**Landtag Brandenburg** **Drucksache 3/2481**
3. Wahlperiode

# Tätigkeitsbericht

# des Landesbeauftragten für den Datenschutz

# und für das Recht auf Akteneinsicht

# zum 31. Dezember 2000

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 8. März 2000 vorgelegten Tätigkeitsbericht 1999 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2000 ab.

Die "Dokumente zu Datenschutz und Informationsfreiheit 2000", auf die in diesem Bericht verwiesen wird, hat der Landesbeauftragte gemeinsam mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht wieder als gesonderten Anlagenband veröffentlicht. Tätigkeitsbericht und Anlagenband sind aus unserem Internet-Angebot unter http://www.lda.brandenburg.de abrufbar.

Datum des Eingangs: 05.03.2001 / Ausgegeben: 08.03.2001

# Tätigkeitsbericht

# des Landesbeauftragten für den Datenschutz

# und für das Recht auf Akteneinsicht

# zum 31. Dezember 2000

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 8. März 2000 vorgelegten Tätigkeitsbericht 1999 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2000 ab.

Die "Dokumente zu Datenschutz und Informationsfreiheit 2000", auf die in diesem Bericht verwiesen wird, hat der Landesbeauftragte gemeinsam mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht wieder als gesonderten Anlagenband veröffentlicht. Tätigkeitsbericht und Anlagenband sind aus unserem Internet-Angebot unter http://www.lda.brandenburg.de abrufbar.

**Impressum**

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

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

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

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Brandenburgische Universitätsdruckerei und
Verlagsgesellschaft Potsdam mbH

**Inhaltsverzeichnis** Seite

**Behördenverzeichnis** Gliederungspkt.

## Einleitung

Die Entwicklung des Datenschutzes und des Akteneinsichtsrechts in Brandenburg an der Schwelle zum 21. Jahrhundert ist durch widersprüchliche Tendenzen gekennzeichnet. Der Beginn des Jahres 2000 stand ganz im Zeichen befürchteter weltweiter Computerausfälle wegen der Datumsumstellung, die aber kaum in nennenswertem Umfang tatsächlich auftraten, weil rechtzeitig Vorsorge getroffen worden war. Stattdessen verursachte wenig später ein Virus mit der hinterhältigen Bezeichnung "I love you" sehr viel größere Schäden, weil er strukturelle Schwächen in standardisierter Mail-Software und die Neugier zahlloser Anwender ausnutzte. Damit wurde auf unerwartete Weise die Verletzlichkeit von Rechnern, die an das Internet angeschlossen sind und mit denen zugleich sensible personenbezogene Daten verarbeitet werden, demonstriert.

Das Wissen um diese Verletzlichkeit und um die Möglichkeiten effektiven Selbstschutzes muss weiter gestärkt werden, wenn der Nutzen des Internets für die Menschen gegenüber den Risiken überwiegen soll[1]. Im Jahr 2000 nutzte in Brandenburg schon jeder achte Haushalt das weltweite Datennetz, etwa doppelt so viel wie im Jahr zuvor[2]. Doch die Möglichkeit für die Bürgerinnen und Bürger, Kontakte zur Verwaltung auf elektronischem Wege über Internetportale und Serviceläden aufzunehmen, lässt sich bisher nur in Ansätzen erkennen. Auch die weit reichenden Ziele des Aktionsplans "*e*Europe - eine Informationsgesellschaft" der Europäischen Kommission[3], bis Ende 2000 auch durch die Mitgliedstaaten einen elektronischen Zugang in beiden Richtungen für die Menschen zu eröffnen (Informationsabruf und Erledigung von Antragsverfahren), wurden nicht in nennenswertem Umfang erreicht. Grund dafür ist in erster Linie das Fehlen einer Sicherheitsinfrastruktur mit verlässlichen elektronischen Signaturen und kostengünstiger Technik für die Kunden der Verwaltung. Sobald diese sich entwickelt und attraktive Angebote gemacht werden, könnte die virtuelle Verwaltung (Electronic Government) den Schub der Verwaltungsmodernisierung auslösen, der dringend erforderlich ist, um die Leistungsfähigkeit von Staat und Verwaltung angesichts neuer Herausforderungen zu bewahren und zu stärken[4]. Der Zugang zu Informationen, sei es durch Akteneinsicht oder durch den elektronischen Zugriff auf Angebote des virtuellen Rathauses, wird zu einer zentralen

---

1 s. Pkt. A 2.2

2 laut einer Erhebung des Landesbetriebes für Datenverarbeitung und Statistik, Märkische Allgemeine Zeitung vom 3.1.2001

3 BR-Drs. 28/00 (vgl. insbes. Kap. 10: Regierung am Netz)

4 vgl. Electronic Government als Schlüssel zur Modernisierung von Staat und Verwaltung, Memorandum des Fachausschusses Verwaltungsinformatik der Gesellschaft für Informatik e. V. und des Fachbereiches 1 der Informationstechnischen Gesellschaft im VDE, September 2000

Voraussetzung für eine moderne serviceorientierte Verwaltung.
Der Datenschutz ist kein bürokratisches Hemmnis in diesem Zusammenhang, sondern hat die Aufgabe, die Entscheidungsfreiheit des Einzelnen gerade im Zeitalter immer rascher wachsender, aber auch unüberschaubarer werdender Datenverarbeitungssysteme zu erhalten. Angesichts der Komplexität moderner Datenverarbeitung sind die staatlichen und kommunalen Stellen verpflichtet, die Bürgerinnen und Bürger bei der Nutzung dieser technischen Möglichkeiten am häuslichen PC oder am öffentlichen Internet-Kiosk zu beraten und zu unterstützen. Es darf gerade im Verhältnis zwischen Bürgern und Verwaltung weder zu einer "digitalen Kluft" zwischen den Wissenden und den Nicht-Wissenden noch zu einer Art faktischem Anschluss- und Benutzungszwang kommen, der zur Folge hätte, dass die reale Verwaltung hinter dem virtuellen Rathaus verschwindet.

So begrüßenswert die "Medienoffensive" der Landesregierung ist, mit der alle Schulen alsbald einen Internet-Zugang erhalten sollen[5]: sie wird erst dann erfolgreich sein, wenn den Schülerinnen und Schülern die nötige Medienkompetenz und damit auch das Wissen darüber vermittelt wird, wie sie sich souverän und selbstbestimmt im Netz bewegen können, welche Möglichkeiten des effektiven Selbstschutzes es gibt und wie man sie nutzt.

Die Diskussion um die Videoüberwachung öffentlicher Straßen und Plätze in Brandenburg im vergangenen Jahr hat erneut gezeigt, dass die Ausweitung polizeilicher Befugnisse zur Registrierung unverdächtiger Personen trotz gravierender datenschutzrechtlicher Einwände vorangetrieben wird[6]. Dennoch hat der Gesetzgeber diese Einwände nicht völlig unberücksichtigt gelassen, sondern hat zum ersten Mal in Deutschland die Befugnis zur Videoüberwachung befristet und eine unabhängige Evaluation der praktischen Anwendung dieser Technik vorgesehen. Insgesamt zwingt die außerordentlich schnelle technische Entwicklung in diesem Bereich von IT-kabellosen zuckerwürfel-großen Webcams (Kameras, die aufgenommene Bilder direkt im Internet bereitstellen) bis hin zu "schlauem Staub" (mikroelektronische Sensoren), der Informationen und Bilder registrieren kann, dazu, dass effektive technische und rechtliche Regeln für die Begrenzung der Sammlung von Bildinformationen im öffentlichen wie im privaten Bereich entwickelt werden. Gelingt dies nicht, dann ist die individuelle Freiheit des Einzelnen in ihrem Wesensgehalt bedroht. Wir leben zunehmend in einer Welt, in der Informationen durch Bilder von Personen übermittelt werden. In dem Maße, wie der unverdächtige Einzelne die Möglichkeit verliert, über sein Abbild zu verfügen, ist seine Selbstbestimmung

[5] s. Pkt. A 6.2

[6] s. Pkt. A 4

in Gefahr.

Positiv war im Berichtszeitraum festzustellen, dass das allgemeine voraussetzungslose Informationszugangsrecht auch in Deutschland zunehmend Anhänger findet[7]. In erstaunlich kurzer Zeit beginnt sich auch außerhalb Brandenburgs die Erkenntnis durchzusetzen, dass die gesetzliche Verankerung eines allgemeinen Akteneinsichtsrechts nicht länger aufgeschoben werden sollte. Zwar ist diese Entwicklung ihrerseits uneinheitlich. Auch kann die Verabschiedung von Gesetzen allein ohnehin das traditionelle Geheimhaltungsdenken in vielen Verwaltungen nicht verändern. Aber eine Veränderung kommt in dem Maße in Gang, wie Menschen von ihren neuen Rechten Gebrauch machen und die Behörden erkennen, dass das Bereitstellen von nicht schützenswerten Informationen für eine bürgernahe Verwaltung selbstverständlich sein sollte.

Diese Erkenntnis wird unterstützt durch die im Dezember 2000 proklamierte Charta der Grundrechte der Europäischen Union, die sowohl das Recht auf Datenschutz als auch auf Zugang zu den Dokumenten der Europäischen Institutionen verankert hat. Insoweit hat die brandenburgische Landesverfassung eine europäische Entsprechung gefunden. Die Charta enthält auch ein bemerkenswertes "Recht auf eine gute Verwaltung" (Artikel 41), das das prinzipielle Recht jeder Person auf Zugang zu den sie betreffenden Akten umfasst. Damit ist erstmals auf dieser Ebene der Grundsatz festgeschrieben worden, dass Datenschutz und Transparenz Qualitätsmerkmale einer modernen serviceorientierten Verwaltung sind.

[7] s. Pkt. B 1.2

# Teil A

# Datenschutz

## 1 Brennpunkte des Datenschutzes

### 1.1 Entwicklung des Datenschutzrechts

#### 1.1.1 Stufenweise Modernisierung des Bundesdatenschutzgesetzes

Fast zwei Jahre nach Ablauf der Umsetzungsfrist für die EG-Datenschutzrichtlinie hat die Bundesregierung am 14. Juni 2000 unter dem massiven Druck des von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahrens den Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze beschlossen[8]. Damit soll das allgemeine und bereichsspezifische Bundesrecht an die Vorgaben der Europäischen Datenschutzrichtlinie angepasst werden. Ob die Bundesrepublik durch die Verabschiedung dieses Gesetzentwurfes einer Verurteilung durch den Europäischen Gerichtshof wegen unzureichender Umsetzung der Richtlinie entgehen kann, ist zweifelhaft, zumal die meisten Bundesländer (Brandenburg bildet hier eine lobenswerte Ausnahme) ihr Landesrecht noch nicht an das Gemeinschaftsrecht angepasst haben. Sicher ist allerdings, dass der Entwurf der Bundesregierung den Ansprüchen an ein modernes Datenschutzrecht in keiner Weise genügt.

Immerhin enthält er Elemente des Systemdatenschutzes wie das Gebot zur Datenvermeidung und Datensparsamkeit und den Vorrang anonymer und pseudonymer Formen der Datenverarbeitung sowie eine Regelung zum Datenschutz-Audit. In beiden Fällen folgt der Gesetzentwurf des Bundes dem Beispiel des Brandenburgischen Datenschutzgesetzes, in das der Landtag bereits Ende 1999 entsprechende Vorschriften aufgenommen hatte.

Der Entwurf des Bundesdatenschutzgesetzes enthält außerdem eine Regelung zur Videoüberwachung im Bereich der Privatwirtschaft, die allerdings auf Grund ihrer weiten Formulierung die bestehenden praktischen Probleme kaum lösen wird. Zwar würde damit erstmals eine Rechtsgrundlage für die Videoüberwachung im nicht-öffentlichen Bereich geschaffen, die aber als Neuerung nur die Pflicht zum Hinweis auf die Tatsache der Videoüberwachung sowie zur Löschung der gewonnenen Daten nach Zweckerreichung oder bei entgegenstehenden schutzwürdigen Interessen der Betroffenen enthält.

---

[8] BR-Drs. 461/00

Angesichts der allgegenwärtigen Aufzeichnungstechnik bietet eine solche Regelung aus datenschutzpolitischer Sicht keinen hinreichenden Schutz des Einzelnen vor einer Rundumbeobachtung durch privat betriebene Kameras. Ein Ausgleich kann auch nicht das Kunsturhebergesetz von 1907 sein, das noch immer eine gültige Strafvorschrift enthält, die die Verbreitung von Bildnissen (auch und gerade im Internet) ohne Einwilligung des Abgebildeten unter Strafe stellt. Der Schutz des Rechts am eigenen Bild kann aber auf Dauer nicht allein dem Zivil- oder dem Strafrecht überlassen bleiben, sondern muss in den Schutzbereich einer modernen Datenschutzgesetzgebung einbezogen werden. Dabei reicht es nicht aus, die Tatsache der kameragestützten Beobachtung für den Betroffenen transparent zu machen. Vielmehr müssen engere materielle Grenzen für die Videoüberwachung formuliert und technisch-organisatorisch unterstützt werden.

Die Bundesregierung lässt das bisherige Medienprivileg mit der vorgesehenen Aufnahme einer Rahmenvorschrift in das Bundesdatenschutzgesetz weitgehend unangetastet. Der Landesgesetzgeber soll nach diesen Plänen lediglich die Rahmenbedingungen für die Datenverarbeitung durch Presseunternehmen zu eigenen, journalistisch-redaktionellen Zwecken bestimmen. Obwohl die EG-Datenschutzrichtlinie (Artikel 9) Ausnahmen von ihren Bestimmungen nur insoweit zulässt, als diese notwendig sind, um das Recht auf Privatsphäre mit der Freiheit der Meinungsäußerung in Einklang zu bringen, will die Bundesregierung die Presse - wie schon bisher - von der Kontrolle durch unabhängige Aufsichtsbehörden freistellen. Presseunternehmen müssten auch in Zukunft anders als die Rundfunkanstalten keinen internen Datenschutzbeauftragten bestellen. Stattdessen hat der Deutsche Presserat sein bisheriges Verfahren der Selbstkontrolle weiterentwickelt[9] und will mit einem Verhaltenskodex und einem presseinternen Beschwerdeverfahren eine effektive Datenschutzkontrolle sicherstellen. Ob dies gelingt, bleibt abzuwarten. Ungewiss ist aber schon jetzt, ob die Bundesrepublik mit dieser Regelung im Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof bestehen kann; insofern sind Zweifel angebracht.

[9] s. Jahrbuch 2000 des Deutschen Presserates (Schwerpunkt Redaktions-Datenschutz)

Der Bundesrat hatte in seiner Stellungnahme zum Regierungsentwurf für ein Bundesdatenschutzgesetz unter anderem die Streichung der Vorschrift für das Datenschutz-Audit verlangt[10]. Demgegenüber will die Bundesregierung daran festhalten, die Möglichkeit einer freiwilligen Auditierung auch im allgemeinen Datenschutzrecht für den öffentlichen und den nicht-öffentlichen Bereich einzuführen. Dies ist zu begrüßen, weil ein richtig eingesetztes Datenschutz-Audit die gesetzlich vorgeschriebene Kontrolle durch Datenschutzbeauftragte und Aufsichtsbehörden unterstützen und die Marktkräfte zu Gunsten von datenschutzfreundlichen Verfahren und Produkten ähnlich wie im Umweltbereich zur Geltung bringen kann. Der Bund würde damit dem Beispiel Brandenburgs folgen, das eine solche Möglichkeit für den öffentlichen Bereich bereits seit zwei Jahren in seinem Datenschutzgesetz vorsieht.

Selbst wenn der Entwurf der Bundesregierung für ein Bundesdatenschutzgesetz im Frühjahr 2001 verabschiedet wird, so besteht doch Einigkeit darüber, dass dies nicht der große Wurf für eine neue Datenverkehrsordnung ist, die dem 21. Jahrhundert und den Bedingungen der Informationsgesellschaft angemessen wäre. Deshalb hat das Bundesinnenministerium gemeinsam mit den Koalitionsfraktionen im Deutschen Bundestag einen Gutachter-Ausschuss zur Modernisierung des Datenschutzrechts berufen, der bis zum Sommer 2001 ein Gutachten für die sog. zweite Stufe der Novellierung des Bundesdatenschutzgesetzes erarbeiten soll. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird die Arbeit der Gutachter in einer Begleitkommission unterstützen.

