenschutzgesetz verlangt in § 9 allgemein technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten. Die in der Anlage zu § 9 BDSG beschriebenen Regelungen (die auch denen einiger Länderdatenschutzgesetze entsprechen) definieren Sicherheitsmaßnahmen und haben im Wesentlichen die technischen Komponenten von Datenverarbeitungsanlagen zum Gegenstand. Dadurch sind sie stark technologieabhängig und anpassungs- bzw. erläuterungsbedürftig. Deshalb empfiehlt es sich, sich – wie im Folgenden – zukünftig auf einem abstrakteren Niveau an primär an den Daten ausgerichteten Sicherheitszielen zu orientieren. Dies ist bereits im Rahmen der Novellierung des Datenschutzrechtes in einigen Ländergesetzen geschehen. Sofern andere gesetzliche Regelungen noch den herkömmlichen Katalog der "Zehn Gebote des Datenschutzes" enthalten, sind diese bei Beachtung der Grundziele und ihrer Umsetzung innerhalb eines Datenschutzkonzeptes in jedem Fall abgedeckt.

Im Folgenden werden die grundlegenden Sicherheitsziele definiert, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen:

### **1. Vertraulichkeit**

"Wer sich in Behandlung begibt, muss und darf erwarten, dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt. Nur so kann zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt, weil es die Chancen der Heilung vergrößert und damit – im ganzen gesehen – der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient." (BVerfGE 32, 373, 380). Die in der ärztlichen Berufsordnung und dem Strafgesetzbuch normierte ärztliche Schweigepflicht schützt das Vertrauensverhältnis zwischen Patient und Arzt. Der Arzt muss die Vertraulichkeit der erhobenen,

gespeicherten, übermittelten oder sonst verarbeiteten Daten gewährleisten, d.h. nur Befugte dürfen personenbezogene Daten zur Kenntnis erhalten bzw. davon Kenntnis nehmen können. Auch die datenschutzrechtlichen Regelungen, die das Recht des Patienten auf informationelle Selbstbestimmung konkretisieren, schützen die Vertrauensbeziehung zwischen Patient und Arzt. Eine Kenntnisnahme medizinischer Daten durch Unbefugte (z. B. Arbeitgeber, Versicherungen, Pharmaindustrie) kann erhebliche soziale bzw. materielle Folgen für den Patienten nach sich ziehen.

## **2. Authentizität (Zurechenbarkeit)**

Die Authentizität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. der Urheber von patientenbezogenen bzw. der Verantwortliche für patientenbezogene Daten sowie der Auslöser eines Verarbeitungsvorgangs bzw. der Verantwortliche für einen Verarbeitungsvorgang muss jederzeit eindeutig feststellbar sein. Ggf. kann auch die Art und Weise der Erhebung der Daten von Bedeutung sein (z. B. Datenerhebung durch ein medizinisches Gerät). Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen und Begutachtungen ungeeignet.

## **3. Integrität**

Die Integrität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. personenbezogene Daten müssen während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben. Der Behandlungsauftrag in Einrichtungen des Gesundheitswesens umfasst eine sorgfältige Diagnose und Therapie mit dem Ziel der Heilung des Patienten. Die Echtheit, Korrektheit und Vollständigkeit der Daten, vor, während und nach der Bearbeitung und Übertragung ist für die Erfüllung des Behandlungsauftrags von großer Bedeutung. Eine Verfälschung oder Unvollständigkeit der Daten kann zu falschen medizinischen Entscheidungen mit u. U. lebensbedrohenden Folgen für den Patienten führen, verbunden mit rechtlichen Konsequenzen für den Mediziner.

## **4. Verfügbarkeit**

Die Verfügbarkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Die zeitgerechte Verfügbarkeit medizinischer Informationen kann entscheidend sein für eine erfolgreiche Erfüllung des Behandlungsauftrags. Nicht oder nicht rechtzeitig zur Verfügung stehende Daten können zur Handlungsunfähigkeit bzw. zu einem zu späten Handeln oder Behandlungsfehlern des Mediziners führen und u. U. lebensbedrohende Folgen für den Patienten sowie rechtliche Konsequenzen für den Mediziner haben. Die Verfügbarkeit der Daten impliziert natürlich die Verfügbarkeit der zur ordnungsgemäßen Verarbeitung erforderlichen Komponenten (Hard- und Software) des IT-Systems.

## **5. Revisionsfähigkeit**

Die Revisionsfähigkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können und es muss festgestellt werden können, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat. Für den Arzt bzw. das Krankenhaus besteht nach der Berufsordnung die Pflicht zur Dokumentation der Behandlung. Sie ist eine unselbstständige Nebenpflicht aus dem Behandlungsvertrag. Eine lückenhafte Dokumentation kann im Haftungsprozess eine Beweislastumkehr zugunsten des Patienten nach sich ziehen. Es muss nachvollziehbar sein, wer welche Diagnose gestellt und welche Therapie verordnet hat und aufgrund welcher Daten ein Arzt seine Entscheidung über Behandlungsmaßnahmen getroffen hat. Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Authentizität.

## **6. Validität**

Die Validität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d.h. personenbezogene Daten müssen aktuell in der für den Nutzungszweck angemessenen Qualität verarbeitet werden. Diese Forderung betrifft insbesondere Bilddaten, bei denen es auf Qualitätsmerkmale wie Bildauflösung und Farbechtheit ankommt. Die Validität wird von der Integrität nicht umfasst, da die Daten zwar integer im Sinne von vollständig und unversehrt sein können, die Darstellungsqualität und Aktualität aber dennoch für medizinische Nutzungszwecke unzureichend sein kann.

## **7. Rechtssicherheit**

Für jeden Verarbeitungsvorgang und dessen Ergebnisse ist der Verursachende bzw. Verantwortliche beweiskräftig nachweispflichtig. Ist die Rechtssicherheit nicht gegeben, können Patienten eventuelle Schadensansprüche u. U. nicht geltend machen bzw. können Mediziner u. U. die Korrektheit ihres Handelns nicht nachweisen. Die notwendige Voraussetzung für die Gewährleistung der Rechtssicherheit ist die Gewährleistung der Revisionsfähigkeit. Die Revisionsfähigkeit alleine gewährleistet aber noch nicht die beweiskräftige Überprüfbarkeit von Verarbeitungsvorgängen in gerichtlichen Verfahren.

## **8. Nicht-Abstreitbarkeit von Datenübermittlungen**

Die Nicht-Abstreitbarkeit des Sendens und des Empfangens von patientenbezogenen Dokumenten muss gewährleistet sein. D.h. einerseits ist zu gewährleisten, dass der Sender eines patientenbezogenen Dokuments sicher sein kann, dass das Dokument seinen Empfänger erreicht hat, und er darf nicht abstreiten können, genau dieses Dokument an genau den Empfänger gesendet zu haben. Andererseits muss der Empfänger eines patientenbezogenen Dokuments sicher sein können, genau dieses Dokument von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau das Dokument von einem bestimmten Sender empfangen zu haben. Die Nicht-Abstreitbarkeit ist eine Voraussetzung der Revisionsfähigkeit.

## 9. Nutzungsfestlegung

Medizinische Datenverarbeitungssysteme müssen es ermöglichen, für jedes patientenbezogenes Dokument den Nutzerkreis sowie abgestufte Nutzungsrechte festzulegen und Nutzungsausschlüsse zu definieren.

## IV. Formen der Datenhaltung

In diesem Kapitel werden Systeme zur einrichtungsübergreifenden Verarbeitung patientenbezogener Daten in Kategorien unterteilt, die in den folgenden Szenarien beschrieben werden. Die Kriterien für die Kategorisierung orientieren sich an den grundlegenden Formen der Datenhaltung. Es ist zu erwarten, dass jedes medizinische Datenverarbeitungssystem zur einrichtungsübergreifenden Kommunikation einer dieser Kategorien angehört oder sich als eine Kombination dieser darstellt. Damit wird es möglich Systeme einzuordnen und die zu den einzelnen Szenarien getroffenen Aussagen entsprechend auf das jeweils zu betrachtende System zu übertragen.