### 1.1.2 Datenexporte in "sichere" und "unsichere Häfen"

Von zunehmender Bedeutung in der Informationsgesellschaft ist der grenzüberschreitende Datenverkehr. Die Europäische Datenschutzrichtlinie soll die Übermittlung personenbezogener Daten innerhalb der Union erleichtern, indem sie ein harmonisiertes Datenschutzniveau in allen Mitgliedsstaaten schafft. Der Export personenbezogener Daten in Drittstaaten (außerhalb der Europäischen Union) ist nach der Richtlinie und nach dem Brandenburgischen Datenschutzgesetz grundsätzlich nur dann zulässig, wenn im Empfängerland ein angemessenes Datenschutzniveau herrscht.

[10] BR-Drs. 461/00 (Beschluss)

Nach mehrjährigen Verhandlungen zwischen der Europäischen Kommission und dem US-Handelsministerium hat die Kommission im Berichtszeitraum auf der Grundlage der Prinzipien des "Sicheren Hafens" (Safe Habor) die Angemessenheit des Datenschutzniveaus bei solchen Unternehmen in den USA anerkannt, die diese Prinzipien akzeptieren[11]. Diese Entscheidung hat auch Auswirkungen auf den Datenschutz in Brandenburg, denn es muss sichergestellt werden, dass personenbezogene Daten nur dann von brandenburgischen Behörden oder Unternehmen in die USA übermittelt werden, wenn gewährleistet ist, dass sie dort "im sicheren Hafen" ankommen, also keinem geringeren Schutz unterliegen als in ihrem Ursprungsland. Bisher haben nur wenige US-Unternehmen die Grundsätze des sicheren Hafens akzeptiert. Für den Fall, dass der erforderliche Schutz nicht gewährleistet ist, hat die Kommission allen Kontrollstellen in der Europäischen Union ausdrücklich die Befugnis zugesprochen, die Datenübermittlung an amerikanische Stellen auszusetzen.

Auch im Verhältnis zu europäischen Nachbarländern, die nicht Mitglied der Union sind, muss der grenzüberschreitende Datenverkehr an den Kriterien der Richtlinie gemessen werden. Dies gilt etwa für die Übermittlung von Sozialdaten durch Sozialversicherungsträger, aber auch für andere Informationsbeziehungen zwischen brandenburgischen und ausländischen Behörden. Polen hat insoweit eine Vorreiterrolle, als es bereits über eine Datenschutzgesetzgebung verfügt, die sich an den Standards der Europäischen Union ausrichtet.

### 1.1.3 Novellierung des Multimedia-Rechts

Parallel zur Novellierung des Bundesdatenschutzgesetzes hat das Bundeswirtschaftsministerium im Berichtszeitraum den Entwurf für ein Erstes Gesetz zur Änderung des Teledienstedatenschutzgesetzes erarbeitet und in einer Arbeitsgruppe, an der wir uns beteiligt haben, eingehend erörtert. Dabei konnte eine ganze Reihe von Verbesserungen für den Datenschutz bei Multimedia-Diensten erreicht werden. Die Länder bereiten eine parallele Anpassung des Mediendienste-Staatsvertrages vor, der schon bisher weitgehend inhaltsgleiche Datenschutzregeln für meinungsbildende Verteil- und Abrufdienste vorsah. Da wesentliche Elemente des moderneren Datenschutzrechts für Multimedia-Dienste in das Bundesdatenschutzgesetz bereits in der ersten Stufe übernommen werden sollen, können das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag insoweit verschlankt werden. Von zentraler Bedeutung ist die weitere Angleichung der

---

[11] Entscheidung der Kommission vom 27.07.2000

s. Dokumente zu Datenschutz und Informationsfreiheit 2000, A II

Vorschriften für Tele- und Mediendienste auch im Bereich der Sanktionen. Bisher enthielt nur der Mediendienste-Staatsvertrag Bußgeldtatbestände für die Verletzung von materiell-rechtlichen Vorschriften wie etwa der Pflicht zum Angebot für anonyme und pseudonyme Nutzungsmöglichkeiten. Dies sollte nun für Teledienste entsprechend geregelt werden. Auch im allgemeinen Datenschutzrecht wäre die Einführung von spürbaren Sanktionen für den Verstoß gegen materielle datenschutzrechtliche Vorschriften sinnvoll, denn nur auf diese Weise kann der von der Europäischen Richtlinie vorgeschriebene Schutz betroffener Personen vor Rechtsverstößen sichergestellt werden.

Langfristig ist eine Entwicklung vorstellbar, bei der das allgemeine Datenschutzrecht und das besondere Datenschutzrecht für Tele- und Mediendienste weitgehend verschmolzen werden. Diese Überlegung drängt sich auch deshalb auf, weil immer mehr Rechtsgeschäfte des täglichen Lebens und Kontakte zwischen Bürgerinnen und Bürgern mit der Verwaltung unter Nutzung solcher Dienste abgewickelt werden. Dies wird eines der zentralen Themen der Modernisierung des Datenschutzes in der zweiten Stufe sein. Es sollte aber nicht übersehen werden, dass es spezifische Risiken für das informationelle Selbstbestimmungsrecht gibt, die sich gerade aus der Nutzung von Tele- und Mediendiensten ergeben können und die einer speziellen gesetzgeberischen Antwort bedürfen.

Das geänderte Teledienstedatenschutzgesetz soll im Rahmen eines Artikelgesetzes zur Anpassung des deutschen Rechts an die Vorgaben der europäischen E-Commerce-Richtlinie ebenfalls im Frühjahr 2001 vom Parlament beschlossen werden und gleichzeitig mit dem novellierten Datenschutzgesetz in Kraft treten.

### 1.1.4 Elektronische Signatur im Verwaltungsverfahren

Bei der Entwicklung des Datenschutzrechts wird auch der bevorstehende verstärkte Einsatz von digitalen Signaturen zu berücksichtigen sein. Das deutsche Signaturgesetz hat bisher noch nicht dazu geführt, dass diese Möglichkeit der Unterschrift per Chipkarte in der Praxis in nennenswertem Umfang genutzt wird. Ursache dafür war auch die fehlende Gleichsetzung der elektronischen Unterschrift mit der eigenhändigen Unterschrift. Nun verpflichtet die Ende 1999 verabschiedete EU-Richtlinie über die Rahmenbedingungen für elektronische Signaturen[12] die Bundesrepublik dazu, diese Gleichsetzung für den Rechtsverkehr vorzunehmen.

[12] Richtlinie 1999/93/EG über Gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. Nr. L 1/3/12 v. 19.01.2000

Die Bundesregierung hat mit ihrem Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften[13] die Voraussetzungen dafür geschaffen, dass im liberalisierten europäischen Rahmen die hohen Sicherheitsanforderungen des geltenden deutschen Signaturgesetzes aufrechterhalten werden können. Das ist von besonderer Bedeutung für den Zugang der Bürgerinnen und Bürger zu Verwaltungsdienstleistungen mittels der Informations- und Kommunikationstechnik im "virtuellen Rathaus". Allerdings sind die Vorarbeiten für die erforderliche Gleichstellung der elektronischen mit der eigenhändigen Unterschrift bei gleichzeitiger Wahrung der Warn- und Sicherungsfunktion der persönlichen Unterschrift für den Bereich des Privatrechts weiter vorangeschritten als für den Bereich des Verwaltungsverfahrensrechts, da für den zuletzt genannten Bereich die Gesetzgeber in Bund und Ländern eigene Zuständigkeiten haben. Um die Verwaltung in die Lage zu versetzen, möglichst bald elektronische Bürgerdienste auch in rechtlich verbindlicher Form anbieten zu können, sollte der bisher vorliegende Musterentwurf von Bund und Ländern für ein Gesetz zur Änderung des Verwaltungsverfahrensrechts zügig in die parlamentarische Beratung eingebracht werden. Dabei sollte in bestimmten Zusammenhängen auch die Möglichkeit der Verwendung von Pseudonymen erhalten bleiben, die das Signaturgesetz vorsieht. Schließlich muss die Festlegung von Standards für den Einsatz qualifizierter elektronischer Signaturen vorangetrieben werden, um die Voraussetzung für den praktischen Einsatz zu schaffen. Dabei ist zu berücksichtigen, dass unveränderliche personenbezogene Signaturen, zu deren Einsatz die Betroffenen möglicherweise in Zukunft rechtlich oder faktisch gezwungen werden könnten, einem verfassungswidrigen Personenkennzeichen gleich kämen.

Im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[14] wurden Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung erarbeitet ("Vom Bürgerbüro zum Internet"). Diese enthalten detaillierte Beispiele für eine datenschutzgerechte bürgerorientierte Verwaltung und können bei uns kostenlos angefordert werden. Die Verwendung von Signierverfahren ist zum Beispiel auch bei scheinbar belanglosen Kontakten mit Verwaltungen und öffentlichen Dienstleistern wie der elektronischen Bestellung der Sperrmüllabfuhr anzuraten, damit die Identität des Bestellers zweifelsfrei festgestellt werden kann und so massenhaften Bestellungen unter falschem Namen, die im Internet mit wenigen Mausklicks ausgelöst werden können, wirksam begegnet werden kann. In den USA ist dieses Problem des "Identitätsdiebstahls (identity theft)"

---

[13] BR-Drs. 496/00

[14] Entschließung der 60. Konferenz vom 12./13.10.2000, Dokumente zu Datenschutz und Informationsfreiheit 2000, A I

bereits weit verbreitet. Das Beispiel macht deutlich, dass die elektronische Signatur auch ein wichtiges Werkzeug zur Sicherung des Persönlichkeitsrechts und des Grundrechts auf Datenschutz in der Informationsgesellschaft sein kann.

## 1.2 Datenschutz im Data Warehouse - ein "weißer Rabe"?

*Der Einsatz von automatisierten Datenverarbeitungssystemen hat sich in den letzten Jahren in allen Bereichen des Lebens durchgesetzt. Mit der ständig zunehmenden Leistungsfähigkeit der eingesetzten Informations- und Telekommunikationstechnik wächst die Menge der automatisiert gespeicherten personenbezogenen Daten unaufhaltsam. Der Zugriff auf die Daten kann aufgrund der leistungsfähigen Hardware immer schneller erfolgen. Auf einer Festplatte können heutzutage Datenmengen von 80 GByte und mehr gespeichert werden, was in etwa 10 Millionen Schreibmaschinenseiten entspricht.*

Daten aus allen Lebensbereichen werden beispielsweise durch Nutzung von Chipkartensystemen und neuen Kommunikationsmedien preisgegeben und sowohl in Privatunternehmen als auch im Bereich der öffentlichen Verwaltung gespeichert und genutzt. Dabei spielen Datensparsamkeit und Datenvermeidung noch immer und z. T. ganz bewusst eine untergeordnete Rolle.

In Unternehmen und Behörden wächst das Interesse, das gesammelte Datenmaterial effektiver als bisher zu nutzen. Dabei wird davon ausgegangen, dass zu einem Betroffenen (Kunden) nicht durch Bewertung einzelner Daten ein aussagefähiges Gesamtbild entsteht, sondern erst durch die Analyse der Gesamtheit aller verfügbaren Daten einer Person und ihrer Beziehungen zueinander.

Das Data Warehouse ("Daten-Lagerhaus") ermöglicht diese neue Betrachtungsweise der Daten, weil in ihm alle im Unternehmen bzw. in der Behörde verfügbaren Daten nach bestimmten Kriterien sortiert gespeichert und zur Analyse und Auswertung bereitgehalten werden. Bisher unbekannte Zusammenhänge zwischen Einzeldaten sollen sich mit Hilfe des so genannten Data Mining ("Daten-Bergbau") aus der Gesamtheit des Datenbestandes herauslösen lassen, um aus diesen - die Aussagekraft der einzelnen Angaben meist deutlich übersteigenden - Informationen vor allem wirtschaftliche Vorteile für die speichernde Stelle erzielen zu können. Angesichts des steigenden Wertes personenbezogener Daten verweist der Begriff "Data Mining" treffend auf den industriellen Abbau von Mineralien und Edelsteinen. Dabei ist beabsichtigt, dem Manager und künftig wohl bald auch dem Behördenleiter aus der Fülle des Datenmaterials nur die strategisch wichtigen Informationen - möglichst in ansprechender und visuell einprägsamer Form - darzustellen.

Aus Sicht des Datenschutzes entsteht beim Data Warehouse und Data Mining die Frage nach der Rechtmäßigkeit der Verarbeitung personenbezogener Daten. So dürfen öffentliche Einrichtungen gem. § 4 BbgDSG personenbezogene Daten nur verarbeiten, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene ohne jeden Zweifel eingewilligt hat. Weiterhin ist die Datenverarbeitung so zu organisieren, dass die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Auch unterliegen alle personenbezogenen Daten einer strengen Zweckbindung, das heißt, die Daten dürfen nur für den Zweck verarbeitet werden, für den sie auch erhoben wurden. Eine weitere Forderung besteht darin, dass Suchkriterien in Datenbankanwendungen so genau definiert werden, dass freie Abfragen grundsätzlich nicht möglich sein dürfen. Data Mining steht im krassen Widerspruch zu dieser Forderung, da es gerade das Ziel des Data Mining ist, die Datenbestände nach unbestimmten Zusammenhängen zu durchsuchen.
Vor diesem Hintergrund hat die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2000 in Hannover eine Entschließung verabschiedet, die datenschutzrechtliche Bedenken gegen den Einsatz von Data Warehouse und Data Mining aufzeigt und die Verwendung datenschutzfreundlicher Technologien anmahnt[15].

Da auch öffentliche Stellen ein Interesse haben könnten, die Technologie von Data Warehouse und Data Mining für ihre Zwecke zu nutzen, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern ein Arbeitspapier erstellt, in dem die rechtlichen Möglichkeiten des Einsatzes von Data Warehouse und Data Mining im öffentlichen Bereich erörtert werden[16].

Der Bundesgesetzgeber wird im Zuge der grundlegenden Modernisierung des Bundesdatenschutzgesetzes zu prüfen haben, mit welchen rechtlichen Mitteln der Einsatz von Data Warehouse- und Data Mining-Technologien im Bereich der Wirtschaft zu kontrollieren ist.

---

[15] Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Dokumente zum Datenschutz A I.

[16] Anlage 2

Besonders der Grundsatz der Zweckbindung der Datenverarbeitung in der öffentlichen Verwaltung (dass die Bürgerinnen und Bürger wissen müssen, zu welchen Zwecken ihre persönlichen Daten verarbeitet werden) sowie der Grundsatz der Erforderlichkeit (die Pflicht, nicht mehr Daten zu verwenden, als zur Aufgabenerfüllung unbedingt benötigt werden) lassen die Nutzung dieser Technologien im öffentlichen Bereich nur in engen Grenzen zu.