### Szenario 1: Dezentrale Datenhaltung:

Bei der dezentralen Datenhaltung werden die Daten dort gespeichert, wo sie auch erzeugt wurden. Somit hat jede medizinische Einrichtung ihre eigene Datenhaltung. Die Datenhaltungssysteme der verschiedenen Einrichtungen können zwar über ein Netz miteinander kommunizieren, sind aber ansonsten als vollständig autonom anzusehen. Systemübergreifende einheitliche Dienste gibt es nicht.

Bei einer dezentralen Architektur muss für jeden Kommunikationsvorgang explizit eine Kommunikationsverbindung zwischen dem sendenden und dem empfangenden System aufgebaut werden. Die Initiierung der Kommunikation erfolgt durch den Sender. Dies erfordert, dass vor jeder Übermittlung von Dokumenten eines Patienten dem Sender (z. B. dem überweisenden Arzt) der Empfänger (z. B. der weiterbehandelnde Arzt) bekannt sein muss. Eine nicht-adressierte Kommunikation ist nicht möglich. Die Realisierung einer einrichtungsübergreifenden elektronischen Patientenakte ist daher nicht bzw. nur sehr eingeschränkt möglich (z. B. fallbezogen durch jeweiliges Mitsenden der bereits vorhandenen Dokumente).

Jede Einrichtung ist datenverarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Daten. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte sind nur aufgrund einer rechtlichen Legitimation (z. B. Einwilligung des Patienten im Einzelfall) zulässig. Spezielle rechtliche oder rechtspolitische Probleme bzgl. der ärztlichen Schweigepflicht entstehen bei der dezentralen Datenhaltung nicht.

### Szenario 2: Zentrale Datenhaltung:

Bei der zentralen Datenhaltung werden Daten, deren Verarbeitung in der Verantwortung verschiedener medizinischer Einrichtungen liegt, (technisch) zentral zusammengeführt und in einem zentralen System gespeichert. Es gibt keine redundanten Datenbestände, d.h. bei den verschiedenen beteiligten Einrichtungen selbst werden keine Daten gespeichert.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle i. S. der Datenschutzgesetze für ihre eigenen Datenbestände. Eine einrichtungsübergreifende zentrale Datenhaltung kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein (s. Kapitel II). Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmeschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist und dass Dritte Kenntnis der medizinischen Daten erhalten. In jedem Fall muss die Möglichkeit der Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten soweit wie möglich ausgeschlossen werden.

Im übrigen ist die ärztliche Schweigepflicht gewahrt, wenn der Zugriffskontrollmechanismus des Zentralsystems gewährleistet, dass jede Einrichtung nur auf die eigenen Daten zugreifen kann.

Datenübermittlungen zwischen den angeschlossenen Einrichtungen werden technisch durch entsprechende Rechtevergaben realisiert. Will ein Mediziner der Einrichtung A ein Dokument X an einen Mediziner der Einrichtung B übermitteln, veranlasst er, dass dieser die Zugriffsrechte für dieses Dokument erhält.

Wie bei Szenario 1 muss eine rechtliche Legitimation für die Datenübermittlungen vorliegen. Der Patient kann einwilligen, dass seine Daten einem bestimmten Arzt übermittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Daten zum Abruf durch einen später von ihm bestimmten Arzt bereitgehalten werden. Die Voraussetzungen, unter denen ein Arzt auf die Daten zugreifen darf, müssen in der Einwilligungserklärung festgelegt sein. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Zugriff durch den jeweiligen Arzt vorliegen.

Mit diesem Modell ist die elektronische Patientenakte sowohl fallbezogen als auch umfassend realisierbar, soweit die einen Patienten behandelnden Einrichtungen bzw. Ärzte sich an der zentralen Datenhaltung beteiligen und die Einwilligung des Patienten vorliegt.

Unter rechtspolitischen Gesichtspunkten ist die zentrale Datenhaltung problematisch, weil eine zentrale Datensammlung über Patienten neue Missbrauchsmöglichkeiten eröffnet und neue Begehrlichkeiten nach weiteren zentralen Auswertungs- und Verwendungsmöglichkeiten der Patientendaten wecken kann.

### **Szenario 3: Verteilte Datenhaltung**

Bei der verteilten Datenhaltung werden, wie im Falle der dezentralen Datenhaltung, die Daten auf den Systemen der Einrichtungen gespeichert, die sie auch erzeugt haben. Darüber hinaus gibt es aber systemübergreifende Dienste, die dafür sorgen, dass die einzelnen dezentralen Systeme zu einem Kommunikationsverbund zusammengeschlossen werden. Damit sind die dezentralen Systeme Subsysteme des durch den Verbund entstandenen Gesamtsystems. Den Nutzern eines verteilten Systems bleibt die physikalische Verteilung der Daten auf eine Vielzahl von Subsystemen verborgen (Verteilungstransparenz) und ihnen wird der Eindruck vermittelt, als arbeiten sie mit einem Zentralsystem. Ein verteiltes System benötigt Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente sowie einen systemweiten Zugriffskontrollmechanismus.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle i. S. der Datenschutzgesetze für ihre eigenen Datenbestände. Datenübermittlungen zwischen den verschiedenen Einrichtungen, d.h. zwischen dezentralen Subsystemen, erfordern wie bei der zentralen Datenhaltung eine rechtliche Legitimation und eine entsprechende Rechtevergabe. Möchte ein Mediziner der Einrichtung A (Nutzer des Subsystems A) auf ein Dokument zugreifen, prüft der systemweite Zugriffskontrollmechanismus, ob er die entsprechenden Zugriffsrechte besitzt. Ist dies der Fall, ermittelt ein Systemdienst auf der Grundlage der Metainformationen den Lagerort des Dokumentes. Ist das Dokument bei Subsystem A gespeichert (also ein Dokument der Einrichtung A), erfolgt ein lokaler Datenzugriff. Ist das Dokument bei Subsystem B gespeichert (also ein Dokument der Einrichtung B), erfolgt ein entfernter Zugriff auf Subsystem B unter Nutzung von Kommunikationsmechanismen, ohne dass der Nutzer Kenntnis des Speicherortes haben muss.

Bei der verteilten Datenhaltung bleiben die verschiedenen Einrichtungen datenverarbeitende Stelle i. S. der Datenschutzgesetze für ihre eigenen Daten. Grundsätzlich ist die ärztliche Schweigepflicht gewahrt, wenn jede Einrichtung nur auf ihre eigenen Daten zugreifen kann.

Der Patient kann einwilligen, dass seine Daten an einen bestimmten Arzt übermittelt werden. Es ist auch möglich, dass ein Teil seiner Daten für externe Zugriffe durch später von ihm bestimmte Ärzte unter den von ihm bestimmten Voraussetzungen bereitgehalten werden. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Datenzugriff durch den jeweiligen Arzt vorliegen. Der Aufbau einer einrichtungsübergreifenden ("virtuellen") elektronischen Patientenakte ist bei diesem Modell möglich.

Bei der verteilten Datenhaltung wird das o. a. rechtspolitische Problem der zentralen Datenhaltung gemildert, da selbst im "worst case" nur die Daten zusammengeführt werden können, die für externe Zugriffe freigegeben wurden. Der Beschlagnahmenschutz für die Patientendaten bleibt erhalten. Da die verteilte Datenhaltung keine Datenverarbeitung im Auftrag erforderlich macht, ist das Problem der Kenntnisnahme von personenbezogenen medizinischen Patientendaten durch externe Dritte nicht gegeben.

#### **Szenario 4: Dezentrale Datenhaltung mit zentraler Komponente**

Bei dieser Datenhaltungsform findet eine dezentrale Datenhaltung bei den einzelnen medizinischen Einrichtungen statt. Außerdem können Dokumente der verschiedenen Einrichtungen an einer zentralen Stelle temporär (technisch) zusammengeführt werden.