## 1.3 Datenschutz als Schranke der behördlichen Öffentlichkeitsarbeit

*In mehreren Fällen mussten wir uns im Berichtszeitraum mit der Frage beschäftigen, wie die Öffentlichkeitsarbeit von Behörden datenschutzrechtlich zu bewerten ist.*

*In einem Fall erhielten die Journalisten bei einer Pressekonferenz des Innenministers eine "Dokumentation aller presseöffentlich gemachten Einzelfälle", die detaillierte Informationen über eine ausländische Familie und zwei Einzelpersonen ausländischer Herkunft auflistete. Zwar waren die Namen der Betroffenen und einige andere Angaben geschwärzt, die Nationalität blieb jedoch erkennbar, sodass die Unterlagen auf Grund der vorangegangenen öffentlichen Diskussion den betroffenen Ausländern zugeordnet werden konnten. Die Dokumentation enthielt in der Öffentlichkeit noch unbekannte Angaben zum persönlichen Lebensbereich der Betroffenen. Mit deren Veröffentlichung sollte dem Vorwurf begegnet werden, die Ausländerbehörden und das Innenministerium würden die gesetzlichen Ermessensspielräume nicht zu Gunsten der Betroffenen ausschöpfen und damit dem Rassismus Vorschub leisten.*

*In einem weiteren Fall berichtete die Presse im Herbst 2000 über mehrere Fälle von Abrechnungsbetrug im Gesundheitswesen. Nach Angaben einer Krankenkasse hatten niedergelassene Ärzte angeblich erbrachte Leistungen an verstorbenen Patienten abgerechnet. In zwei Fällen wurde der Ort genannt, an dem die Arztpraxis betrieben wurde, wobei es in diesen Orten jeweils nur eine Praxis dieser Fachrichtung gab. Über zwei andere Ärzte wurde so ausführlich berichtet, dass es mit Hilfe der Gelben Seiten ohne Weiteres möglich war, die Identität der Mediziner festzustellen. Zudem wurden auch personenbezogene Daten einer verstorbenen Patientin in diesem Zusammenhang veröffentlicht.*

*Schließlich war der Minister für Justiz und Europaangelegenheiten öffentlichen Vorwürfen ausgesetzt, er habe in einer Haftsache auf Betreiben eines Rechtanwaltes in die richterliche Unabhängigkeit eingegriffen. In einer Presseerklärung mit detaillierter Chronologie des*

*Geschehens trat der Minister diesen Vorwürfen entgegen, ohne dabei personenbezogene Angaben zu dem inhaftierten Betroffenen zu machen. Dennoch wurden in der Folge der Name des Betroffenen und die näheren Umstände seiner Verhaftung in der Presse wiedergegeben.*

Der freien und unbeeinträchtigten Berichterstattung durch die Medien kommt eine überragende Bedeutung zu. Die Behörden sind nach dem Landespressegesetz deshalb auch verpflichtet, Journalisten die Auskünfte zu erteilen, die Letztere für ihre Berichterstattung benötigen (§ 5 Abs. 1 Landespressegesetz). Allerdings können Auskünfte verweigert werden, wenn und insoweit ein überwiegendes schutzwürdiges privates Interesse durch die Auskunftserteilung verletzt würde (§ 5 Abs. 2 Nr. 3 Landespressegesetz). Zu den schutzwürdigen privaten Interessen gehört insbesondere auch das Grundrecht der Betroffenen auf Datenschutz nach Artikel 11 der Landesverfassung. Die Behörden haben entgegen dem Wortlaut des Pressegesetzes keinen Ermessensspielraum, ob sie Auskünfte, die in das informationelle Selbstbestimmungsrecht Betroffener eingreifen, verweigern, sondern sie sind dazu verpflichtet.

Auf diesen Zusammenhang hat das Brandenburgische Oberlandesgericht im Berichtszeitraum in einem Urteil hingewiesen, in dem es um die zivilrechtliche Bewertung der Erteilung von Auskünften über ein laufendes Disziplinarverfahren an die Presse ging[17]. Das Urteil beschreibt minutiös die rechtlichen Anforderungen, die der Persönlichkeitsschutz an die Öffentlichkeitsarbeit von Behörden stellt. Zwar ging es in dem vom Oberlandesgericht entschiedenen Fall um sensible Personaldaten. Dennoch lassen sich die dort aufgeführten Grundsätze generell auf den Umgang der Behörden mit personenbezogenen Daten anwenden.

Die Verwaltung ist verpflichtet, zwischen dem Informationsinteresse der Öffentlichkeit und dem Grundrechtsschutz der Betroffenen sorgfältig abzuwägen. Das gilt auch, wenn die Verwaltung und ihre Bediensteten in der Öffentlichkeit angegriffen werden. Sowohl das Sozialrecht als auch das Steuerrecht enthalten eng begrenzte Befugnisse zur Offenbarung personenbezogener Daten für den Fall, dass die Verwaltung unwahre Tatsachenbehauptungen richtig stellen muss. Zumindest zur Wahrnehmung der Fürsorgepflicht gegenüber Bediensteten wird eine solche Offenbarungsbefugnis auch in anderen Verwaltungsbereichen anzunehmen sein.

Die Öffentlichkeitsarbeit des Innenministeriums in dem beschriebenen Fall

[17] Urteil vom 22.02.2000 - 2 U 189/98 -

genügte diesen Anforderungen nicht. Es wurde nicht nur der Versuch unternommen, unwahre Tatsachenbehauptungen richtig zu stellen, sondern der wertende, allgemeine politische Vorwurf des Rassismus sollte mit der Offenbarung bisher nicht veröffentlichter personenbezogener Angaben, die zum Teil sogar höchstpersönlicher Natur waren, entkräftet werden. Das Ministerium rechtfertigte dieses Vorgehen mit der Befugnis des § 16 i. V. m. § 13 Abs. 2 Satz 1 Buchst. d) BbgDSG, die die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen (mithin auch die Veröffentlichung) erlaubt, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich ist. Doch selbst wenn das Vertrauen der Bevölkerung in den Rechtsstaat durch den Vorwurf des Rassismus gegen die Ausländerbehörden und den Minister erschüttert worden wäre, läge darin kein Nachteil für das gesellschaftliche Gemeinwohl, sondern allenfalls ein Nachteil für die beteiligten Behörden und Amtsträger, der es nicht rechtfertigt, personenbezogene Daten von Betroffenen aus Verwaltungsverfahren ohne ihre Einwilligung in weitreichender Weise offen zu legen.

Das Ministerium hätte - wie jede andere Behörde - falschen Tatsachenbehauptungen in der Öffentlichkeit aber nicht wehrlos gegenübergestanden. Das Landespressegesetz sieht ein Gegendarstellungsrecht vor, das zumindest dann geltend gemacht werden kann, wenn falschen Tatsachenbehauptungen entgegengetreten werden soll.

Auch dabei müssen die Behörden allerdings zwischen dem schutzwürdigen privaten Interesse der betroffenen Person und dem Interesse der Behörde an richtiger Darstellung sorgfältig abwägen. Hier ging es aber nicht um eine Tatsachenbehauptung, sondern um Werturteile in der politischen Auseinandersetzung. Personenbezogene Daten dürfen nicht für die politische Auseinandersetzung instrumentalisiert werden. Deshalb war das Vorgehen des Innenministeriums zu beanstanden.

Das Innenministerium beharrte demgegenüber auf seinem Standpunkt, die Offenbarung personenbezogener Daten sei zulässig gewesen, weil die Betroffenen selbst einen großen Teil der in der Dokumentation enthaltenen Informationen zuvor öffentlich gemacht hätten.

Im Fall der Krankenkasse ergab eine Anfrage, dass diese sich verpflichtet gesehen hatte, ihre Behauptungen in der Öffentlichkeit durch detaillierte Angaben zu untermauern. Insbesondere meinte die Krankenkasse, schutzwürdige Interessen des verstorbenen Opfers einer vermutlichen Falschabrechnung seien nicht beeinträchtigt, wenn dessen Name veröffentlicht würde. Ihre Mitarbeiter hätten Anfragen von Journalisten entsprechend den Datenschutzbestimmungen beantwortet. Der tatsächliche

Ablauf war allerdings nicht mit letzter Sicherheit zu rekonstruieren, weil Auskünfte an die Presse nur mündlich erteilt worden waren.

Jedoch unterliegen nicht nur die personenbezogenen Daten der Versicherten über ihren Tod hinaus, sondern auch die Tatsache einer ärztlichen Behandlung an sich dem Arzt- oder Sozialgeheimnis, sodass eine Offenbarung von Sozialdaten, wenn überhaupt, nur unter sehr engen Voraussetzungen zulässig ist. Die legitime Warnung vor falsch abrechnenden Ärzten und das Herausstellen eigener Ermittlungsleistungen rechtfertigen eine Offenbarung solcher Daten nicht. Presseerklärungen können in anonymisierter Form abgegeben werden. Eine Personenbeziehbarkeit muss dabei sicher ausgeschlossen sein.

Auch bei den nicht namentlich, aber mit Ortsangabe genannten Ärzten, denen Abrechnungsbetrug vorgeworfen wird, war ein Personenbezug mit Hilfe der gedruckten Branchenverzeichnisse und durch Internet-Recherchen herstellbar. Die Einwohner dieser Orte oder der Nachbarorte wissen, dass es dort nur eine einzige Praxis der genannten Fachrichtung gibt und wer sie betreibt. In Presseerklärungen muss aber auch bei der Darstellung von Straftaten die Unschuldsvermutung berücksichtigt werden, die bis zur rechtskräftigen Verurteilung gilt.
Mit einer hinreichend anonymisierten Darstellung dieses Falles von Abrechnungsbetrug hätte die Krankenkasse in der Öffentlichkeit deutlich gemacht, dass ihr die Wirtschaftlichkeit ebenso wichtig ist wie der Schutz des Sozialgeheimnisses. Zur Aufklärung von Abrechnungsbetrug können die Krankenkassen Sozialdaten an die Strafverfolgungsbehörden übermitteln, diese aber nicht der Öffentlichkeit bekannt geben.

Demgegenüber hat sich das Ministerium für Justiz- und Europaangelegenheiten bei der Auseinandersetzung mit den gegen den Minister erhobenen Vorwürfen datenschutzrechtlich korrekt verhalten. Die personenbezogene Berichterstattung über den Betroffenen beruhte nicht auf einer Veröffentlichung des Ministeriums.

Diese Fälle machen deutlich, dass noch erhebliche Unsicherheit in der Verwaltung herrscht, welche Grenzen das Grundrecht auf Datenschutz der behördlichen Öffentlichkeitsarbeit zieht. Wir haben dem Innenministerium vorgeschlagen, die zukünftige Öffentlichkeitsarbeit in ausländerrechtlichen Fragen durch den Erlass einer Leitlinie datenschutzgerecht zu gestalten und unsere Beratung bei der Erarbeitung einer solchen Leitlinie angeboten. Das Innenministerium hat zwar seinen Standpunkt zu dem beanstandeten Einzelfall bekräftigt, aber Gesprächsbereitschaft für die zukünftige Praxis signalisiert.

Die Behörden müssen bei ihrer Presse- bzw. Öffentlichkeitsarbeit in der Regel auf die Offenbarung von Daten mit Personenbezug verzichten. Die Öffentlichkeit hat keinen "Anspruch auf die ganze Wahrheit", der gegenüber dem Grundrecht der Betroffenen auf Datenschutz Vorrang hätte. Bei der Prüfung der Frage, ob ein Personenbezug gegeben ist, müssen auch allgemein zugängliche Hilfsmittel wie Adressbücher oder gedruckte und elektronische Branchenverzeichnisse berücksichtigt werden.

Lediglich ausnahmsweise können Verwaltungsbehörden bestimmte personenbezogene Angaben soweit offenbaren, wie es zur Richtigstellung falscher Tatsachenbehauptungen unumgänglich ist.

## 1.4 Wahlen und Abstimmungen im Internet ?

*Zunehmend wird in letzter Zeit die Frage diskutiert, inwieweit Wahlen und Abstimmungen auch unter Einsatz der neuen Medien durchgeführt werden können (electronic voting).*

Es gibt verschiedene Modelle von elektronischen Wahlen bzw. Abstimmungen und verschiedene Anwendungsebenen:

1. Bereits jetzt können auf der Grundlage des Bundeswahlgesetzes bei Bundestags- und Europawahlen Wahlgeräte (Wahlcomputer) zur Stimmenauszählung eingesetzt werden. Sie müssen durch den Bundesminister des Innern nach der Bundeswahlgeräteordnung zugelassen werden. Solche Geräte hat die Stadt Köln zuletzt bei der Europawahl 1999 in ihren Wahllokalen eingesetzt und deren „Zählergebnisse“ offline an das Wahlamt übertragen. Das Brandenburgische Ministerium des Innern bereitet eine entsprechende Rechtsverordnung zum Einsatz solcher Wahlgeräte bei den Bürgermeisterwahlen 2001/2002 vor.

2. Wahlen und Abstimmungen könnten auch in der Weise durchgeführt werden, dass einheitlich konfigurierte Rechner (z. B. die unter 1. genannten Wahlcomputer) unter Einsatz einer amtlich zertifizierten Wahlsoftware miteinander vernetzt und von den Wahlberechtigten genutzt werden. Damit würde eine internetgestützte elektronische Briefwahl ermöglicht. So hat u. A. im Juni 2000 eine simulierte Personalratswahl im Brandenburgischen Landesamt für Datenverarbeitung und Statistik stattgefunden. Die Forschungsgruppe „Internet-Wahlen“ der Universität Osnabrück setzt sich dafür ein, diese Möglichkeit der elektronischen Wahl bei den nächsten Wahlen zum Europäischen Parlament im Jahr 2004 anzubieten.

3. Alle Wahlberechtigten könnten sich in einer dritten Stufe unter Einsatz ihrer privaten Computer von zu Hause aus über das Internet oder andere offene Netze an Wahlen und Abstimmungen beteiligen.

Virtuelle Wahlen und Abstimmungen werfen weit reichende Fragen auf, bis hin zu der Problematik, ob demokratische Entscheidungen schnell getroffen werden können („Mausklick-Demokratie“) oder ob Demokratie nicht viel mehr Zeit braucht. Grundsätzlich ist festzustellen, dass Wahlen und Abstimmungen in demokratischen Gemeinwesen nach den Verfassungen des Bundes und der Länder eine zentrale Bedeutung haben. Die Legitimität des Wahlergebnisses ist entscheidend von der Vertrauenswürdigkeit des gesamten Verfahrens abhängig. Das gilt gerade auch angesichts der Erfahrungen mit Wahlfälschungen in der ehemaligen DDR.

Nach deutschem Wahlrecht findet die Stimmabgabe grundsätzlich im realen Wahllokal als Präsenzwahl statt. Dabei sind die Grundsätze der Allgemeinheit, Unmittelbarkeit, Freiheit, Gleichheit und des Wahlgeheimnisses zu beachten (Art. 38 Abs. 1 Satz 1 Grundgesetz). Die verfassungsrechtlich zeitweise umstrittene Briefwahl hat das Bundesverfassungsgericht nur als Ausnahme von der unmittelbaren Präsenzwahl zugelassen, um die Allgemeinheit der Wahl
- höhere Wahlbeteiligung und Wahlmöglichkeit für Personen, die aus gesundheitlichen Gründen nicht persönlich zur Stimmabgabe kommen können - zu gewährleisten[18]. Für eine elektronische Briefwahl fehlt dagegen bisher die Rechtsgrundlage.

Das zentrale Problem der internetgestützten Wahlen und Abstimmungen besteht darin, dass auch beim Einsatz moderner Kommunikationstechnik das Wahlgeheimnis gesichert und zugleich ein Höchstmaß an Transparenz und Überprüfbarkeit des gesamten Wahlverfahrens gewährleistet werden müssen.

Aufgrund dieser Anforderungen können rechtsverbindliche Wahlen und Abstimmungen in offenen Netzen und unter Verwendung von heterogener Hard- und Software (die oben genannte 3. Fallgruppe) nicht verfassungskonform durchgeführt werden. Zur Sicherheit der einzelnen Stimmabgabe und des Gesamtergebnisses einer Wahl darf es nicht dem einzelnen Wahlberechtigten überlassen bleiben, welche technischen Verfahren er zur vertraulichen Übermittlung seiner Stimme wählt.

---

[18] s. BVerfGE 59, 119 ff., 124, 127

Im Gegensatz zu elektronischen Wahlen wird bei konventioneller wie auch bei Briefwahl nach Überprüfung der Wahlberechtigung des Einzelnen die Verbindung zwischen der Person und der abgegebenen Stimme dadurch gelöst, dass der anonyme Stimmzettel entweder in eine Wahlurne eingeworfen oder der nicht markierte Wahlumschlag vom unterschriebenen Wahlschein getrennt und mit den übrigen Stimmzetteln vor der Auszählung zusammengeführt wird. Bei elektronischen Wahlen entsteht dagegen zwangsläufig eine elektronische Datenspur, die ohne weitere Sicherungsmaßnahmen eine personenbezogene Zuordnung der abgegebenen Stimme möglich macht. Wie sich unter diesen Bedingungen sowohl die Sicherung des Wahlgeheimnisses als auch die Nachprüfbarkeit des Wahlvorganges technisch realisieren lassen, ist bisher nicht völlig geklärt. Aufwändige kryptographische Verfahren müssen hierzu entwickelt und offengelegt werden. Notwendig ist aber auch ein effektiver Schutz der beteiligten Rechner gegen Hacker-Angriffe ebenso wie gegen verteilte Überflutungsangriffe (distributed denial of service attacks), die die Stimmabgabe vereiteln können.

Verfahren des electronic voting sollten zunächst nur bei organisationsinternen Wahlen wie Personal- und Betriebsratswahlen eingesetzt werden, sofern die rechtlichen Voraussetzungen hierfür gegeben sind. Keine Bedenken bestehen gegen den Einsatz von unvernetzten Wahlcomputern in den Wahllokalen etwa auf kommunaler Ebene. Erst in einer nächsten Stufe könnte man dazu übergehen, amtliche Wahlcomputer bei Wahlen zu gesetzgebenden Körperschaften miteinander zu vernetzen. Beim Einsatz nicht-zertifizierter Hard- und Software zur Teilnahme an allgemeinen Wahlen ist das Risiko auf absehbare Zeit zu groß, weil die Integrität des demokratischen Wahlvorgangs vor allem technisch und organisatorisch noch nicht sichergestellt werden kann.

# 2 Technisch-organisatorische Entwicklungen

## 2.1 Sicherheit im Landesverwaltungsnetz

Bereits in zurückliegenden Tätigkeitsberichten haben wir über datenschutzrechtliche Aspekte beim Anschluss lokaler Netze an das Landesverwaltungsnetz Brandenburg (LVN) berichtet. Die folgende Darstellung zeigt, dass dieses Thema nichts an Aktualität eingebüßt hat.

### 2.1.1 Sicherheitskonzepte der Fachnetzbetreiber

Das Landesverwaltungsnetz Brandenburg besteht aus dem Fachnetz des Landesbetriebes für Datenverarbeitung und Statistik (LDS), dem Fachnetz

der Polizei und dem Fachnetz der Finanzverwaltung. Bereits vor einigen Jahren vereinbarten die Netzbetreiber, dass für jedes Fachnetz ein separates Sicherheitskonzept erstellt wird. Im letzten Jahr wurde nun endlich auch das letzte Sicherheitskonzept, nämlich das des Fachnetzes der Finanzverwaltung, fertiggestellt.

Die Erstellung von Sicherheitskonzepten ist eine wichtige organisatorische Maßnahme, die realisiert werden sollte, bevor eine so komplexe Infrastruktur, wie die des Landesverwaltungsnetzes, den Betrieb aufnimmt. Auch bei zukünftigen Erweiterungen des LVN sollten die Sicherheitskonzepte stets den aktuellen Gegebenheiten angepasst werden. Eine der wichtigsten Maßnahmen ist dabei die landesweite Einführung eines einheitlichen Verschlüsselungssystems.

Nachdem für die Fachnetze des Landesverwaltungsnetzes nunmehr die erforderlichen Sicherheitskonzepte vorliegen, sind diese permanent zu aktualisieren und konsequent umzusetzen.

### 2.1.2 GroupWise oder Exchange oder was?

Vor einigen Jahren war das Programm GroupWise noch das einzige Bürokommunikationssystem des Landes Brandenburg. Seit einiger Zeit steht mit Microsoft (MS) Exchange eine zweite Kommunikationsplattform zur Verfügung. Für die Kopplung der beiden Welten ist ein sog. Connector zuständig. Er konvertiert die E-Mails, Termine, Jobs usw. von einem Kommunikationssystem in das jeweils andere. Im Berichtszeitraum kam es vor, dass E-Mails bei der Übertragung von einem System in das andere verloren gingen, weil der Connector nicht funktionierte. Dadurch war die Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt. Auch der in diesem Jahr aufgetretene Virus „I love you“[19] hatte Auswirkungen auf die Nutzung des MS Exchange-Systems. Positiv ist in diesem Zusammenhang hervorzuheben, dass nach dem Bekanntwerden des Virus der LDS auf der zentralen Firewall des Landes sofort einen entsprechenden Virus-Filter einrichtete, um größeren Schaden bei den am LVN angeschlossenen Einrichtungen zu verhindern.

Es bleibt zu hoffen, dass sich das Land Brandenburg in den nächsten Jahren nicht noch für weitere Bürokommunikationsplattformen entscheidet, um Personal und andere Ressourcen nicht für Anpassungsarbeiten der verschiedenen Bürokommunikationsplattformen zu vergeuden, sondern sich wichtigeren Dingen, wie z. B. der Einführung eines landeseinheitlichen Verschlüsselungs- und Signaturverfahrens, zu widmen.

---

[19] s. Punkt A 2.2

Der "Love-Letter"-Virus hat gezeigt, dass bestimmte Systeme der Bürokommunikation besonders gefährdet sind. Viren-Filter und Firewall-Technik können größere Schäden jedoch verhindern. Ein Wildwuchs verschiedener Kommunikationsformen muss vermieden werden.

### 2.1.3 Ungesicherte, externe Zugänge zum Landesverwaltungsnetz

Die Sicherheit im Landesverwaltungsnetz hängt im starken Maße von den angeschlossenen lokalen Netzen ab. Im letzten Berichtszeitraum wurde bekannt, dass am LVN angeschlossene Daten verarbeitende Stellen eigene externe, ungesicherte Internet-Zugänge betreiben. In den Empfehlungen für den Einsatz von Informationstechnik in der Landesverwaltung ist eindeutig geregelt, dass externe Zugänge nur in Absprache mit dem LDS und unter Verwendung zusätzlicher Sicherheitseinrichtungen realisiert werden dürfen. Es ist daher unzulässig, z. B. mit Hilfe eines Modems, eine ungesicherte Verbindung zum Internet aufzubauen.

Die Fachnetzbetreiber sollten in ihren Netzen überprüfen, ob illegale Zugänge bestehen und in solchen Fällen die lokalen Netze der betroffenen Daten verarbeitenden Stellen vom LVN trennen.

### 2.1.4 Richtfunkstrecken und Funk-LAN-Systeme

Im zunehmenden Maße werden von den am LVN angeschlossenen Einrichtungen auch Richtfunkstrecken und Funk-LAN-Systeme eingesetzt. Da ein Abhören von personenbezogenen Daten bei diesen Verbindungen nicht ausgeschlossen werden kann, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI), die übertragenen Daten mit sicheren kryptographischen Verfahren zu verschlüsseln. Diese Empfehlung ist nachhaltig zu unterstützen. Wir beabsichtigen, die im LVN genutzten Richtfunkstrecken und Funk-LAN-Systeme im nächsten Berichtszeitraum bezüglich eingesetzter Verschlüsselungsverfahren zu überprüfen.

### 2.1.5 Sicherheit durch Firewalls

Die Arbeitskreise „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben die Orientierungshilfe zu „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ überarbeitet. Die aktuelle Fassung mit Stand vom November 2000 kann von unserer Website[20] abgerufen werden. Die Themen „Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall“ und „Zusatzmaßnahmen bei der Verarbeitung sensibler Daten“ wurden in die

[20] http://www.lda.brandenburg.de/empfehl/oh_inter/oh_int.htm

Orientierungshilfe neu aufgenommen.

Selbst bei ausschließlicher Nutzung des Protokolls HTTP kann eine unzulässige Datenübermittlung nicht ausgeschlossen werden. Sowohl die HTTP-Anfragen als auch die HTTP-Antworten können beliebige Nutzlasten transportieren. Durch Missbrauch von HTTP können selbst restriktiv konfigurierte Firewalls oder Proxy-Server „durchtunnelt“ werden. Das Simple Object Access Protocol (SOAP) nutzt beispielsweise HTTP und XML, damit Programme in verteilten Umgebungen auf verschiedenen Plattformen miteinander kommunizieren können.
Der Anschluss von Netzen der öffentlichen Verwaltung an das Internet kann nur dann datenschutzgerecht erfolgen, wenn sicherheitsrelevante Entwicklungen aktuell berücksichtigt werden. Auch bei umfangreichen technisch-organisatorischen Maßnahmen bleibt ein Restrisiko in jedem Fall erhalten.

## 2.2 Virtuelle "Liebesbriefe" und andere Computerviren

*Mit der zunehmenden Vernetzung der Computersysteme steigt die Gefahr des Verlustes oder der Verfälschung von Daten durch Computerviren. Im Jahr 2000 gelangte diese Problematik durch den "Love Letter"-Virus in die Schlagzeilen.*

Computerviren können im Prinzip bei allen Betriebssystemen auftreten. Am meisten bedroht sind jedoch IBM-kompatible Personalcomputer (PC). Im UNIX-Bereich sind bisher kaum Viren zu konstatieren und im Großrechnerbereich spielen Viren aufgrund von besseren Sicherheitseinrichtungen und der geringen Verbreitung keine Rolle.

Die Anzahl und die Art verschiedener Viren steigen täglich. Klassische Computerviren sind die Boot- und Fileviren. Bootviren infizieren den Bootsektor und den Partitionssektor von Datenträgern und verbreiten sich über infizierte Disketten beim Warmstart eines Rechners. Fileviren infizieren Programme (Wirtsprogramme) und werden durch deren Aufruf aktiviert.

Eine weitere Variante sind die Makroviren. Sie können sich über Betriebssystemgrenzen hinaus verbreiten, da sie über Anwendungen mit der Möglichkeit der Makroprogrammierung gekoppelt sind. Verbreitet sind Makroviren vor allem für Microsoft-Anwendungen (Word, Excel und Access), aber auch in anderen Office-Produkten sind inzwischen Makroviren vorgekommen.

Eine andere Gruppe Schaden stiftender Software sind die sog. Trojanischen Pferde. Sie haben im Gegensatz zu Viren keinen Vermehrungsteil, sondern setzen sich als Programme auf einem Computer fest und versuchen, diesen

auszuforschen. So können auf dem befallenen Computer Kennworte ausgelesen, Dateien kopiert, umbenannt oder gelöscht sowie andere Aktionen vom Computer des Angreifers her ausgeführt werden. Trojanische Pferde werden über E-Mail-Sendungen, aber zunehmend auch über Java-Applets und ActiveX-Controls innerhalb des WorldWideWeb (WWW) in lokale Netze eingeschleppt.

Neben vielen weiteren Virenarten haben im Jahr 2000 vor allem die "Würmer" oder Internet-Mail-Viren für Aufregung gesorgt. Sie sorgen durch ihre massenhafte und kurzfristige Vermehrung für Systemabstürze. Dazu wird das Adressbuch des Mail-Clients genutzt, um den Virus an verschiedene Internetteilnehmer im "Schneeball-System" zu verschicken.

Der Computervirus "Love Letter" hat sich Anfang Mai 2000 äußerst schnell weltweit mit Hilfe des Microsoft E-Mail-Programms Outlook auf Millionen von Windows-Rechnern verbreitet. Neben der erheblichen Beeinträchtigung des E-Mail-Verkehrs, der teilweise zum Zusammenbruch befallener Systeme führte, sind zudem auch Dateien auf den Rechnern der Anwender gelöscht oder unbrauchbar gemacht worden. Diese Virenattacke hat eindrucksvoll bewiesen, dass ein einzelner Computervirus per E-Mail innerhalb kürzester Zeit ganze Wirtschafts- und Verwaltungsbereiche lahm legen kann. Da auf diese Weise personenbezogene Daten nicht mehr verfügbar sind, ist dadurch auch der Datenschutz beeinträchtigt.

Nach Angaben des Innenministeriums hat die Landesverwaltung Brandenburg diesen "berühmtesten" Virenbefall im Jahr 2000 ohne nennenswerte Beeinträchtigungen überstanden. Dies lag vor allem daran, dass im Landesverwaltungsnetz hauptsächlich GroupWise und nicht das angegriffene Mail-Programm Microsoft Outlook eingesetzt wird. Da weltweit etwa 90 Prozent der Desktop-Rechner unter Windows laufen und diese Nutzer auch meist Outlook oder Outlook-Express als Mail-Programm nutzen, sind diese Programme häufig das Ziel von Hacker-Angriffen. Als Konsequenz daraus sollten E-Mails auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern stets darauf hin geprüft werden, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde. Weiterhin sollten keine ausführbaren Programme (*.COM, *.EXE) oder Script-Sprachen (*.VBS, *.BAT) geöffnet werden.

Behörden, die besonders sensible personenbezogene Daten verarbeiten, sollten auf einen Internetanschluss ihres Netzes vollkommen verzichten und sich nur über Einzelplatz-PCs an das WWW anschließen. Das Internet ist die

Hauptquelle von Computerviren aller Art. Auch wenn ein lokales Netz einer Behörde am Landesverwaltungsnetz angeschlossen ist, sollte der zentrale Zugang über ein Firewallsystem mit einem integrierten Virenscanner erfolgen. Entscheidend für einen gut funktionierenden Virenschutz ist eine stets aktuelle Anti-Virensoftware.

Moderne Virenscanner sind in der Lage, auch die Anlagen einer E-Mail zu öffnen und diese z. B. auf Makroviren zu überprüfen. Ein Problem stellen allerdings verschlüsselte Nachrichten dar. Diese können erst nach der Entschlüsselung auf Viren untersucht werden. Es ist deshalb erforderlich, auf den besonderen Rechnern, auf denen die Mails entschlüsselt werden, ebenfalls Virenscanner einzusetzen.

Neben den externen Anschlüssen sollte auch der Import über Datenträger kontrolliert werden. Laut einer Studie des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) sind häufig Original-Software und vorinstallierte Geräte Quellen von Computerviren. Alle Dateien - auch Standardsoftware - sind vor dem Kopieren in das System auf Viren zu überprüfen. Die Disketten- und CD-Laufwerke der Nutzer sollten nach Möglichkeit gesperrt und Dateien nur über eine zentrale Stelle mit Virenprüfung im- und exportiert werden. Ist ein System trotz aller Vorsichtsmaßnahmen verseucht, kann oft die Funktionsfähigkeit nur durch eine Neuinstallation der Software wieder hergestellt werden. Dann ist eine virenfreie aktuelle Datensicherung Grundlage eines schnellen und nacharbeitsarmen Wiederanlaufes des Rechnernetzes.

Im Internet gibt es z. B. über die Seiten des BSI[21] oder über das seit Anfang Dezember 2000 in Betrieb genommene gemeinsame Portal der Datenschutzbeauftragten[22] ("Das virtuelle Datenschutzbüro") ausführliche Informationen über Computerviren, vorbeugende Maßnahmen und zum Verhalten bei Befall.

Lokale Computernetze sollten möglichst wenig externe Ein- und Ausgabemöglichkeiten besitzen, die zudem stets mit aktueller Virenscannersoftware betrieben werden sollten. Beim ersten Auftreten eines Virus kann allerdings auch diese - genau wie bei einem Impfstoff - noch nicht helfen. Hohe Aufmerksamkeit und eine gesunde Skepsis sind beim Umgang mit E-Mails daher angebracht. Es muss davon abgeraten werden, lokale Netze ohne strikte Sicherheitsmaßnahmen mit dem Internet zu verbinden.

## 2.3 Open-Source-Software für mehr Transparenz in der Datenverarbeitung

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

[22] http://www.datenschutz.de

*Unter Open-Source-Software (OSS) versteht man Software, deren Quelltext offen gelegt und für jeden frei verfügbar ist. So kann prinzipiell jeder fachkundige Nutzer prüfen, ob das Programm tatsächlich die angegebene Funktionalität realisiert und darüber hinaus keine unerwünschten Funktionen ausführt. Bei Bedarf wird eine Anpassung oder Weiterentwicklung durch den Nutzer möglich. OSS ist in der Regel frei kopierbar und damit sehr preiswert. Dies dürfte ein wesentlicher Grund dafür sein, dass sie gerade jetzt besonderes Interesse in der öffentlichen Verwaltung findet. So fördert das Bundesministerium für Wirtschaft und Technologie die Entwicklung eines Kompetenzzentrums für OSS u. a. mit dem Ziel, die Sicherheit und den Wettbewerb in der Informationsgesellschaft zu fördern und die Öffentlichkeit über Vor- und Nachteile beim Einsatz von OSS zu informieren.*

Im Gegensatz dazu halten die großen Hersteller von weit verbreiteten proprietären Betriebssystemen ihre Quellcodes seit jeher geheim. Das hat im vergangenen Jahr dazu geführt, dass das Bundesamt für die Sicherheit in der Informationstechnik das Betriebssystem Windows 2000 erst positiv bewertet hat, nachdem der Hersteller sich bereit erklärt hatte, ein kritisches Modul zu entfernen, das angeblich Daten des Anwenders ausspähen und an Dritte weitergeben konnte. Eine Offenlegung des Quellcodes hatte der Hersteller abgelehnt. OSS wird von uns demgegenüber als besonders datenschutzfreundliche Technologie eingeschätzt, da sie u. a. die folgenden Forderungen erfüllt:

1. Durch die Offenlegung des Quellcodes ist sie transparent und kann durch unabhängige Experten uneingeschränkt überprüft werden. Damit erhöht sich die Revisionsfähigkeit der Software maßgeblich.