Die verschiedenen Einrichtungen bleiben datenverarbeitende Stelle i. S. der Datenschutzgesetze für ihre eigenen Daten, auch bei der zentralen Speicherung eines Teildatenbestandes. Bei diesem Modell bildet die zentrale Speicherkomponente einen Puffer, der allen angeschlossenen Einrichtungen zum Up- und Download zur Verfügung steht. Dokumente werden vom Sender auf diesen zentralen Speicher übertragen (Upload) und können dann vom Empfänger von dort abgeholt (Download) werden. Rechtlich handelt es sich beim Up- und dem zugehörigen Download um eine Datenübermittlung, die einer rechtlichen Legitimation (z. B. Einwilligung des Patienten) bedarf. Der Patient kann im Einzelfall einwilligen, dass seine Daten einem bestimmten Arzt über die zentrale Speicherkomponente über-

mittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Krankheitsdaten in den zentralen Datenbestand eingestellt wird und dort zum Abruf durch später von ihm bestimmte Ärzte bereitgehalten wird. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Abruf der Daten durch den jeweiligen Arzt vorliegen. Auf dem zentralen Speicher können Dokumente zur (fallbezogenen) elektronischen Patientenakte zusammengeführt werden, soweit der den Patienten behandelnde Arzt an die zentrale Speicherkomponente angeschlossen ist und eine Einwilligung des Patienten in die Bereitstellung der Daten für den Abruf durch andere Ärzte vorliegt.

Die zentrale einrichtungsübergreifende Speicherung eines Teildatenbestandes aller Einrichtungen kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein. Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmenschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist. Die Möglichkeiten einer Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten müssen in jedem Fall soweit wie möglich ausgeschlossen werden.

Bei der dezentralen Datenhaltung mit zentraler Komponente entsteht das auch bei der zentralen Datenhaltung dargelegte rechtspolitische Problem: Es entsteht eine neue zentral (Teil-)Datensammlung, die neue Möglichkeiten des Datenmissbrauchs eröffnet und neue Begehrlichkeiten nach weiteren zentralen Datenauswertungen und -verwendungen wecken kann.

## **V. Spezielle Datensicherheitsmaßnahmen**

Zur Realisierung der in Kapitel III definierten Sicherheitsziele sind für jedes medizinische Datenverarbeitungssystem auf der Grundlage einer Bedrohungs- und Risikoanalyse die individuell erforderlichen Sicherheitsmaßnahmen zu ermitteln. Naturgemäß ergibt sich eine Vielzahl zu treffender technischer und organisatorischer Sicherheitsmaßnahmen, die abhängig von den jeweiligen technischen Systemausprägungen und den unterschiedlichen Rahmenbedingungen von System zu System sehr unterschiedlich sein können. Aufgrund des hohen Schutzbedarfs der Daten, die von medizinischen Systemen verarbeitet werden, ergeben sich aber spezielle Sicherheitsmaßnahmen, die aus datenschutzrechtlicher Sicht als unabdingbar anzusehen sind. Diese Maßnahmen werden im Folgenden für die einzelnen Sicherheitsziele und Systemarchitekturen erläutert.

### **1. Sicherstellung der Vertraulichkeit**

Der Vertraulichkeit kommt aufgrund der hohen Sensibilität medizinischer Daten und der Pflicht zur Wahrung des Arzt-Patienten-Geheimnisses eine große Bedeutung zu. Insofern muss bei jeder Phase der Datenverarbeitung sichergestellt werden, dass nur Befugte patientenbezogene Daten zur Kenntnis nehmen können. Eine hinreichende Gewährleistung der Vertraulichkeit mit den hohen Anforderungen des Gesundheitswesens kann nur durch Verschlüsselung der patientenbezogenen Daten mit starken kryptografischen Verfahren erreicht werden. Zum einen ist eine Verschlüsselung aller Daten zu fordern, die über ein Kommunikationsnetz übertragen werden und zwar unabhängig davon, ob es sich um ein lokales oder um ein öf-

fentliches Netz handelt. Daneben sind alle bei den datenhaltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass Systemadministratoren, Wartungspersonal oder sonstige Dritte (z. B. durch Diebstahl) Kenntnis von Daten erhalten, die dem Arzt–Patienten–Geheimnis unterliegen.

### **(a) Verschlüsselung übertragener Daten:**

Die Übertragung patientenbezogener Daten in dezentralen Systemen erfordert eine Verschlüsselung auf Anwendungsebene. Da die Systeme in dezentralen Architekturen autonom sind und sich somit aus der Sicht eines Systems die übrigen Systeme jeweils wie Black Boxes darstellen, kann nur die an Personen adressierte Verschlüsselung sicherstellen, dass nur Befugte die übermittelten Daten zur Kenntnis nehmen können.

In zentralen Systemen reicht eine Verschlüsselung auf Transportebene aus, da alle Nutzer dem Zugangs- und Zugriffskontrollmechanismus des Systems unterliegen.

In einem verteilten System reicht ebenso eine Verschlüsselung auf Transportebene aus, wenn es für den systemübergreifenden Datenaustausch einen einheitlichen, systemweiten Zugangs- und Zugriffskontrollmechanismus gibt.

Die dezentrale Architektur mit zentraler Komponente kann im Prinzip gehandhabt werden wie eine dezentrale Architektur, da die zentrale Komponente die Funktion eines "Postfaches" übernimmt, aus dem sich der Empfänger seine Nachricht abholt.

### **(b) Verschlüsselung gespeicherter Daten:**

Die verschlüsselte Speicherung der Daten bei den datenhaltenden Systemen kann realisiert werden durch den Einsatz entsprechender Systemsoftware (z. B. Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (z. B. Tools zur Verschlüsselung von Plattenbereichen). Eine andere Möglichkeit zur Lösung dieses Problems besteht in der Verschlüsselung der patientenbezogenen Dokumente auf Anwendungsebene. Dabei bietet sich eine Hybridverschlüsselung an, wobei das Dokument selbst mit einem symmetrischen Schlüssel (Session Key) verschlüsselt wird und der symmetrische Schlüssel jeweils mehrfach nach einem asymmetrischen Verfahren mit den öffentlichen Schlüsseln der berechtigten Nutzern. Der für ein Dokument verantwortliche Mediziner legt dann (u.U. unter Mitwirkung des Patienten) bei der Aktivierung des Verschlüsselungsvorgangs die berechtigten Personen fest. Diese Vorgehensweise stellt sicher, dass nur berechtigte Nutzer in die Lage versetzt werden, ein Dokument zu entschlüsseln und realisiert damit gleichzeitig einen Zugriffskontrollmechanismus (bezogen auf Lesevorgänge). Das Verschlüsselungskonzept muss ein Verfahren vorsehen, dass eine Verfügbarmachung der Daten im Notfall gewährleistet.

## **2. Gewährleistung der Authentizität**

Patientenbezogene Dokumente sind von ihrem Urheber bzw. von dem verantwortlichen Mediziner elektronisch zu signieren und mit einem Zeitstempel zu versehen. Nur durch die elektronische Signatur kann die Zurechenbarkeit von Dokumenten zum Urheber bzw. zum Verantwortlichen sichergestellt werden.

Die erforderlichen Mechanismen zur elektronischen Signatur von Dokumenten sind unabhängig von der gewählten Architektur der Datenhaltung.

### **3. Sicherstellung der Integrität**

Mit dem elektronischen Signieren eines patientenbezogenen Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt, da der Signaturvorgang eine bewusste Handlung vom Signierenden erfordert. Der Mediziner, der ein Dokument elektronisch signiert, also sozusagen elektronisch unterschreibt, bestätigt mit seiner Signatur nicht nur, dass er der Urheber bzw. der Verantwortliche ist, sondern gleichzeitig, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Darüber hinaus sichert das der elektronischen Signatur zugrunde liegende kryptografische Verfahren die Erkennbarkeit einer nachträglichen Veränderung eines Dokuments. Die erfolgreiche Verifikation der Signatur eines Dokuments stellt damit gleichzeitig die Unversehrtheit des Dokumenteninhalts sicher.