2. Die Programme können dem individuellen Bedarf angepasst werden, z. B. um lediglich die benötigten Module für die erforderliche Funktionalität zu installieren. Dies dient der Datensparsamkeit und Datensicherheit.

3. Eine Evaluation und Zertifizierung nach IT-Sicherheitskriterien ist bei OSS-Produkten einfacher möglich, insbesondere kann der Code auf Trojanische Pferde oder einprogrammierte Hintertüren besser untersucht werden.

4. Es wird überprüfbar, ob ein System auf ausgereiften Sicherheitsmechanismen basiert, etwa auf anerkannt sicheren kryptographischen Verfahren, denn im Bereich der Kryptographie gilt die Offenlegung von Algorithmen bei vielen Experten als wichtige Voraussetzung für deren

Wirksamkeit.

5. Das Vertrauen des Anwenders in OSS wird gestärkt, da er überprüfen kann, welche Daten wie verarbeitet werden, wohin diese Daten übertragen werden und wie Sicherheitsfunktionen aktiviert werden. Die Nutzung der Informationstechnik wird für den Anwender dadurch transparenter.

Viele Anwender werden allerdings mangels spezieller Programmierkenntnisse und angesichts der hohen Komplexität moderner Datenverarbeitungsprogramme die oben aufgeführten Vorteile der OSS nicht voll nutzen können. Vor ihrem Einsatz sollte man sich auch über die möglichen Einschränkungen, die ihre Nutzung mit sich bringen kann, informieren. Dazu gehören u. a.:

1. Entwickler bieten in der Regel keine Gewährleistung oder Haftung und keinen regelmäßigen Support.

2. Die Revision von OSS durch unabhängige Fachleute ist nicht automatisch sichergestellt und eine zeitnahe Fehlerbehebung wird nicht garantiert.

3. Qualitätssicherungsmaßnahmen sind mitunter stark eingeschränkt und oftmals liegt keine ausreichende Programmdokumentation vor.

4. Gegebenenfalls noch vorhandene Sicherheitslücken sind für potentielle Angreifer leichter nutzbar. Transparenz erhöht nicht automatisch die Datensicherheit, sondern nur die Wahrscheinlichkeit, dass Sicherheitsmängel aufgedeckt werden.

Die Nutzung von Open-Source-Software ist ein geeignetes Verfahren, um die Transparenz der Datenverarbeitung zu erhöhen. Sie ermöglicht die Prüfung und Revision durch fachkundige Experten und ist somit geeignet, das Vertrauen der Anwender in die von ihnen genutzte Software zu stärken.

## 2.4 Verschlüsselung von personenbezogenen Daten auf mobilen Computern

*Tragbare Computer können die Tätigkeit von Behördenbediensteten erleichtern. Personenbezogene Daten, die auf ihnen gespeichert werden, sind jedoch besonders gefährdet.*

In den Verwaltungen werden in zunehmendem Maß mobile Computer, wie Laptops, Notebooks u. ä. Geräte eingesetzt. Im Gegensatz zum Arbeitsplatz-

computer ergeben sich durch die Mobilität und das Fehlen eines definierten Arbeitsumfeldes eine Reihe zusätzlicher Bedrohungen. Werden personenbezogene Daten auf den mobilen Rechnern verarbeitet, so sollten diese mittels sicherer kryptographischer Verfahren (z. B. 3DES, IDEA, RSA) verschlüsselt werden. Durch den Einsatz kryptographischer Verfahren wird ein hohes Maß an Datensicherheit erreicht, sodass gerade bei mobilen Rechnern ein Missbrauch personenbezogener Daten nahezu ausgeschlossen werden kann. Bei Diebstahl eines solchen Gerätes wäre zwar ein materieller Schaden zu beklagen, die verschlüsselten Daten könnten jedoch nicht sinnvoll verwendet werden.

Als positives Beispiel kann man in diesem Zusammenhang das Gesundheitsamt der Stadt Potsdam hervorheben, bei dem alle auf Laptops verarbeiteten personenbezogenen Daten verschlüsselt gespeichert werden.

Bei der Verwendung mobiler Rechner entspricht der Einsatz von Sicherheitssoftware zur Verschlüsselung personenbezogener Daten dem heutigen Stand der Technik und ist deshalb datenschutzrechtlich unabdingbar.

## 2.5 Berücksichtigung technisch-organisatorischer Maßnahmen bereits bei der Gebäudeplanung

*Mit der letzten Novellierung des Brandenburgischen Datenschutzgesetzes im Jahre 1999 wurden die in § 10 enthaltenen Anforderungen an technisch-organisatorische Maßnahmen bei der automatisierten Verarbeitung personenbezogener Daten erhöht.*

Während es sich in der 1. Fassung des Brandenburgischen Datenschutzgesetzes zunächst um die Erfüllung von gewissen Mindestanforderungen handelte, die sich am erforderlichen Aufwand orientieren sollten, geht es jetzt um eine Einzelfallbetrachtung, die Risikoanalyse und die ständige Ausrichtung der technisch-organisatorischen Maßnahmen am jeweiligen Stand der Technik. Damit sind diese neuen Bestimmungen auf Zukunft angelegt und stellen eine bedeutende Verbesserung dar.

Die betreffenden Maßnahmen müssen dem angestrebten Schutzzweck entsprechen. Die Beurteilung der Angemessenheit unterliegt teilweise subjektiven Kriterien und stellt die Behörden vor die nicht leichte Entscheidung, die auf den speziellen Einzelfall zugeschnittenen Datensicherungsmaßnahmen selbst festlegen zu müssen. Neben der Art der zu verarbeitenden personenbezogenen Daten und dem damit möglichen Missbrauchspotential ist auch das gesamte organisatorische und territoriale Umfeld innerhalb der Einrichtung zu berücksichtigen.

Unsere Kontrollen ergaben, dass der Aufwand für Datensicherungsmaßnahmen besonders in solchen Einrichtungen wesentlich reduziert werden konnte, in denen man die Maßnahmen in der Bauplanung möglichst frühzeitig berücksichtigte. So sind beispielsweise für einen im Gebäudeinneren liegenden, fensterlosen Serverraum wesentlich geringere Aufwendungen für die Datensicherheit erforderlich, als für einen Server, der sich in einem Raum im Erdgeschoss eines Gebäudes mit einem Fenster zu einer öffentlich zugänglichen Straße befindet. Bei der Erstellung eines Projektes vernachlässigte Sicherheitsanforderungen führen meist zu Nachrüstungen, die sich häufig als schwierig und kostenintensiv erweisen. Wir würden es deshalb begrüßen, wenn alle Bauämter bereits bei der Projektierung von Gebäuden für öffentliche Stellen gesetzliche Vorgaben des Datenschutzrechts berücksichtigten.

Fehlentscheidungen wie in einem neu errichteten Finanzamt, in dem sich die Telekommunikationsanlage mit der dazugehörigen Gebührendatenverarbeitungsanlage in einem völlig ungeeigneten Raum befindet, könnten so für die Zukunft vermieden werden. Allerdings zeigte das Ministerium der Finanzen in diesem Fall aus Kostengründen bisher keine Bereitschaft, entsprechende, von uns empfohlene Nachrüstungen vorzunehmen oder zumindest die sensiblen Gebührendatenbestände sicherer unterzubringen.

Durch die frühzeitige Berücksichtigung datenschutzrechtlicher Forderungen bereits in der Projektierungsphase lassen sich die Kosten für Sicherheitsmaßnahmen wesentlich reduzieren.

# 3 Telekommunikation und Medien

## 3.1 Datenfriedhöfe bei Telekommunikationsunternehmen - neues Datenschutzrecht in der Telekommunikation

*Am 22. November 2000 hat die Bundesregierung die seit langem überfällige neue Telekommunikations-Datenschutzverordnung (TDSV) verabschiedet, nachdem zuvor der Bundesrat zugestimmt hat[23]. Gegenüber der bisher geltenden Verordnung sowie den ersten Entwürfen[24] konnten in einigen Punkten datenschutzrechtliche Verbesserungen erreicht bzw. Verschlechterungen verhindert werden, was nicht zuletzt auf das einheitliche Vorgehen der Datenschutzbeauftragten des Bundes und der Länder zurückzuführen ist. Dennoch enthält die neue TDSV auch Veränderungen, die das Recht der Bürgerinnen und Bürger auf freie und*

[23] *BGBl. I 2000 S.1740 ff.*

[24] *s. Tätigkeitsbericht 1999, Pkt. 3.2, S. 34 f.*

*unbeobachtete Telekommunikation zum Teil erheblich einschränken.*

Die Bundesregierung hatte zunächst bereits im Mai 2000 die neue TDSV verabschiedet, die jedoch noch der Zustimmung durch den Bundesrat bedurfte. Bereits in dieser Fassung waren auch einige unserer Kritikpunkte berücksichtigt worden. So wurde die Absicht fallen gelassen, auch rückwirkende Fangschaltungen zu ermöglichen. Ebenso bleibt die Invers-Auskunft, bei der man mit Hilfe der Telefonnummer den Namen oder die Anschrift des Teilnehmers ermitteln kann, verboten. Zu begrüßen ist die Verpflichtung der Diensteanbieter, sich bei der Verarbeitung personenbezogener Daten an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten. Schließlich wurde die Befugnis eingeschränkt, einen Gesamtdatenbestand aus Bestands- und Verbindungsdaten zur Missbrauchsbekämpfung durchzurastern. Dies ist jetzt nur in pseudonymisierter Form erlaubt.

Zu kritisieren ist aber, dass der Bundesrat auf Druck der Innenministerien des Bundes und der Länder einer Erweiterung der Befugnis der Diensteanbieter, Verbindungsdaten zu Abrechnungszwecken zu speichern, von bisher 80 Tagen auf sechs Monate seit Ende der Verbindung zugestimmt hat. Dabei hatte der Wirtschaftsausschuss des Bundesrates die Annahme eines Kompromissvorschlages empfohlen, den die Datenschutzbeauftragten des Bundes und der Länder mit dem Länderarbeitskreis "Telekommunikation, Informationswirtschaft, Post" erarbeitet hatten. Dieser Vorschlag sah kürzere Speicherfristen vor, die aus Sicht der Wirtschaftsministerien und der Telekommunikationsunternehmen für den Zweck der Gebührenabrechnung ausreichend gewesen wären. Obwohl wir die Ministerien für Wirtschaft und des Innern gebeten hatten, der Empfehlung des Wirtschaftsausschusses zu folgen, hat die Landesregierung im Bundesratsplenum einer Verlängerung der Speicherfristen zugestimmt.

Ursprünglich dienten die Speicherfristen allein dazu, die von den Nutzerinnen und Nutzern in Anspruch genommenen Telekommunikationsdienstleistungen abzurechnen. Die nun erfolgte Verlängerung bezweckt aber nicht mehr, den Anbietern das Abrechnungsverfahren zu erleichtern, sondern die Zugriffsmöglichkeiten der Sicherheitsbehörden erheblich zu erweitern. Vor diesem Hintergrund kommt die Verlängerung der Speicherfrist einer verfassungsrechtlich bedenklichen Datenspeicherung auf Vorrat für eventuell in der Zukunft stattfindende Zugriffe der Sicherheitsbehörden gleich. Damit werden alle Nutzenden zu potentiellen Kriminellen abgestempelt. Die Verlängerung der Speicherfrist ist für den genannten Zweck allerdings ohnehin nicht geeignet, da die Kundinnen und Kunden im Einzelfall eine Verkürzung der Speicherungsdauer vertraglich vorsehen können. Zudem sei

daran erinnert, dass in den vor der Digitalisierung bestehenden analogen Telefonnetzen eine weitgehend spurlose Telekommunikation möglich war. Die ISDN-Technik und die neue TDSV machen moderne Telekommunikationsnetze zugleich zu einer überwachungsgeneigten Infrastruktur.

Die neue Telekommunikations-Datenschutzverordnung behält in wesentlichen Punkten das hohe Datenschutzniveau für Nutzerinnen und Nutzer von Telekommunikationsdiensten bei. Zu kritisieren ist aber insbesondere die Verlängerung der Speicherfristen von Verbindungsdaten im Interesse der Sicherheitsbehörden und damit zu einem sachfremden Zweck.

## 3.2 Kampf gegen die Datennetzkriminalität - aber wie?

*Das Internet entwickelt sich zunehmend zum neuen Massenmedium neben den herkömmlichen Printmedien, Hörfunk und Fernsehen. Es wird zur weltweiten Kommunikation, zur Informationssammlung, zum Abschluss elektronischer Rechtsgeschäfte, zum Spielen, aber auch zur Begehung von Straftaten genutzt. Anbieter von Informationen und Dienstleistungen werden selbst Opfer von kriminellen Angriffen mit Computerviren [25] oder von "Überflutungsangriffen" (Denial of Service-Attacks), die sich im vergangenen Jahr mehrten. Das Computerstrafrecht ist weltweit sehr unterschiedlich entwickelt. So sind bestimmte Manipulationen in Datennetzen zwar nach deutschem Strafrecht, nicht aber unbedingt nach dem Strafrecht anderer Staaten zu ahnden.*

Der Europarat hat in Zusammenarbeit mit mehreren außereuropäischen Industriestaaten wie den USA, Kanada, Japan und Südafrika Entwürfe für eine Konvention gegen Datennetzkriminalität (Convention on Cyber-Crime) erarbeitet[26]. Die Unterzeichnerstaaten sollen sich verpflichten, bestimmte einheitliche Straftatbestände zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Datenverarbeitungssystemen einzuführen. Des Weiteren sollen die verfahrensrechtlichen Voraussetzungen geschaffen werden, damit gespeicherte Daten einschließlich der Verbindungsdaten grenzüberschreitend anderen Vertragsstaaten der Konvention beschleunigt zur Verfügung gestellt werden können. Außerdem sollen die Vertragsstaaten Maßnahmen treffen, um die Echtzeit-Überwachung des Internet-Verkehrs einschließlich des Abfangens von Inhaltsdaten ohne präzise Zweckbestimmung zu ermöglichen.

---

[25] *s. Pkt. A 2.2*

[26] zuletzt der 25. Entwurf, in englischer Sprache abrufbar unter <http://conventions.coe.int/treaty/EN/projets/cybercrime.25.htm>

Auch wenn der Konventions-Entwurf noch nicht unterschriftsreif ist, zeichnet sich hier eine Entwicklung ab, die aus verschiedenen Gründen Anlass zur Kritik gibt. Obwohl der Europarat eine lange Tradition bei der Sicherung des grenzüberschreitenden Datenschutzes seit der Verabschiedung der Datenschutzkonvention Nr. 108 von 1981 hat, nimmt der Entwurf für eine Konvention gegen Datennetzkriminalität darauf keinen Bezug. Vielmehr ist der neue Entwurf gekennzeichnet von einer vorrangigen Berücksichtigung der Interessen der Sicherheitsbehörden. Die schutzwürdigen Belange unverdächtiger Internet-Nutzer bleiben unberücksichtigt.

Zwar ist ein Vorbehalt des jeweiligen innerstaatlichen Rechts vorgesehen. Dennoch besteht die Gefahr, dass die Strafverfolgungsbehörden das Schutzniveau des jeweiligen nationalen Rechts, in Deutschland vor allem das Telekommunikationsgeheimnis des Grundgesetzes, durch internationale Absprachen aufweichen wollen. Es soll internationaler Druck auf den nationalen Gesetzgeber erzeugt werden, die Überwachungsmöglichkeiten unter Hinweis auf weitergehende Tendenzen auf internationaler Ebene über das in Deutschland verfassungsverträgliche Maß hinaus auszudehnen.

Diese Tendenz hat bereits in einem Beschluss der deutschen Innenministerkonferenz vom 24. November 2000 ihren Niederschlag gefunden, in dem der Bundesgesetzgeber aufgefordert wird, für Zwecke der Strafverfolgung den Providern und Betreibern von Servern eine Pflicht zur Protokollierung der IP-Adresse und des Nutzungszeitraumes sowie eine angemessene Aufbewahrungszeit der Daten "vorzuschreiben".

Eine derartige Regelung verstieße gegen die eindeutigen Vorgaben des Grundgesetzes, die nach der Rechtsprechung des Bundesverfassungsgerichts die Speicherung personenbezogener Daten ausschließen, wenn sie zu einer Rundumbeobachtung der Bürgerinnen und Bürger führt. Eine generelle Protokollierung von personenbezogenen Informationen über die Internet-Nutzung käme einer Verpflichtung der Post gleich, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen zukünftigen Strafverfolgung bereit zu halten. Mit einer solchen pauschalen Registrierungspflicht würde das Internet in ein Fahndungsnetz verwandelt und alle rechtstreuen Internet-Nutzer würden unter Generalverdacht gestellt. Ein derart massiver Eingriff in die informationelle Selbstbestimmung und Kommunikationsfreiheit ist deshalb unverhältnismäßig. Eine unbeobachtete Nutzung des Internets im Sinne einer Informationsquelle und eines virtuellen Marktplatzes muss allen Bürgerinnen und Bürgern grundsätzlich auch in Zukunft möglich sein. Schon das geltende Recht sieht vor, dass Provider Adressen von an das Internet angeschlossenen Computern ab dem Zeitpunkt eines entsprechenden

richterlichen Beschlusses vorzuhalten haben. Dies stellt eine angemessene Lösung dar.

Aus diesem Grund ist der Entwurf des Europarates für eine Konvention gegen Datennetzkriminalität auch international von Fachleuten abgelehnt worden. Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat in einem gemeinsamen Standpunkt [27] die Bedeutung des Telekommunikationsgeheimnisses im weltweiten Zusammenhang hervorgehoben und darauf hingewiesen, dass neue und sehr unbestimmt formulierte Straftatbestände nicht nur strafwürdige Manipulationen an Datenverarbeitungsnetzen, sondern auch legitime Verhaltensweisen erfassen können. Wichtiger als die Schaffung neuer Straftatbestände ist eine Verpflichtung der Diensteanbieter, die notwendigen Sicherheitsmaßnahmen zum Schutz ihrer Systeme vor Angriffen zu treffen, bevor sie diese an das weltweite Netz anschließen. Der allgemeine Sicherheitsstandard im Internet muss drastisch erhöht werden, was durch neue Straftatbestände nicht erreicht wird. Aus diesen Gründen hat auch der Vorsitzende der Internationalen Datenschutzkonferenz 2000 den Konventions-Entwurf gegenüber dem Europarat kritisiert. Sogar die Handelskammer der Vereinigten Staaten hat den Kongress aufgefordert, das Abkommen abzulehnen, weil es auch die Entwicklung des elektronischen Handels gefährde.

Internationale Kooperation ist zweifellos erforderlich, um Kriminalität im Internet auch grenzüberschreitend kontrollieren zu können. Dies muss aber anlassbezogen und unter strenger Zweckbindung stattfinden und darf nicht dazu führen, dass das Internet zu einem weltweiten Überwachungsnetz wird.

Bei den weiteren Beratungen über den Konventionsentwurf wird es deshalb darum gehen, die prinzipielle Möglichkeit zur unbeobachteten Nutzung internationaler Datennetze bei gleichzeitiger Gewährleistung der Zusammenarbeit der Strafverfolgungsbehörden im konkreten Einzelfall sicherzustellen.

## 3.3 Anbieterkennzeichnung

*Im Internet präsentieren sich immer mehr Landesbehörden, Kreise, Ämter und Gemeinden. Ein wichtiger Punkt, der beim Internetauftritt berücksichtigt werden muss, ist die Anbieterkennzeichnung. Im Berichtszeitraum stellten wir fest, dass auf den Websites der Landesbehörden nicht immer zu erkennen war, wer für diese verantwortlich zeichnete.*

[27] s. Dokumente zu Datenschutz und Informationsfreiheit 2000, A III

Gemäß § 6 Nr. 1 und 2 Mediendienstestaatsvertrag (MDStV) bzw. § 6 Teledienstegesetz (TDG) haben Diensteanbieter für ihre Angebote den Namen und die Anschrift sowie bei Personenvereinigungen und -gruppen auch den Namen und die Anschrift des Vertretungsberechtigten anzugeben.

Diese Vorschriften sind auch für den Datenschutz von Bedeutung, denn beim Abruf von Informationen aus dem World Wide Web verarbeiten die Anbieter häufig personenbezogene Daten und können sich ihren gesetzlichen Verpflichtungen nicht entziehen, indem sie unerkannt bleiben. Auf den Websites muss insbesondere auch erkennbar sein, ob es sich z. B. um Angebote der Stadtverwaltung oder die von privaten Firmen handelt. Die Angaben des Anbieters mit Namen und Dienstanschrift der verantwortlichen Person sollten - wie beim Impressum einer Zeitung - auf jeder Homepage zu finden sein.

Die gesetzliche Anbieterkennzeichnungspflicht ist bei der Präsentation im Internet einzuhalten; die entsprechenden Informationen sind leicht auffindbar anzuordnen.

## 3.4 Unzulässige Speicherung von Verbindungsdaten

### 3.4.1 Praktische Umsetzung der Dienstanschlussvorschriften durch die Landesbehörden

*Wie wir in unserem letzten Tätigkeitsbericht dargestellt haben, haben wir im Landesamt für Bauen, Wohnen und Straßenverkehr (LBVS) sowie in einem Finanzamt festgestellt, dass Verbindungsdaten dienstlicher Gespräche der dort Beschäftigten in unzulässiger Art und Weise gespeichert werden[28]. Während der erstgenannte Fall mit einem aus datenschutzrechtlicher Sicht zufriedenstellenden Ergebnis abgeschlossen werden konnte, ist die Lage bei den Finanzämtern nach wie vor nicht befriedigend.*

Das LBVS hat nach unserer datenschutzrechtlichen Prüfung im Jahre 1999 nicht nur die von uns empfohlenen technischen und organisatorischen Maßnahmen zur Sicherung insbesondere des Gebührencomputers umgesetzt, sondern auch die Gebührendatenverarbeitung entsprechend den Dienstanschlussvorschriften (DAV) gestaltet. So wird die noch relativ neue Telekommunikationsanlage (TK-Anlage) des Landesamtes für Bauen, Verkehr und Straßenbau nunmehr mit einer Software betrieben, die nach den datenschutzrechtlichen Vorschriften der DAV arbeitet. Diese ermöglicht es, per Zufallsprinzip eine bestimmte Zahl von Nebenstellen auszuwählen, deren Verbindungsdatensätze für einen bestimmten Zeitraum gespeichert werden.

[28] *s. Tätigkeitsbericht 1999, Pkt. A 3.3.1*

Alle übrigen werden entsprechend Ziff. 3.1.3 DAV mit Verbindungsende gelöscht. Damit ist einer wesentlichen datenschutzrechtlichen Forderung entsprochen.

Anders stellt sich die Lage in den Finanzämtern des Landes Brandenburg dar. Wie wir in unserem letzten Tätigkeitsbericht ausgeführt hatten[29], wurden die Verbindungsdaten dienstlicher Gespräche nach unserem Hinweis nicht mehr gespeichert, mit der Folge, dass wegen der unzureichenden Software auch eine stichprobenartige Kontrolle nicht stattfinden konnte.

Obwohl die Finanzämter nach wie vor nicht mit DAV-gerechter Software ausgestattet sind, hält es das Ministerium der Finanzen dennoch für geboten, die stichprobenartigen Kontrollen der dienstlichen Gespräche wieder aufzunehmen. Es hat uns daher eine Übergangslösung bis zur Neufassung der Dienstanschlussvorschriften vorgeschlagen, die im Wesentlichen vorsieht, dass für die Dauer von einem Monat nach dem Ende der Verbindung wieder die Verbindungsdaten aller Dienstgespräche gespeichert werden sollen. Durch organisatorische Vorkehrungen soll sichergestellt werden, dass eine missbräuchliche Verwendung der gespeicherten Daten ausgeschlossen ist.

Diese Übergangslösung ist aus datenschutzrechtlicher Sicht nicht akzeptabel. Sie führt dazu, dass für einen Zeitraum, dessen Ende nicht abzusehen ist, in unverhältnismäßiger Weise personenbezogene Daten der Beschäftigten und ihrer Gesprächspartner gespeichert werden.

Eine Übergangslösung kann aus unserer Sicht deshalb nur so aussehen, dass auf die Speicherung von Verbindungsdaten dienstlicher Gespräche so lange verzichtet wird, wie die Gebührendatenverarbeitung der jeweiligen TK-Anlage nicht den Anforderungen der DAV entspricht. Auch durch organisatorische Maßnahmen können Verstöße gegen geltendes Recht nicht legitimiert werden.

Solange TK-Anlagen in Betrieb sind, die nicht den datenschutzrechtlichen Bestimmungen - insbesondere den DAV - entsprechen, muss im Zweifel auf die Speicherung von Verbindungsdaten dienstlicher Gespräche verzichtet werden. Alle öffentlichen Stellen des Landes sollten die inzwischen auf dem Markt verfügbare datenschutzfreundliche Software zur Gebührendatenverarbeitung so bald wie möglich einsetzen.

### 3.4.2 Telekommunikationsgeheimnis auch in der Kommunalverwal-

[29] s. Tätigkeitsbericht 1999, Pkt. A 3.3.1

**tung**

*Um ein einheitliches Datenschutzniveau beim Umgang mit personenbezogenen Daten im Zusammenhang mit der Nutzung von TK-Anlagen bei allen öffentlichen Stellen zu gewährleisten, haben wir im Berichtszeitraum die TK-Anlage einer Kreisverwaltung geprüft.*

Auch bei dieser Prüfung haben wir festgestellt, dass bei allen Dienstgesprächen Datum und Uhrzeit des Anrufs, Nebenstellen, vollständige Zielrufnummer, Dauer des Gesprächs sowie die verbrauchten Gebühreneinheiten erfasst und längstens drei Monate gespeichert werden. Die vollständige Speicherung der genannten Verbindungsdaten über einen längeren Zeitraum erfolgt hier ebenfalls zu dem Zweck, stichprobenartige Kontrollen der dienstlich geführten Gespräche vorzunehmen. Auch dies haben wir als Verstoß gegen das Telekommunikationsgeheimnis und gegen § 29 BbgDSG bemängelt. Allerdings liegt hier formal kein Verstoß gegen die DAV vor, da sich deren Geltungsbereich nicht auf die Kommunalverwaltung erstreckt. Dennoch haben wir empfohlen, dass sich auch Kommunalverwaltungen an die Vorschriften der DAV halten, da andernfalls ein unterschiedliches Datenschutzniveau für die Beschäftigten im öffentlichen Dienst des Landes Brandenburg herrschen würde.

Die Verbindungsdaten von Dienstgesprächen unterliegen dem verfassungsrechtlich durch Art. 10 Grundgesetz und Art. 16 der Brandenburgischen Landesverfassung geschützten Telekommunikationsgeheimnis. Dieses ist nicht auf Erbringer von Telekommunikationsdienstleistungen im Sinne des Telekommunikationgesetzes beschränkt. Da sich aus den Verbindungsdaten mitarbeiterbezogene Rückschlüsse auf deren Arbeits-, Sozial- und Telefonierverhalten ergeben können, sind die Mitarbeiter nicht nur in ihrer amtlichen Funktion betroffen, sondern durchaus auch als Träger von Grundrechten gegenüber ihrem Dienstherrn bzw. Arbeitgeber. Zudem führt die Speicherung vollständiger Zielrufnummern zur Verarbeitung von Daten Dritter. Aus diesen Erwägungen heraus haben auch Kommunalverwaltungen das Telekommunikationsgeheimnis zu wahren, obwohl die DAV hier nicht ausdrücklich anwendbar sind.

Wir haben der Kreisverwaltung daher empfohlen, die Gebührendatenverarbeitung so einzurichten, dass die Verbindungsdaten von Dienstgesprächen nur gespeichert werden, so weit sie zur stichprobenartigen Kontrolle erforderlich sind. Alle übrigen Verbindungsdaten müssen unmittelbar nach Verbindungsende gelöscht werden. Die technischen Voraussetzungen waren in der überprüften Kreisverwaltung vorhanden, da diese die gleiche TK-Anlage betreibt wie das unter 3.3.1 beschriebene

Landesamt für Bauen, Verkehr und Straßenbau. Im Übrigen entsprach die Verarbeitung personenbezogener Daten im Zusammenhang mit der TK-Anlage sowohl in rechtlicher als auch in technisch-organisatorischer Hinsicht den Anforderungen des Datenschutzes.

Das Telekommunikationsgeheimnis gilt für den Inhalt und die näheren Umstände der Telefongespräche von Beschäftigten der Kommunalverwaltungen. Die Kommunalverwaltungen sollten sich an die gleichen datenschutzrechtlichen Vorgaben beim Umgang mit TK-Anlagen halten wie die Landesbehörden. Wir empfehlen den Kommunen, die DAV entsprechend anzuwenden.

## 3.5 Einzelverbindungsnachweise für das Finanzamt - Registrierung der Telefon- und Internetnutzung am Arbeitsplatz für steuerliche Zwecke

*Das Bundesministerium der Finanzen hatte im Mai 2000 die Nachweispflichten von Steuerpflichtigen bei der steuerlichen Behandlung von Telefon- und Internetnutzung im Zusammenhang mit dem Arbeits- bzw. Dienstverhältnis neu geregelt[30]. Drei verschiedenen Fallkonstellationen wurden berücksichtigt:*

- *Für den Fall, dass der Arbeitnehmer seinen privaten Telefon- oder Internetanschluss in der Wohnung für betriebliche Zwecke nutzt und die daraus entstehenden Kosten vom Arbeitgeber ersetzt bekommt, sind diese Ersatzleistungen nach § 3 Nr. 50 Einkommenssteuergesetz (EStG) steuerfrei. Die betriebliche Veranlassung der Nutzung vom Arbeitnehmer sollte durch einen Einzelverbindungsnachweis der Telefongesellschaft bzw. eine detaillierte Abrechnung des Providers nachgewiesen werden.*

- *Für den Fall, dass der Arbeitgeber Telefon- bzw. Internetnutzungen von privaten Anschlüssen des Arbeitnehmers nicht erstattet, kann der Arbeitnehmer diese Aufwendungen als Werbungskosten geltend machen. Auch hier sollte die berufliche Veranlassung mit Einzelverbindungsnachweisen nachgewiesen werden.*

- *Gestattet der Arbeitgeber dem Arbeitnehmer die private Nutzung von dienstlichen Telekommunikations- bzw. Internet-Anschlüssen, so muss nach bisher geltendem Recht der Arbeitnehmer den daraus gewonnenen Vorteil als geldwerten Vorteil versteuern. Auch für diesen Fall sollten entsprechende Einzelverbindungsnachweise dem Finanzamt vorgelegt werden.*

---

[30] *Schreiben des Bundesministeriums für Finanzen vom 24. Mai 2000, BStBl. I S. 613*

Dieser Plan des Bundesministeriums der Finanzen stieß auf deutliche Kritik aus Wirtschaft und Verwaltung, weil er zu einem erheblichen bürokratischen Mehraufwand geführt hätte. Das Vorhaben war aber auch aus datenschutzrechtlicher Sicht zu kritisieren, da die detaillierte Nachweispflicht Daten betroffen hätte, die dem Telekommunikationsgeheimnis und dem Grundrecht auf informationelle Selbstbestimmung unterliegen. In diese Rechte wäre mit dem Erlass des Bundesfinanzministeriums in unverhältnismäßiger und ungeeigneter Weise eingegriffen worden, ohne dass die Abgabenordnung hierfür eine gesetzliche und verfassungsmäßige Grundlage enthält. Eine bloße Verwaltungsvorschrift des Bundesministeriums für Finanzen kann einen derart schwerwiegenden Eingriff nicht rechtfertigen.