### **4. Sicherstellung der Verfügbarkeit**

Bei der Sicherstellung der Verfügbarkeit, teilen sich die verschiedenen Architekturansätze in zwei Lager:

- Sowohl im Falle der zentralen Datenhaltung als auch im Falle der dezentralen Datenhaltung mit zentraler Komponente ist eine hohe Verfügbarkeit realisierbar. Da bei der zentralen Datenhaltung ausschließlich die zentrale Datenverarbeitungsanlage Daten speichert und verarbeitet, sind die technischen Möglichkeiten gegeben für diese Anlage und damit für das gesamte System eine Hochverfügbarkeit zu gewährleisten. Die Situation bei der dezentralen Datenhaltung mit zentraler Komponente ist vergleichbar. Die für den einrichtungsübergreifenden Datenaustausch vorgesehenen Daten werden von der zentralen Komponente gespeichert, für die ebenso eine Hochverfügbarkeit realisierbar ist. Einschränkungen der Verfügbarkeit des Gesamtsystems können sich nur ergeben aus einer temporären Nichtverfügbarkeit von angeschlossenen dezentralen Systemen für einen notwendigen Upload oder Download.
- Bei der dezentralen und verteilten Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit aller beteiligten (Sub-)Systeme ab. Bei der dezentralen Datenhaltung müssen die datenhaltenden Systeme als autonom angesehen werden, was einer systemweiten Verfügbarkeitsregelung entgegensteht. Insbesondere im niedergelassenen Bereich dürften sich die Verfügbarkeitszeiten der Systeme auf die Praxiszeiten beschränken, die zudem von Praxis zu Praxis noch unterschiedlich sein können. Insofern ist schon aus organisatorischen Gründen eine hohe Verfügbarkeit des Gesamtsystems nicht realisierbar. Bei der verteilten Datenhaltung müssen Kommunikationsprozesse – im Gegensatz zum dezentralen Fall – nicht explizit von den Nutzern eines Subsystems initiiert werden, sondern können durch systemweit verfügbare Kommunikationsmechanismen angestoßen werden. Insofern wird die Verfügbarkeit nicht notwendigerweise von beschränkten Praxiszeiten determiniert. Allerdings kann es zu technisch bedingten Ausfällen von Subsystemen kommen, die ohne Eingriffe vor Ort nicht behebbar sind. Solchen Schwierigkeiten kann man technisch dadurch begegnen, dass Datenreplikate an verschiedenen Speicherorten vorge-

halten werden. Bei Nichtverfügbarkeit eines bestimmten Subsystems wird dann auf das entsprechende Replikat zurückgegriffen. Diese Vorgehensweise ist allerdings datenschutzrechtlich als sehr problematisch einzustufen, wenn die Replikate sich nicht im selben Herrschaftsbereich befinden, wie ihre Originale. Außerdem ergeben sich durch Replikate nicht zu unterschätzende Konsistenzprobleme. Letztlich ist auch im verteilten Fall die Verfügbarkeit abhängig von der Verfügbarkeit der beteiligten Subsysteme. Eine Hochverfügbarkeit dürfte nicht oder nur mit sehr hohem Aufwand realisierbar sein.

## **5. Gewährleistung der Revisionsfähigkeit**

Grundvoraussetzung für die Gewährleistung der Revisionsfähigkeit ist das elektronische Signieren der patientenbezogenen Dokumente, weil hiermit die Verantwortlichkeit bzw. Urheberschaft anerkannt wird. Da der Inhalt ein signierten Dokuments nachträglich nicht mehr verändert werden kann, ohne die Signatur zu verletzen, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdokument plus Ergänzungen wiederum digital signiert, kann die Historie eines Dokuments manipulationssicher festgehalten werden.

Die von der Dokumentensignatur nicht erfassbaren Verarbeitungsschritte des Übermitteln eines Dokuments und des Lesen eines Dokuments sind mittels einer manipulationssicheren Protokollierung einer Revision zugänglich zu machen. Das vollständige Löschen eines Dokuments muss aus Gründen der Dokumentationspflicht in jedem Fall vom Zugriffskontrollmechanismus unterbunden werden.

Eine Protokollierung ist bei zentralen Systemen naturgemäß recht einfach und umfassend zu realisieren, da hierbei die Datenverarbeitung von nur einem System vorgenommen wird, welches damit auch die Kontrolle über alle Verarbeitungsphasen eines Dokuments hat und außerdem die einzelnen Verarbeitungsschritte den Personen zuordnen kann, die sie verursacht haben.

Hingegen durchläuft ein Dokument im Zuge seiner Verarbeitung bei einem dezentralen System u. U. mehrerer lokale Systeme. Da es in einem dezentralen System keine zentrale Kontrollinstanz über die Verarbeitungsschritte der Einzelsysteme gibt, ist eine zentrale Protokollierung nicht möglich. Hier bleibt nur die Protokollierung durch die lokalen Systeme. Die Protokollierung von Lesevorgängen ist problemlos möglich. Die Protokollierung von Übermittlungsvorgängen erfordert allerdings die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten. Für die Revision der Gesamtheit aller Verarbeitungsschritte eines Dokuments ist allerdings das Zusammenführen der relevanten Protokolldaten aller lokaler Systeme erforderlich, die das Dokument durchlaufen hat.

Bei verteilten Systemen können systemweit zur Verfügung stehende Dienste zur Protokollierung von Verarbeitungsschritten genutzt werden, die systemübergreifende Wirkung haben (also im Wesentlichen Datenübermittlungen). Alle anderen Aktivitäten, die nicht von systemweiten Diensten abhängen, können wie in dezentralen Systemen nur von den beteiligten lokalen Subsystemen protokolliert werden.

Die dezentrale Datenhaltung mit zentraler Komponente erlaubt eine Protokollierung aller Aktivitäten, die sich auf die zentrale Komponente beziehen, wie die zentrale Datenhaltung. Alle Aktivitäten, die sich auf die lokalen Systeme beschränken, müs-

sen von diesen protokolliert werden. Die Protokollierung von Datenübermittlungen zwischen den lokalen Systemen und der zentralen Komponente erfordert wiederum die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten.

## **6. Gewährleistung der Validität**

Die Sicherstellung der Validität ist prinzipiell unabhängig von der Architektur der beteiligten Systeme. Sie ist aber in hohem Maße abhängig von einer Standardisierung der für die Validität relevanten Systemkomponenten (Hard- und Softwarekomponenten). Insofern ist anzunehmen, dass eine valide Datenverarbeitung umso schwieriger herstellbar ist, je heterogener die zu betrachtende Systemlandschaft ist.

## **7. Gewährleistung der Rechtssicherheit**

Die Voraussetzung für die Rechtssicherheit ist die Revisionsfähigkeit und damit auch das elektronische Signieren eines jeden patientenbezogenen Dokuments. Damit eine elektronische Signatur rechtsverbindlich einer verantwortlichen Person zugeordnet werden kann, bedarf es der qualifizierten Signatur. Erst die qualifizierte Signatur gewährleistet eine rechtswirksame Überprüfbarkeit der Zuordnung einer Signatur zu der Person, die die Signatur erzeugt hat.

## **8. Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen**

Die Nichtabstreitbarkeit des Sendens und Empfangs spielt primär eine Rolle in Architekturen mit dezentraler Ausrichtung, da aufgrund der Autonomie der lokalen Systeme eine Datenübermittlung explizit von einem Systemnutzer angestoßen werden muss und es keine systemübergreifenden Kontrollmechanismen gibt, die einen Übermittlungsvorgang technisch überwachen und im Fehlerfall entsprechende Maßnahmen einleiten.