Die vom Bundesministerium der Finanzen letztlich geforderte Vollprotokollierung der Zugriffe von Arbeitnehmerinnen und Arbeitnehmern im Internet widerspricht zudem diametral dem Grundsatz der Datensparsamkeit, wie er im Multimediarecht des Bundes und der Länder und auch in anderen neuen datenschutzrechtlichen Regelungen niedergelegt ist. Hinzu kommt, dass gerade bei der Nutzung des Internets nicht festgestellt werden kann, ob die Nutzung dienstlich oder privat veranlasst war, da nach dem geltenden Multimediarecht Nutzungsdaten wie die Adressen einzelner aufgerufener Seiten nach dem Ende der Verbindung gelöscht werden müssen.

Schließlich wäre die geplante detaillierte Nachweispflicht in der Praxis immer schwerer umzusetzen gewesen, weil gerade Unternehmen und Behörden aus Kostengründen zunehmend von Pauschaltarifen ohne zeitliche oder mengenmäßige Begrenzung (Flatrates) Gebrauch machen. Da hier einzelne Zugriffe nach Ende der Verbindung nicht einmal mehr für Abrechnungszwecke gespeichert werden dürfen, ist die Trennung des privaten Anteils an der Nutzung von dem beruflich veranlassten schon logisch nicht denkbar.

Aufgrund der massiven Kritik aus Wirtschaft, Verwaltung und der Datenschutzbeauftragten hat das Bundesministerium der Finanzen zwischenzeitlich das Schreiben vom 24. Mai 2000 wieder aufgehoben. Damit sind die bisherigen Regelungen zur steuerlichen Behandlung der vom Arbeitgeber ersetzten Ausgaben für Telefongespräche in der Wohnung des Arbeitnehmers und zur lohnsteuerlichen Behandlung der Aufwendungen für ein Autotelefon wieder anzuwenden.

Erfreulicherweise ist das Bundesministerium der Finanzen noch einen Schritt weitergegangen und plant nunmehr, die Telefon- und Internetnutzung am Arbeitsplatz künftig steuerfrei zu stellen, zumal angesichts der sinkenden Kommunikationskosten nennenswerte Steuerausfälle nicht zu erwarten sein

dürften. So soll im Rahmen einer geplanten Änderung des Investitionszulagengesetzes auch das Einkommenssteuergesetz so geändert werden, das die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen Personalcomputern und Telekommunikationsgeräten steuerfrei sind. Zu diesem Zweck soll eine neue Nr. 45 in § 3 EStG eingeführt werden. Damit wird in Zukunft jede Nachweispflicht bei der vom Arbeitgeber gestatteten privaten Nutzung von Kommunikationseinrichtungen entfallen. Dies ist aus datenschutzrechtlicher Sicht sehr zu begrüßen.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht begrüßt ausdrücklich die Absicht der Bundesregierung, die private Nutzung von Kommunikationseinrichtungen am Arbeitsplatz künftig von der Steuer freizustellen. Damit wird ein bürokratisches, aufwändiges und zudem datenschutzunfreundliches Verfahren aufgegeben.

## 3.6 Datensparsamkeit bei der Rundfunkfinanzierung

*Im Zusammenhang mit der letzten Erhöhung der Rundfunkgebühren durch den 5. Rundfunkänderungsstaatsvertrag und angesichts der fortschreitenden technischen Entwicklung beim Empfang von Radio und Fernsehen ist die Finanzierung des öffentlich-rechtlichen Rundfunks ins Blickfeld öffentlicher Diskussionen geraten. Das gegenwärtig praktizierte Verfahren zur Finanzierung des öffentlich-rechtlichen Rundfunks begegnet auch der Kritik der Datenschutzbeauftragten des Bundes und der Länder.*

Jeder, der ein Rundfunkgerät zum Empfang bereithält, muss sich bei der Gebühreneinzugszentrale (GEZ) anmelden. Da dessen ungeachtet viele Geräte nicht angemeldet sind, werden große Anstrengungen unternommen, um jeden Rundfunkteilnehmer zu erfassen. Dazu dienen folgende Datenquellen:

- die regelmäßige Übermittlung von Meldedaten,

- die Beschaffung von Anschriften potentieller Rundfunkteilnehmer von privaten Adresshändlern,

- die Tätigkeit der Rundfunkbeauftragten, die einzelne Haushalte aufsuchen.

Die auf dem jetzigen Modell der Rundfunkfinanzierung beruhende Verarbeitung personenbezogener Daten durch die Rundfunkanstalten und die GEZ ist aus folgenden Gründen zu kritisieren:

- Die GEZ speichert an zentraler Stelle personenbezogene Daten von über

30 Millionen Haushalten. Dies kommt praktisch einem "Bundesmelderegister" gleich, das immer wieder Begehrlichkeiten auch rundfunkfremder Stellen weckt, auf diesen Datenbestand zuzugreifen.

- Die inzwischen in fast allen Bundesländern praktizierte regelmäßige Datenübermittlung aus dem Melderegister ist ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung, da nach unseren Erkenntnissen etwa 70% der übermittelten Meldedaten für die Aufgaben der GEZ nicht erforderlich sind.

- Viele Bürgerinnen und Bürger beschweren sich bei uns über die Art und Weise der Ermittlung von sog. "Schwarzsehern" oder "Schwarzhörern" durch die Rundfunkbeauftragten sowie die umfangreichen Mailing-Aktionen nach Art der Direktmarketing-Branche[31].

Offen ist auch, wie in Zukunft mit der Tatsache umgegangen werden soll, dass Rundfunkempfang auch über PC‘s mit Internet-Zugang oder andere Technologien, wie UMTS, möglich ist. Derzeit werden auf diese Nutzungen noch keine Rundfunkgebühren erhoben. Das Problem ist durch den 5. Rundfunkänderungsstaatsvertrag allerdings lediglich bis Ende 2004 vertagt worden.

In einer auf der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedeten Entschließung[32] haben die Datenschutzbeauftragten die Bundesländer aufgefordert, bei einer Neuordnung ein Modell zugrunde zu legen, dass sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert.

Das bisherige System der Finanzierung des öffentlich-rechtlichen Rundfunks begegnet vielfältigen datenschutzrechtlichen Bedenken. Wir werden uns daher dafür einsetzen, dass im Zuge der ohnehin anstehenden Neuordnung der Rundfunkfinanzierung insbesondere die Grundsätze von Datenvermeidung und Datensparsamkeit berücksichtigt werden.

---

[31] zu den Mailing-Aktionen vgl. Tätigkeitsbericht 1999, Pkt. 3.4.2

[32] s. Dokumente zu Datenschutz und Informationsfreiheit 2000, A I

# 4. Inneres

## 4.1 Polizei

### 4.1.1 Änderung des Polizeirechts insbesondere zur Videoüberwachung öffentlicher Plätze

Am 23. Dezember 2000 trat das Zweite Gesetz zur Änderung des Brandenburgischen Polizeigesetzes in Kraft, mit dem erstmals eine offene Videoüberwachung bestimmter öffentlich zugänglicher Straßen und Plätze durch die Polizei zugelassen wurde[31]. Dieser Entscheidung des Gesetzgebers war eine lange und kontroverse Diskussion vorausgegangen, in der sich der Landesbeauftragte prinzipiell gegen die Schaffung einer solchen Befugnis ausgesprochen hatte. Er verwies dabei auf das Grundrecht aller Menschen, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch staatliche Kameras aufgezeichnet wird[32]. Der Schleswig-Holsteinische Landtag hat am 08.06. 2000 in einer Entschließung hervorgehoben, Videoüberwachung im öffentlichen Raum erfasse vor allem rechtstreue Bürgerinnen und Bürger und berge das Risiko eines sozialen Konformitätsdrucks, der weit über die Erwirkung rechtstreuen Verhaltens hinausschieße und Unbefangenheit und Freiheit zerstöre[33]. Die Personen, die sich in diesem Raum bewegen, können nämlich nicht wissen, ob und aus welchem Anlass die (offene) Beobachtung in eine Aufzeichnung übergeht und ihr Tun und Lassen damit staatlicherseits registriert wird. Diese Unsicherheit kann die Betroffenen in der freien Entfaltung ihrer Persönlichkeit hemmen.

---

[31] GVBl. I 2000, S. 179

[32] so auch die Entschließung der 59. Datenschutzkonferenz zu Risiken und Grenzen der Videoüberwachung, s. Dokumente 2000, A I

[33] LT-Drs. 15/154

Neben dieser grundsätzlichen Kritik haben wir uns im Gesetzgebungsverfahren aber auch dafür eingesetzt, dass die Voraussetzungen für die offene Videoüberwachung sog. Kriminalitätsschwerpunkte möglichst präzise und restriktiv formuliert werden. Dem hat der Gesetzgeber weitgehend Rechnung getragen, sodass die neu in das Polizeigesetz aufgenommene Vorschrift (§ 31 Abs. 3) im bundesweiten Vergleich zu den restriktivsten Befugnissen dieser Art zählt. Zu begrüßen ist insbesondere, dass schon die Landesregierung in ihrem Entwurf die Regelung zur Videoüberwachung auf sechs Jahre befristet hat. Der Landtag hat in einer Entschließung anlässlich der Verabschiedung des Gesetzes[34] eine Evaluation der Effekte der Videoüberwachung durch unabhängige Wissenschaftler gefordert. Damit würde erstmals in der Bundesrepublik die Frage beantwortet, ob durch Videoüberwachung die Sicherheit im öffentlichen Raum tatsächlich erhöht werden kann. Der Landtag hat die Landesregierung zudem aufgefordert, bereits vor Ablauf der Erprobungsphase einen jährlichen Bericht zur Prüfung der Normeffizienz an den Landtag zu geben. Es wird darauf ankommen, dass die mehrjährige Erprobungsphase für die offene Videoüberwachung in Brandenburg ergebnisoffen und rückholbar gestaltet wird, damit der Gesetzgeber ggf. diese Befugnis zu Eingriffen in die Grundrechte Unverdächtiger wieder rückgängig machen kann, wenn sie sich als ungeeignet erweist. Ferner hat der Landtag entsprechend einer Anregung des Landesbeauftragten klare und überprüfbare Regelungen zur technischen und organisatorischen Durchführung und Verarbeitung der personenbezogenen Daten wie z. B. eine rechnergestützte Protokollierung der Überwachungsmaßnahmen und eine Verschlüsselung digitaler Bildaufzeichnungen gefordert, um deren Beweiseignung vor Gericht zu sichern. Schließlich ist die Landesregierung um Prüfung gebeten worden, ob der strafrechtliche Schutz gegen die Zweckentfremdung und Weitergabe von Videoaufzeichnungen aus der polizeilichen Tätigkeit an Dritte durch das Datenschutzgesetz ausreichend gewährleistet ist und ob ergänzend das Kunsturhebergesetz über eine Bundesratsinitiative in der Weise geändert werden sollte, dass schon die unbefugte Bildaufzeichnung unter Strafe gestellt wird.

Der Gesetzgeber hat aber nicht nur die Videoüberwachung öffentlicher Plätze in Brandenburg eingeführt, sondern dies auch zum Anlass genommen, das Gesetz auf der Grundlage der 1999 ergangenen Entscheidung des Landesverfassungsgerichts[35] zu überarbeiten. Obwohl die Regelungen über den verdeckten Einsatz technischer Mittel zu Ton- und Bildaufzeichnungen einschließlich des "Großen Lauschangriffs" sowie über den Einsatz von V-Perso-

---

[34] LT-Drs. 3/2162

[35] Urt. v. 30.06.1999 - VfGBbg 3/98; s. Tätigkeitsbericht 1999, Pkt. A 4.1.2

nen im Wesentlichen verfassungskonform sind, hat das Landesverfassungsgericht ausgeführt, dass die Vorschriften des Brandenburgischen Polizeigesetzes insgesamt restriktiv auszulegen und die Befugnisse in engen Schranken, die sich am Grundgesetz und an der Brandenburgischen Verfassung orientieren, einzusetzen sind. Bei der jetzt erfolgten Novellierung sind alle Regelungen, bei denen durch verdeckte Datenerhebungsmaßnahmen selbst nicht tatverdächtige, zum Umfeld des Betroffenen gehörende Personen als Kontakt- oder Begleitpersonen erfasst werden, den Ausführungen des Gerichts entsprechend enger gefasst worden. Darüber hinaus wird klargestellt, dass durch die verdeckten Datenerhebungsmaßnahmen nicht in ein gesetzlich geschütztes Vertrauensverhältnis zwischen dem Betroffen und einem Amts- bzw. Berufsgeheimnisträger eingegriffen werden darf. Insgesamt hat das Brandenburgische Polizeigesetz dadurch an Rechtsklarheit gewonnen.

Ungeachtet der bundesweit zu beobachtenden Tendenz, die Befugnisse der Polizei bereits im Vorfeld der konkreten Gefahr einsetzen zu lassen und auch auf Nichtstörer zu erstrecken, ist die Befugnis zur Schleierfahndung etwas entschärft worden. Erst wenn ein entsprechendes Lagebild vorliegt, dürfen Identitätskontrollen aller sich im Grenzgebiet aufhaltenden Personen durchgeführt werden. Damit wird bei den von der Maßnahme Betroffenen zwar die Eingriffsschwelle nicht wieder auf das ursprüngliche Niveau der Störereigenschaft angehoben, aber im Unterschied zu verdachtslosen Identitätsfeststellungen ist die Befugnis jetzt immerhin an eine objektive Voraussetzung geknüpft.

Geändert wurden auch die allgemeinen Regelungen der Datenübermittlungen. Durch den Verweis auf die Vorschriften zur verdeckten Datenerhebung mit besonderen Mitteln, wie z. B. durch Observation oder den Einsatz technischer Mittel innerhalb und außerhalb von Wohnungen wird deutlicher als bisher, dass solche Daten nur an Polizeibehörden übermittelt werden dürfen. Diese Änderung ist im Hinblick auf die im vergangenen Berichtszeitraum beanstandete Übermittlung personenbezogener Daten von Kontakt- und Begleitpersonen an die Verfassungsschutzbehörde[36] zu begrüßen.

[36] s. Tätigkeitsbericht 1999, Pkt. A 4.1.4.6

Das geänderte Brandenburgische Polizeigesetz regelt die offene Videoüberwachung bestimmter öffentlich zugänglicher Straßen und Plätze mit grundrechtssichernden Verfahrensschritten. Die Wirkung dieser Befugnis muss durch die Landesregierung und unabhängige Wissenschaftler evaluiert werden, wobei auch das Recht auf prinzipiell unbeobachtete Bewegungsfreiheit unverdächtiger Bürgerinnen und Bürger zu berücksichtigen ist. Zu begrüßen sind die präziseren Regelungen zur Schleierfahndung und zur Datenübermittlung.

### 4.1.2 Prüfung der Datei "Gewaltprävention St" im Landeskriminalamt

*Der Abteilung Staatsschutz im Landeskriminalamt (LKA) steht für ihre Datenverarbeitung die Datei "Gewalttäter St" zur Verfügung. Die Datei erfüllt nicht nur die Funktion einer Personen-, Sachen- und Ereignisregistratur, sondern sie hält für einzelne Ermittlungsverfahren oder verfahrensübergreifende Komplexe weit darüber hinausgehende Recherche- und Analysemöglichkeiten bereit. Ein Segment dieser Datei wird von der Mobilen Einsatzgruppe gegen Ausländerfeindlichkeit (MEGA) genutzt, die dort seit 1998 die Datei "Gewaltprävention St" betreibt.*

Die Mobile Einsatzgruppe gegen Ausländerfeindlichkeit (MEGA) ist im Juni 1998 im Landeskriminalamt eingerichtet worden. Sie setzte sich aus einem Führungsstab, bestehend aus Beamten des LKA und 5 von den Polizeipräsidien abgeordneten Einsatzgruppen zusammen. Im Berichtszeitraum wurde die MEGA mit Erlass des Innenministers "disloziert". Die 5 Einsatzgruppen wurden wieder ihren jeweiligen Polizeipräsidien unterstellt und in den dortigen Dienstbetrieb eingegliedert. Im LKA selbst verblieb nur ein kleiner Führungsstab sowie - wenn auch in deutlich reduziertem Umfang - die Datei "Gewaltprävention St". Daneben betreibt jedes Polizeipräsidium unterdessen auch eine solche Datei für seine MEGA.