Die Nicht-Abstreitbarkeit in einem dezentralen System ist nur über ein Quittungsverfahren unter Verwendung elektronischer Signaturen zu realisieren. Der Sender eines Dokuments versieht dieses zunächst mit einer elektronischen Signatur und sendet es an den Empfänger. Der Empfänger verifiziert die Signatur, um festzustellen, ob das Dokument von dem angegebenen Sender stammt. Dann muss der Empfänger dem Sender bestätigen, dass er ein Dokument mit bestimmten Inhalt von ihm bekommen hat. Diese Empfangsbestätigung kann realisiert werden, indem von dem empfangenen Dokument der Hashwert gebildet wird und dieser zusammen mit einem das Dokument identifizierenden Merkmal (und evtl. mit der Eingangszeit) vom Empfänger elektronisch signiert an den Sender gesendet wird. Der Sender verifiziert die Signatur der Quittung, bildet seinerseits den Hashwert des von ihm gesendeten Dokuments und vergleicht diesen mit dem in der Quittung zugesandten Hashwert. Stimmen beide Werte überein, kann der Sender sicher sein, dass genau der von ihm spezifizierte Empfänger (aufgrund der Signaturverifikation) auch genau das von ihm gesendete Dokument (aufgrund des Vergleichs der Hashwerte) erhalten hat. Schlägt die Signaturverifikation oder der Hashwertvergleich fehl, muss sich der Sender mit dem Empfänger in Verbindung setzen. Erhält der Empfänger keine Reklamation durch den Sender, dann kann er seinerseits sicher sein, dass das empfangene Dokument genau von dem vermuteten Sender kommt, mit genau dem vom Sender gesendeten Inhalt. Erhält bei diesem Quittungsverfahren der Sender nach einer gewissen Zeit keine Quittung für seine gesendete Nachricht, so ist entweder

die Nachricht oder die Quittung nicht zugestellt worden. Für diesen Fall ist eine adäquate Handlungsweise zu vereinbaren (z. B. erneutes Senden der Nachricht nach einer Wartefrist oder Kontaktieren des Empfängers).

Solch ein Quittungsverfahren ist natürlich softwaretechnisch entsprechend so zu unterstützen, dass es so weit wie möglich automatisiert abläuft. Ein Standard-Email-System ist nicht in der Lage, die Forderung der Nicht-Abstreitbarkeit zu erfüllen. Bei einem dezentralen System mit zentraler Komponente ist ein solches Quittungsverfahren in modifizierter Form ebenfalls realisierbar. Hier erhält der Sender einer Nachricht eine Quittung von der zentralen Komponente und der Empfänger sendet seine Quittung an die zentrale Komponente. Die Nicht-Abstreitbarkeit ist dann über die Informationskette Sender, Protokolldaten der zentralen Komponente, Empfänger herstellbar.

Die Signatur von Dokumenten zur Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen ist nicht zu verwechseln mit der Signatur von Dokumenten zur Gewährleistung der Authentizität. Im ersten Fall dient die Signatur der Zuordnung eines Dokuments zu seinem Sender, im zweiten Fall der Zuordnung eines Dokuments zu seinem Urheber. Da der Sender eines Dokuments aber nicht notwendigerweise auch der Urheber ist, muss jedes Dokument bei einer Übermittlung vom Sender elektronisch signiert werden.

Bei zentralen und verteilten Architekturen ist die Nicht-Abstreitbarkeit auf der Grundlage der entsprechenden Protokollinformationen realisierbar.

## **9. Gewährleistung der Nutzungsfestlegung**

Da im zentralen Fall der Zugriffskontrollmechanismus eine systemweite Kontrolle ausüben kann, ist eine Nutzungsfestlegung prinzipiell umfassend zu realisieren. Es kommt nur darauf an welche Differenzierung das Berechtigungskonzept bzw. die Zugriffskontrolle des jeweiligen Systems zulässt. Aufwendig könnte die Umsetzung eines Nutzungsausschlusses sein (z. B. leseberechtigt sind alle Mediziner der Abteilung A (Rolle) mit Ausnahme von Herrn Dr. X der Abteilung A).

Existiert in einem System mit verteilter Datenhaltung ein systemweites Berechtigungskonzept und ein systemweiter Zugriffskontrollmechanismus sind Nutzungsrechte, die systemübergreifende Bedeutung haben, wie bei einem Zentralsystem definierbar.

Bei dezentralen Systemen sind Nutzungsrechte mittels des Zugriffskontrollmechanismus jeweils für die lokalen Systeme definierbar. Wird ein Dokument von einem lokalen System an ein anderes übermittelt, müssen die u. U. bestehenden Nutzungsrechte bzw. Nutzungsausschlüsse mit dem Dokument übermittelt werden. Der Empfänger des Dokuments muss dann für deren Einhaltung sorgen.

Dezentrale Systeme mit zentraler Komponente können Zugriffskontrollmechanismen für die zentrale Komponente wie im zentralen Fall realisieren. Dokumente, die sich im Speicherbereich der Subsysteme befinden oder in deren Speicherbereich gelangen, entziehen sich dem zentralen Zugriffskontrollmechanismus und sind wie im dezentralen Fall zu behandeln.

## **VI. Beispiele für Ansätze/Projekte zur Kommunikation im Gesundheitswesen**

### **1. Patientenbegleitende Dokumentation (PaDok)**

PaDok wurde vom Fraunhofer-Institut für Biomedizinische Technik als technische Lösung zur Erfüllung eines großen Teils der alltäglichen Kommunikation von Leistungserbringern im Gesundheitswesen entwickelt. Technisch realisiert sind zur Zeit der elektronische Arztbrief, die elektronische Überweisung, die elektronische Einweisung, die elektronische Quartalsabrechnung, das elektronische Rezept und die elektronische Fall-Akte. Von seiner Architektur unterstützt PaDok eine dezentrale Datenhaltung mit zentraler Komponente. Die zentrale Komponente wird von einem PaDok-Server gebildet, der als Nachrichtenpuffer dient. Der Absender einer Nachricht versieht eine elektronische Information mit einer Empfänger-Kennung und schickt sie an den PaDok-Server, der an einer zentralen Stelle im regionalen Netzwerk steht. Der Empfänger der Nachricht kann sich dann die Nachricht vom PaDok-Server abholen. Insofern gleicht das Grundprinzip von PaDok dem der E-Mail. Alle PaDok-Nachrichten werden elektronisch signiert und mittels eines asymmetrischen Verfahrens verschlüsselt. Damit ist die Vertraulichkeit, Integrität und Authentizität von PaDok-Nachrichten sichergestellt.

Im Gegensatz zu einem Standard-Mailingsystem erlaubt PaDok die nicht-adressierte Kommunikation. Wird beispielsweise ein Patient von seinem Hausarzt zwecks einer internistischen Weiterbehandlung überwiesen, steht u.U. zum Zeitpunkt der Überweisung der Internist als Person noch nicht fest, da der Patient die freie Arztwahl hat. Das Problem besteht nun darin, dass zum Verschlüsseln der zu übermittelnden Dokumente mittels eines asymmetrischen Verfahrens der öffentliche Schlüssel des Empfängers erforderlich ist, also zum Zeitpunkt der Verschlüsselung der konkrete Empfänger feststehen muss. PaDok löst dieses Problem, indem es die Dokumente des Absenders (hier der Hausarzt), die an den Empfänger (hier der noch nicht feststehende Internist) übermittelt werden sollen, mit einer Vorgangskennung versieht. Diese Vorgangskennung besteht aus zwei Teilen. Der eine Teil dient der Identifikation der Dokumente und der andere Teil wird als Schlüssel (Vorgangsschlüssel) verwendet. Vereinfacht ausgedrückt werden nun die Dokumente durch ein zweistufiges Verschlüsselungsverfahren verschlüsselt. Dazu ist der Vorgangsschlüssel und der öffentliche Schlüssel des PaDok-Servers erforderlich. Die verschlüsselten Dokumente werden an den PaDok-Server versandt und der Patient erhält die Vorgangskennung, entweder in ausgedruckter Form oder auf einer Chipkarte. Findet sich der Patient schließlich bei einem weiterbehandelnden Internisten seines Vertrauens ein, so übergibt er ihm die Vorgangskennung. Der identifizierende Teil der Vorgangskennung dient nun der Selektion der Dokumente auf dem PaDok-Server. Der PaDok-Server entschlüsselt die selektierten Dokumente mit dem geheimen Server-Schlüssel und verschlüsselt sie anschließend mit dem öffentlichen Schlüssel des anfordernden Internisten. Die Verschlüsselung, die mit dem Vorgangsschlüssel erfolgte, bleibt bei diesem Umschlüsselungsvorgang erhalten, so dass die Dokumente auf dem Server zu keinem Zeitpunkt lesbar sind. Die umgeschlüsselten Dokumente werden dann an den Internisten geschickt. Dieser benötigt zur Entschlüsselung seinen geheimen Schlüssel und den in der Vorgangskennung enthaltenen Vorgangsschlüssel. Mit diesem Verfahren ermöglicht PaDok eine nicht-adressierte Kommunikation unter Wahrung einer adressierten Vertraulichkeit. Der Patient wird dadurch in die Lage versetzt, den Adressaten seiner Dokumente (hier der weiterbehandelnde Internist) selbst zu bestimmen, ohne dass er diesen dem

Absender der Dokumente (hier der überweisende Hausarzt) mitteilen muss. Außerdem ist sichergestellt, dass nur der vom Patienten bestimmte Absender die Dokumente lesen kann.

Der Mechanismus der nicht-adressierten Kommunikation ermöglicht es außerdem, patientenbezogene Fallakten anzulegen. Hierzu können die für einen Fall relevanten Dokumente von der an der Behandlung des Patienten beteiligten Ärzten in einer temporären Akte auf dem PaDok-Server hinterlegt werden. Der Patient selbst hat auf der Grundlage des oben beschriebenen Verfahrens zu jedem Zeitpunkt seiner Behandlung die Entscheidung darüber, welcher behandelnde Arzt Dokumente seiner Fallakte einsehen kann.

## **2. Die "Elektronische Patientenakte" (EPA)**

Der Begriff "Elektronische Patientenakte" wird in unterschiedlichen Ausprägungen verwendet. Zum einen wird unter einer Elektronischen Patientenakte eine Sammlung medizinischer Informationen zu einem Patienten innerhalb einer Institution auf digitalen Datenträgern verstanden. Dies kann die Krankenakte über einen Patienten in einem Krankenhaus sein, aber auch die ärztliche Dokumentation in einer Praxis. Daneben wird der Begriff zunehmend auch werbewirksam von kommerziellen Anbietern benutzt. Sie bieten an, medizinische Daten über eine Person über das Internet zur Verarbeitung oder/und zum Abruf durch einen Arzt, Krankenhaus etc. bereitzuhalten. Im Rahmen der Diskussion der Reform im Gesundheitswesen wird allerdings der Begriff in einer anderen Bedeutung verwendet. Unter einer "elektronischen Patientenakte" ist dabei die jederzeit verfügbare, institutionsübergreifende und unter Kontrolle des Patienten und (eines) Arztes befindliche Kopie aller relevanten Daten der Krankengeschichte zu sehen. Auf der Basis dieser Definition wurden von verschiedenen Gruppen beispielsweise "Junge Mediziner in der SPD", Konzepte entwickelt, die einerseits die Vorteile der informationstechnischen Verarbeitung medizinischer Daten nutzen und andererseits durch den Einsatz von datenschutzfreundlichen Techniken den Datenschutz und die Datensicherheit für diese Informationen sichern will.

Die Grundkonzeptionen aller EPA-Modelle geht dabei von einer Kombination einer Chipkarte mit Schlüsselfunktion und einem gesicherten Zugang zu pseudonymisierten Daten aus. In den vorgestellten Projekten sollen folgende technische Maßnahmen den Datenschutz sicherstellen:

Nur mit einer Chipkarte und der Einwilligung des Patienten ist ein Zugang zu seiner EPA technisch überhaupt möglich.

Die Einwilligung kann auf einzelne Ärzte oder Krankenhäuser beschränkt werden.

Ein Widerruf ist jederzeit möglich, auch die Löschung aller Daten ist auf Wunsch des Patienten vorgesehen.

Die Modelle variieren dahingehend, dass der Ort der Speicherung der Daten, beispielsweise auf der Chipkarte des Patienten oder auf zentralen und dezentralen, regionalen Servern und der Umfang der medizinischen Daten (Arztbrief, Rezept, Röntgenaufnahmen etc.) verschieden ist.

Der Zugang zu den medizinischen Daten steht allerdings immer unter der Prämisse , dass keine Daten ohne Karte des Patienten aus dem System gelangen können und damit von Unbefugten, also auch Ärzten, gelesen werden können, d.h., der Patient kontrolliert den Zugang zu seinen Daten. Eingeschränkt wird dieser Zugang des Patienten in manchen Modellen dadurch, dass für den Zugang auch ein Arzt benötigt wird. Die Speicherung der medizinischen Daten erfolgt in der Regel in pseudonymisierter Form.

Technisch wird der Zugang zu den medizinischen Daten mit Hilfe von Verschlüsselungsverfahren sichergestellt. Ein Modell geht dabei von folgendem Verfahren aus:

Die medizinischen Daten werden auf einem regionalen Server, beispielsweise in einem Krankenhaus verschlüsselt gespeichert. Zur Pseudonymisierung der Daten erzeugt die Software auf der Chipkarte des Versicherten einen Code, der den Zugang zu Daten ermöglicht, d.h. (selbst) der Rechner des Arztes kennt nicht das Pseudonym des Patienten. Mit Hilfe des Codes, also weder mit dem Namen des Patienten, noch seinem Pseudonym, werden Daten von einem (regionalen) Server angefordert oder geschrieben. Zur Absicherung des Abrufes und/oder der Verarbeitung von Daten muss zunächst die Authentifizierung des Arztes mit Hilfe eine Health Care Professional Card erfolgen, sowohl beim (regionalen) Server wie gegenüber der Patientenchipkarte. Die Einwilligung des Patienten zu der Verarbeitung bzw. zum Abruf der Daten wird über die Vorlage bzw. Benutzung der Patientenchipkarte realisiert. Damit sichergestellt wird, dass ein Widerruf der Verarbeitung der Daten möglich ist, wird zudem auf der Karte des Patienten ein Code generiert, der den Arzt zur Datenabfrage /Datenverarbeitung berechtigt ("upload code"). Mit Hilfe dieses UPLOAD-Code kann ein Arzt allerdings nur eine befristete Zeit beispielsweise 3 Monate auf die Daten des Patienten zugreifen, danach erlischt dieses Recht, der UPLOAD-Code wird ungültig. Die Übertragung der Daten zum bzw. vom Server wird zudem über Session-Keys verschlüsselt. Geht der Patient im Rahmen einer Behandlung zu einem anderen Arzt, kann dieser bei Vorlage der Patientenchipkarte und bei Freigabe der Daten durch den einstellenden Arzt befristet auf die Daten zugreifen.

Die der EPA zugrunde liegen Modelle sehen in allen Fällen einerseits die Verarbeitung von medizinischen Daten zu besseren und wirtschaftlicheren Versorgung des Patienten vor, andererseits soll durch die Pseudonymisierung der Daten anderen Bedarfsträgern (Gesundheitsministerium, Krankenkassen, Forschung und Wissenschaft) die Möglichkeit gegeben werden, statistische Auswertung auf den Daten durchführen zu können. Aus Gründen des Datenschutzes kann auch eine Pseudonymisierung der Arztdaten in diesen Datensätzen vorgesehen werden. Modellversuche mit einer (größeren) Anzahl von Patienten und Ärzten bzw. medizinischen Institutionen stehen noch aus.

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

Stand: 1. Januar 2003

Landesbeauftragter für den Datenschutz  
und für das Recht auf Akteneinsicht

Dr. Alexander Dix

Stellvertreter

Kurt Urban

Sekretariat

Christine Objartel  
App. 10

#### **Bereich Recht und Verwaltung**

Bereichsleiter

Dr. Frank Jendro  
App. 34

Arbeitsgebiete:

- Rechtliche Grundsatzfragen
- Wissenschaft, Forschung, Kultur
- Justiz und Europaangelegenheiten  
(außer Staatsanwaltschaften)
- Landesrechnungshof
- Landtag, Staatskanzlei
- Beauftragter des Haushalts

Arbeitsgebiete:

- Telekommunikation und Medien
- Kommunalrecht
- Rechtsfragen der elektronischen Verwaltung  
(eGovernment)

Sven Hermerschmidt  
App. 40

Arbeitsgebiete:

- Polizei, Verfassungsschutz
- Verkehrsordnungswidrigkeiten
- Ausländer, Asylverfahren
- Staatsanwaltschaften
- Presse- und Öffentlichkeitsarbeit

Lena Schraut  
App. 41

Arbeitsgebiete: Susann Burghardt  
– Landwirtschaft, Umweltschutz, Raumordnung App. 45  
– Stadtentwicklung, Wohnen, Verkehr  
– Personaldaten allgemein

Arbeitsgebiete: Dipl. Verwaltungs-  
wissenschaftler  
– Akteneinsicht und Informationszugang Sven Müller  
– Verwaltungsmodernisierung App. 20  
– Redaktion von Veröffentlichungen  
– Koordination des Internetangebots

Arbeitsgebiete: Gabriele Peschenz  
– Finanzen App. 22  
– Bildung, Jugend, Sport  
– Wirtschaft

Arbeitsgebiete: Anja Tönse  
– Arbeit, Soziales, Gesundheit, Frauen App. 44  
– Sozial- und Gesundheitsdaten allgemein

Arbeitsgebiete: Oliver F. Hoff  
– Inneres App. 36

Arbeitsgebiete: Dipl.-Betriebswirtin (FH)  
– Büroleitungsaufgaben Ursel Leunig  
– Haushaltsangelegenheiten App. 42  
– Beschaffungen

Arbeitsgebiete: Dipl. Betriebswirtin (FH)  
– Personal- und Verwaltungs- Gabriela Berndt  
angelegenheiten App. 12  
– Bibliothek  
– Schreibdienst

## **Bereich Technik**

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	Dipl.–Ingenieur für Informationstechnik Veikko Müller App. 32
Arbeitsgebiete: – Personalinformationssysteme – elektronische Akteneinsicht – Datenbanksysteme – Wartung und Fernwartung	Dipl.–Ingenieur Roy Pfitzner App. 31
Arbeitsgebiete: – Statistik – Umgang mit Datenträgern – Datenschutzaudit – Isolierte und vernetzte PC	Dipl.–Ingenieur (FH) Udo Thiele App. 33
Arbeitsgebiete – Einsatz von IT–Sicherheitsprodukten – Risikoanalysen und Sicherheitskonzepte – Organisations– und Dienstanweisungen – Gebäudesicherung – Computerviren	Dipl.–Ingenieur (FH) Jens Budszus App. 35
Arbeitsgebiete: – Schreibdienst – Informationsmaterialien	Monika Schäfer App. 43
Gleichstellungsbeauftragte	Frau Berndt App. 12
Personalrat	Frau Burghardt App. 45
Behördlicher Datenschutzbeauftragter	Herr Hermerschmidt App. 40

## Anlage 4

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

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

## Abkürzungsverzeichnis

ABl.	=	Amtsblatt
ABIEU	=	Amtsblatt der Europäischen Union
Abs.	=	Absatz
ADV	=	Automatische Datenverarbeitung
AIG	=	Akteneinsichts- und Informationszugangs- gesetz
Anl.	=	Anlage
APIS	=	Arbeitsdatei PIOS innere Sicherheit
AsylVfG	=	Asylverfahrensgesetz
AusIG	=	Ausländergesetz
BASIS	=	Buchhaltungs- und Abrechnungssystem im Strafvollzug
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BDSG	=	Bundesdatenschutzgesetz
Beschl.	=	Beschluss
BGBI.	=	Bundesgesetzblatt
BGH	=	Bundesgerichtshof
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtsgesetz
BR-Drs.	=	Bundesrats-Drucksache
BSHG	=	Bundessozialhilfegesetz
BSI	=	Bundesamt für die Sicherheit in der Informationstechnik
BT-Drs.	=	Bundestagsdrucksache
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BVerfG	=	Bundesverfassungsgericht
bzw.	=	beziehungsweise
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DES3	=	Data Encryption Standard (56 Bit Schlüssellänge)
d. h.	=	das heißt
DMS	=	Dokumentenmanagement-System
Drs.	=	Drucksache
EDV	=	Elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft
ELREV	=	Elektronischer Rechtsverkehr
E-OTD	=	Enhanced Observed Time Difference
EPA	=	elektronische Patientenakte

ff.	=	folgende
gem.	=	gemäß
GEMA	=	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
GO	=	Gemeindeordnung
GPS	=	Global Positioning System
GRUR	=	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GSiG	=	Grundsicherungsgesetz
HTML	=	HyperText Markup Language
HTTP	=	HyperText Transfer Protocol
ID	=	Identification (Benutzerkennung)
i. d. R.	=	In der Regel
IETF	=	Internet Engineering Task Force
IMSI	=	International Mobile Subscriber Identity
INPOL	=	Informationssystem der Polizei
IP	=	Internet Protocol
IPSEC	=	Internet Protocol Security
i. S. v.	=	im Sinne von
IT	=	Informationstechnik
KAN Land	=	Landeskriminalaktennachweis
KVBB	=	Kassenärztliche Vereinigung Brandenburg
LBS	=	Location Based Services
LBG	=	Landesbeamtengesetz
LDA	=	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDS	=	Landesbetrieb für Datenverarbeitung und Statistik
LKA	=	Landeskriminalamt
LKrO	=	Landkreisordnung
LVN	=	Landesverwaltungsnetz
MDIS	=	Meldedateninformationssystem
NADIS	=	Nachrichtendienstliches Informationssystem
NJW	=	Neue Juristische Wochenschrift
Nr.	=	Nummer
OBG	=	Ordnungsbehördengesetz
ORB	=	Ostdeutscher Rundfunk Brandenburg
PaDok	=	Patienten begleitende Dokumentation
PASS	=	Polizeilichen Auskunftssystem Straftaten
PC	=	Personalcomputer
PDSV	=	Postdienste-Datenschutzverordnung
PERIS	=	Personalinformationssystem

PersVG	=	Personalvertretungsgesetz
PGP	=	Pretty Good Privacy
PIOS	=	Verbunddatei Personen, Informationen, Objekte, Sachen
PostG	=	Postgesetz
RBB	=	Rundfunk Berlin–Brandenburg
RSA	=	Verschlüsselungsalgorithmus nach den Entwicklern Rivest, Shamir und Adleman
RTP	=	Realtime Transport Protocol
s.	=	siehe
S.	=	Seite; Satz
SFB	=	Sender Freies Berlin
SGB	=	Sozialgesetzbuch
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB V	=	Fünftes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
SMS	=	Short Message Service
s. o.	=	siehe oben
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
StVollzG	=	Strafvollzugsgesetz
TCP	=	Transmission Control Protocol
TDSV	=	Telekommunikations–Datenschutzverordnung
TK	=	Telekommunikation
TKG	=	Telekommunikationsgesetz
u. a.	=	unter anderem
UDP	=	User Datagram Protocol
UIG	=	Umweltinformationsgesetz
URL	=	Uniform Resource Locator
usw.	=	und so weiter
u. U.	=	unter Umständen
v.	=	von, vom
v. a.	=	vor allem
VersammlG	=	Versammlungsgesetz
VfGBbg	=	Verfassungsgericht des Landes Brandenburg
vgl.	=	vergleiche
z. B.	=	zum Beispiel
z. T.	=	zum Teil

## Stichwortverzeichnis

Aarhus–Konvention	98
Abhören von Gesprächen	19
Abrechnungsdaten	28
Abwasseranlage	108
Access Provider	27
Adresshändler	36
Adressmittlungsverfahren	82
Akteneinsicht	
elektronische	112
Akteneinsichts– und Informationszugangsgesetz	115
Aktenplan	112
Amtsausschuss	61
Anwendungshinweise	111
Arbeitskreis Medien	115
Archivgesetz	85
Arzt	91
Asylbewerber	48, 110
Aufsichtsbehörde für den Datenschutz im nicht–öffentlichen Bereich	11
Aufzeichnung	30
Ausländerbehörde	51
Behinderung	86
Bekanntmachung	
öffentliche	62
Beschaffungen	101
Bestandsdaten	26, 28
Bestimmung	
hinreichende	106
Besucherbuch	48
Besucherkarte	50
Betriebsgeheimnis	65, 101
Betriebssystem	19
Biometrie	16, 46
Brandenburg–Tag	118
Briefwahl	61
Bundesamt für die Sicherheit in der Informationstechnik	34
Bundesdatenschutzgesetz	11
Bundessozialhilfegesetz	86
Bußgeldverfahren	42
Chipkarte	55, 92
Content Provider	26
Datenschutzaudit	10
Datenschutzbeauftragter	

behördlicher	67, 68, 70
Datenschutzkontrolle	
unabhängige	36
Datenschutzrichtlinie für elektronische Kommunikation	22
Datensparsamkeit	10
Datenverarbeitung im Auftrag	37
Demonstration	38
Digital Rights Management	32
Direktwerbung	23
Dokumentenmanagement	112
Eingaben	102
Eingriffsbefugnis	
hoheitliche	48
Einwilligung	79, 82, 94
Elektronic Copyright Management Systems	32
E-Mail	26, 112
Erlass	110
Fernmeldegeheimnis	30, 52
Fingerabdruck	17
Forschungsprojekt	82
Fotokopie	107, 110
Freiwilligkeit	81
Führungszeugnis	42
Futtermittelherstellung	99
G 10-Kommission	45
Gebührendatenverarbeitungsanlage	30
Gebühreneinzugszentrale	36
Gebührenerfassung	30
Gebühren für den Zugang zu Dokumenten	97
Gemeinde	64
Gemeindeneugliederung	58
Gemeindeordnung	62
Gemeindevertretung	61
Geräteabgaben	32
Geschäftsgeheimnis	65, 101, 109
Geschäftsverkehr mit Gerichten und Staatsanwaltschaften	78
Global Positioning System	25
Grünbuch \	97
Grundbuch	74
elektronisches	77
Grunddatenbestand	13
Grundsicherungsgesetz	83
Gütesiegel	11
Handy	
Lokalisierung von	72

Hausrecht	49, 50, 66
Hundehalterverordnung	42
Identdaten	49
Identitätsfeststellung	48
Immissionsschutz	64
IMSI-Catcher	72
Informationsfreiheitsgesetz für die Bundesverwaltung	99
Informationszugang	64, 97
Interesse	
berechtigtes	74
rechtliches	74, 104
Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation	116
Internet	26, 94, 95, 112
Justizvollzugsanstalt	69
Kassenärztliche Vereinigung	90
Kettenbriefe	33
Kfz-Zulassungsstelle	87
Kindertagesstätte	109
Kommunalverfassung	63
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	115
Konferenz der Justizministerinnen und -minister	78
Kontoauszug	87
Korruption	101
Kostenerhebung	111
Kreistag	61
Landkreis	66
Landkreisordnung	63
Leistungskontrolle	30, 57
Lichtbild	17
Location Based Services	24
Lokalisierungsdienste	24
Luftverkehrsunternehmen	44
Mediendienst	26
Medizinischer Dienst der Krankenversicherung	90
Meldedienst	
kriminalpolizeilicher	41
Melderegister	
zentrales	52
Melderegisterabgleich per Videokamera	60
Mietspiegel	106
Mobilfunk	64
Mobilfunkkataster	65
Mobiltelefon	72
Modernisierung des Datenschutzrechts	10

Musterdienstvereinbarung	30
Nachrichtendienstliches Informationssystem	14
Niederschrift	62
Notiz	
handschriftliche	108
Nutzungsdaten	26, 28
Online–Abrufverfahren	95
Ordnungsmäßigkeit der Datenverarbeitung	34
Orientierungshilfe	20
Ort	
gefährdeter oder gefährlicher	48
Ostdeutscher Rundfunk Brandenburg	35, 36
Outsourcing	12
Passabgleich	46
Pässe	16
Patient	89
Patientenakte	
elektronische	92
Pauschalvergütung	32
PERIS	53
Personalausweis	16, 21
Personaldaten	53, 58
Personaldaten–Pool	53
Personalrat	59
Personalüberhang	80
Personalvertretung	57
Polizei	28
Polizeibeamte	
szenekundige	39
Polizeipräsidium	40
Postdienste	34
Privatisierung	59
Privatkopie	
digitale	32
Produktaktivierung	19
Pseudonym	82
Publikationen	117
Quellen	
allgemein zugängliche	37
Rasterfahndung	13
Rechtsverkehr	
elektronischer	78
Registrierung des Nutzerverhaltens	31
Richtervorbehalt	73
Risikoanalyse	15

Rundfunk Berlin–Brandenburg	35
Rundfunkgebühr	37
Schadensersatz	104, 105
Schüler	
volljährige	79
Schweigepflicht	87
ärztliche	92
Sender Freies Berlin	35
Sicherheitskonzept	14
Signatur	
elektronische	21, 93
qualifizierte elektronische	113
Sitzung	
nicht–öffentliche	61
SOLUM–STAR	77
Sozialamt	86, 87
Sozialdaten	86
Sozialgeheimnis	86
Sozialhilfe	83, 86, 87
SPAM	23
Sportstadion	107
Sprachübertragung	19
Stadtverordnetenversammlung	112
Standortdaten	23, 25
Stasi–Unterlagen–Gesetz	115
Steuerakte	96
Steuergeheimnis	78
Störer	48
Strafverfolgung	28, 73
Systemdatenschutz	68
Teledienst	26, 28
Telefonieren im Internet	18
Telefonkarte	72
Telefonüberwachung	73
Telekommunikationsdienst	26, 28
Telemedizin	92
Terrorismusbekämpfungsgesetz	16, 43, 115
Tierseuchen	99
TK–Anlagen	29
Tracking–Dienste	24
Transparenz	
passive	98
Umweltinformation	98, 109
Umweltinformationsgesetz	65
Umweltinformationsrichtlinie	98

Umweltschutz	65
Unternehmen	101, 106, 108
Unterrichtsgestaltung	114
Unterstützungspflicht	106
Urheberrecht	31
Verbindungsdaten	26, 28, 30, 51
Verbraucherinformationsgesetz	99
Verbunddatei	14
Verbunddatei PIOS Innere Sicherheit	40
Verein	109
Verfahrens- und Anlagenverzeichnis	71
Verfassungsschutz	28
Vergabeverfahren	101
Vergleichsmiete	106
Verhaltenskontrolle	30, 57
Verschlüsselung	21
Verschwiegenheitspflicht	63
Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz	68
Videoüberwachung	50, 66, 69
Videoüberwachung bei Fußballspielen	38
Virenwarnungen	33
Voice over IP	19
Völkerverständigung	44
Volkszählung	60
Vorentwurf	108
Vorgangsverwaltungsdatei automatisierte	43
Vorratsdatenspeicherung	23, 28
Wahlscheinbeantragung per Internet	61
Weltwirtschaftskonferenzen	40
Wertstoffcontainer	66
Windows XP	19
Wohnungsgesellschaft	106
Zensustest	60
Zeugenbefragung	91
Zusammenlegung der Datenschutzkontrolle	12
Zwangsaktivierung	20
Zweckverband	108