Die Datei "Gewaltprävention St" dient laut Dateibeschreibung der Verhütung und Aufklärung rechtsextremistisch und fremdenfeindlich motivierter Straftaten, indem sie die Auswertung und Sortierung von schriftlichen Meldungen aus den Polizeipräsidien sowie sonstiger Erkenntnisse und Informationen unterstützt. Mit Hilfe der Datei sollen die Mobilen Einsatzgruppen für den Deliktsbereich relevante Personen, Personengruppen, Institutionen, Objekte und Sachen sowie ihre Verbindungen untereinander erkennen und Erkenntnisse für ermittlungstaktisches Vorgehen sowie Deliktschwerpunkte gewinnen können. In die Datei eingestellt werden dürfen neben Informationen über Beschuldigte bzw. Störer, deren Kontakt- und Begleitpersonen, aber auch andere Personen wie Erziehungsberechtigte von Beschuldigten bzw. Störern bis hin zu

Fahrzeughaltern oder Grundstücks- und Wohnungseigentümern, wenn ihr Eigentum im Zusammenhang mit einem einschlägigen Delikt genutzt wird. Als Zeitraum für die in regelmäßigen Abständen vorzunehmende Prüfung, inwieweit die Daten für die polizeiliche Aufgabenerfüllung noch erforderlich sind, sieht die Dateibeschreibung für Beschuldigte bzw. Störer ein Jahr nach erstmaliger Speicherung und einen Monat bei allen anderen Personen vor. Die Speicherung in der Datei ist ein tiefgreifender Eingriff in die Persönlichkeitsrechte der Nichtbeschuldigten und Nichtstörer, der nur aufgrund der außerordentlich kurzen Prüffrist von einem Monat hingenommen werden konnte. Daten verarbeitende Stelle ist die jeweilige MEGA. Die Datenverarbeitung richtet sich ausschließlich nach den für die MEGA aufgestellten Grundsätzen. Bedingt durch die Umorganisation war das Datenaufkommen in der LKA-Datei zurückgegangen, sodass der Bestand auf unter 1000 von vorher ca. 3000 - 4000 Datensätze gesunken war.

Die überwiegende Mehrzahl der Datensätze besteht aus sog. "weichen Daten", d. h. der Sachverhalt ist nicht durch weitere Tatsachenfeststellungen belegt. Auch bei einer Datei, die fast ausschließlich zur Unterstützung präventiv-polizeilicher Aufgaben dient, ist dies nur hinnehmbar, wenn die Daten derjenigen Betroffenen, die im Zeitraum der einmonatigen Prüffrist nach der Erstspeicherung nicht wieder aufgefallen sind, gelöscht werden.

### 4.1.3 Prüfung der Datei "Gewalttäter Sport"

*Vor der Fußballeuropameisterschaft haben wir Eingaben von Fußballfans erhalten, die in Erfahrung bringen wollten, ob sie in der Datei "Gewalttäter Sport" erfasst sind. Wir stellten fest, dass die Annahme der meisten Betroffenen, in der Datei gespeichert zu sein, zutraf. Bei Petenten, deren Daten auf Veranlassung von Polizeidienststellen anderer Bundesländer registriert worden sind, konnte das Polizeipräsidium im Berichtszeitraum noch nicht abschließend prüfen, ob die Datenspeicherungen für die Aufgabenerfüllung der Polizei weiterhin erforderlich sind, weil trotz Nachfrage bei den zuständigen Staatsanwaltschaften der Ausgang des Ermittlungsverfahrens noch nicht mitgeteilt worden war.*

Die Datei "Gewalttäter Sport" (GWS) ist keine eigenständige Datei beim Bundeskriminalamt, sondern eine sog. Anlass-/Zweckkombination in der in allen Bundesländern und im Bundeskriminalamt (BKA) geführten Datei "Personenfahndung" des Informationssystems der Polizei (INPOL). Speicherberechtigt sind neben den sog. Bundesligabehörden (Polizeidienststellen, zu deren Einzugsbereich ein Bundesligafußballverein gehört), der Bundesgrenzschutz (BGS), die Zentralstelle Information Sport (ZIS) beim Landeskriminalamt Nordrhein-Westfalen und die Landesstelle Information Sport (LIS).

Abfrageberechtigt sind alle Polizei- und Bundesgrenzschutzdienststellen, die Zugriff auf die INPOL-Personenfahndung haben.

Bundesligabehörde ist das Polizeipräsidium Cottbus. Das für die polizeilichen Aufgaben im Zusammenhang mit Fußballspielen eingerichtete Sachgebiet ist zuständig für die Datenverarbeitung in der Anlass-/Zweckkombination "GWS" einschließlich der Akte "Sport". Es veranlasst über das LKA die Übermittlung der personenbezogenen Daten an das Bundeskriminalamt, das die Speicherung in der Personenfahndungsdatei vornimmt. Erfasst werden Personen, gegen die Ermittlungsverfahren wegen im Zusammenhang mit Sportveranstaltungen begangenen Straftaten, wie gefährliche Eingriffe in den Verkehr, Land- bzw. Hausfriedensbruch, Gewalttaten oder Verstöße gegen das Versammlungsgesetz, eingeleitet worden sind. Bis vor kurzem galt für die seit 1994 betriebene Anlass-/Zweckkombination "GWS" eine zweijährige Prüffrist, vor deren Ablauf das Bundeskriminalamt den zuständigen Bundesligabehörden über die Landeskriminalämter in Listenform diejenigen Datensätze meldet, die zur Löschung anstehen, weil der letzte relevante Eintrag zwei Jahre zurückliegt. Im Gegensatz zu anderen Dateien wird hier nach Ablauf der Zweijahresfrist automatisch gelöscht, wenn die zuständige Polizeidienststelle keine Weiterspeicherung veranlasst hat.

Bei noch nicht abgeschlossenen Ermittlungsverfahren wird die automatische Löschung stets unterbrochen. Diese Praxis ist problematisch, da nicht davon auszugehen ist, dass die Staatsanwaltschaften von sich aus der Polizei den Verfahrensausgang mitteilen. Das hat zur Folge, dass eine Vielzahl von Betroffenen immer noch mit dem Hinweis "GWS" in der INPOL-Personenfahndungsdatei registriert ist, obwohl das die Speicherung auslösende Ermittlungsverfahren von der Staatsanwaltschaft wegen des Fehlens ausreichender Anhaltspunkte für die Begehung einer Straftat nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt worden ist.

Bei der Prüfung haben wir festgestellt, dass bei der Entscheidung, ob ein Datensatz weiterhin für die Aufgabenerfüllung erforderlich ist, vor allem auf den eigenen Erkenntnisstand zurückgegriffen und nicht bei der Staatsanwaltschaft nach dem Stand des Ermittlungsverfahrens gefragt wird. Entscheidend ist die Einschätzung, dass der Betroffene bei sportlichen Veranstaltungen weiterhin "gewalttätig" auftreten wird.

Dies ist datenschutzrechtlich bedenklich. Immerhin hat die Staatsanwaltschaft bei einer Einstellung des Ermittlungsverfahrens festgestellt, dass der Anfangsverdacht durch die Ermittlungen nicht bestätigt worden ist und daher kein Gerichtsverfahren gegen den Betroffenen eingeleitet werden kann.

Die Akte "Sport" enthielt neben den Ausschreibungsformularen, mit denen die personenbezogenen Daten der Betroffenen an das Bundeskriminalamt gemeldet werden, um die Ausschreibung mit GWS in der INPOL-Personenfahndungsdatei zu veranlassen, eine Vielzahl weiterer Meldungen, darunter auch solche ohne Bezug zu Fußball- und Sportveranstaltungen.

Das Polizeipräsidium wird stets informiert, wenn gegen einen mit GWS Ausgeschriebenen ein Ermittlungsverfahren eingeleitet wird, unabhängig davon, ob es sich um ein Delikt aus dem Straftatenkatalog der Errichtungsanordnung "Gewalttäter Sport" handelt oder sonst überhaupt ein Zusammenhang mit einem Sportereignis besteht. Gemeldet wird des Weiteren durch den Bundesgrenzschutz jeder Grenzübertritt der Ausgeschriebenen. Aufgrund dieses durch die Ausschreibung ausgelösten Meldeverfahrens finden sich in der Akte zu den einzelnen Betroffenen eine Vielzahl von Daten, die zur Aufgabenerfüllung des Sachgebiets nicht erforderlich sind. Dieser Datenbestand wird nicht gepflegt, sodass die Meldungen über die den Betroffenen zur Last gelegten Tatvorwürfe in vielen Fällen unrichtig sein dürften. Vernichtet wird der gesamte Bestand erst nach der Ausschreibungslöschung in der INPOL-Personenfahndung.

Wir haben das Polizeipräsidium aufgefordert, diese Meldungen nach Eingangsdatum sortiert in einer gesonderten Akte abzulegen und jeweils nach Jahresfrist zu vernichten.

Das Ergebnis der staatsanwaltschaftlichen Prüfung muss bei der Entscheidung der Polizei über die weitere Datenverarbeitung berücksichtigt werden. Eine Speicherung personenbezogener Daten ist, wenn das staatsanwaltschaftliche Ermittlungsverfahren gegen den Betroffenen eingestellt wurde, nur in Ausnahmefällen zulässig.

### 4.1.4 Errichtungsanordnung "Gewalttäter Sport"

*Im Berichtszeitraum ist uns der Entwurf zur Änderung der Errichtungsanordnung "Gewalttäter Sport" zur Stellungnahme zugegangen.*

Gegen die vorgesehene Verlängerung der Speicherungsfrist von zwei auf vier (bei Kindern) bzw. fünf Jahre (bei Erwachsenen) haben wir angeführt, dass mit einer so langen Prüffrist gegen das Verhältnismäßigkeitsprinzip verstoßen wird. Zwar erfolgt in Brandenburg keine Erfassung von personenbezogenen Daten mit dem Hinweis "GWS" nur aufgrund von Personalienfeststellungen, Platzverweisen und Ingewahrsamnahmen. Dennoch reicht auch hier lediglich die Einleitung eines Ermittlungsverfahrens als Speicherungsvoraussetzung aus. Diese niedrige Voraussetzungsschwelle steht in keinem Verhältnis zu

der fünfjährigen Aussonderungsprüffrist. Dabei ist auch zu berücksichtigen, dass die Registrierung Eingriffe in das Grundrecht auf Bewegungsfreiheit der Betroffenen nach sich ziehen kann.

Das Bundesinnenministerium hat die Verlängerung der Prüffrist damit begründet, dass die einschlägigen Sportveranstaltungen in einem vierjährigen Rhythmus ablaufen und daher die längere Prüffrist benötigt werde, um Informationsverluste zu vermeiden.

Dieses Argument basiert jedoch auf der unrichtigen Annahme, dass Aussonderungsprüffristen mit Löschungsfristen gleichzusetzen wären und die Daten daher bei Fristablauf zu löschen seien. Mit der Aussonderungsprüffrist wird nur ein Zeitpunkt für eine Erforderlichkeitsprüfung festgelegt. Ausschlaggebend sollten nur dateiimmanente Gesichtspunkte sein. Da in der Regel erst unmittelbar vor Fristablauf zum ersten Mal geprüft wird, ob die Speicherung zur weiteren Aufgabenerfüllung noch erforderlich ist, ist die fünfjährige Aussonderungsprüffrist vor allem in den Fällen unverhältnismäßig lang, in denen das Ermittlungsverfahren von der Staatsanwaltschaft bereits im ersten Jahr des Fristenlaufs wegen fehlenden Vorliegens ausreichender Anhaltspunkte für eine Straftat eingestellt worden ist. Und sie führt insbesondere dann zu einer unzulässig langen Aufbewahrungsdauer, wenn nach Ablauf der Aussonderungsprüffrist nicht bei der Staatsanwaltschaft der Ausgang des Ermittlungsverfahrens in den Fällen erfragt wird, in denen diese den Verfahrensausgang nicht mitgeteilt hat und ohne ausreichende Prüfung die weitere Erforderlichkeit festgestellt wird.

Die verlängerte Prüffrist hat zur Folge, dass viele Betroffene zehn Jahre lang (Erwachsene und Jugendliche) bzw. vier Jahre lang (Kinder) mit dem Hinweis "GWS" registriert sind. Bei einer fünfjährigen Aussonderungsprüffrist muss die Erforderlichkeit nur einmal während der zehnjährigen Höchstspeicherungsfrist geprüft werden, gegenüber fünfmal bei einer Prüffrist von zwei Jahren. Es ist davon auszugehen, dass häufigere Erforderlichkeitsprüfungen zur Löschung eines Datensatzes vor Ablauf der Höchstspeicherfrist führen würden.

### 4.1.5 Mitteilungs- und Folgepflichten bei Staatsanwaltschaft und Polizei

*Erneut muss über die Mitteilungspflicht der Staatsanwaltschaft über den Verfahrensausgang des staatsanwaltschaftlichen Ermittlungsverfahrens und über die dem Verfahrensausgang folgenden Pflichten der Polizei berichtet werden. Es ist jedoch zu hoffen, dass das Problem alsbald gelöst wird, weil in diesem Jahr das bei den Staatsanwaltschaften*

*betriebene Automationsverfahren MESTA Schnittstellen enthält, über die die Polizei den Stand des Ermittlungsverfahrens jederzeit online abfragen kann. In der Dateibeschreibung zu der beim Landeskriminalamt betriebenen Datei "Gesellschaftsrechtliche Beziehungen/Wirtschafts-kriminalität (GereB/Wikri)" ist unter der Überschrift "Aufbewahrungsfristen" zum Thema ausgeführt, dass die Löschung der Daten spätestens zum Zeitpunkt der Mitteilung des Ausgangs des Strafverfahrens durch die Staatsanwaltschaft gem. Nr. 11 Anordnung über Mitteilungen in Strafsachen vom 29. April 1998 (MiStra) - hier Mitteilungspflicht der Staatsanwaltschaft gegenüber der Polizei - erfolgt.*

Dies entspricht nicht der Vorschrift des § 47 Abs. 2 Nr. 3 Brandenburgisches Polizeigesetz (BbgPolG), in der festgelegt ist, dass die Daten zu löschen sind, wenn bei der zu bestimmten Terminen vorzunehmenden Prüfung festgestellt wird, dass sie für die polizeiliche Aufgabenerfüllung nicht mehr erforderlich sind.
Erfahrungsgemäß kommen die Staatsanwaltschaften ihrer Verpflichtung nur selten nach, der Polizei unaufgefordert den Verfahrensausgang mitzuteilen. Daher kann die Polizei die Löschung nicht ausschließlich von der Mitteilung der Staatsanwaltschaft über den Verfahrensausgang abhängig machen, weil sie sich so ihrer Verantwortung für die Korrektheit der Datenspeicherung als die Daten verarbeitende Stelle entziehen würde. Als solche ist die Polizei vielmehr verpflichtet, den Verfahrensausgang im Rahmen der nach Ablauf der Prüffrist vorzunehmenden Erforderlichkeitsprüfung von sich aus bei der Staatsanwaltschaft nachzufragen.

Es ist dem Polizeigesetz nicht zu entnehmen, dass die Feststellung der Erforderlichkeit für eine weitere Aufbewahrung der Daten immer dann unterbleiben kann, wenn die Staatsanwaltschaft ihren gesetzlichen Verpflichtungen nicht nachgekommen ist. Die Polizei wird ihrer Pflicht als Daten verarbeitende Stelle nicht enthoben, weil eine andere Stelle ihren Pflichten nicht nachgekommen ist.

## 4.2 Verfassungsschutz

### Neuer Entwurf eines Sicherheitsüberprüfungsgesetzes

*Bei der Erarbeitung eines neuen Entwurfs eines Gesetzes zur Regelung von Sicherheitsüberprüfungen (Brandenburgisches Sicherheitsüberprüfungsgesetz - BbgSÜG) wurden wir so frühzeitig mit einbezogen, dass in einem Gespräch mit der zuständigen Abteilung des Innenministeriums einige unserer datenschutzrechtlichen Einwände noch vor der Verabschiedung des Entwurfs im Kabinett ausgeräumt werden konnten. Allerdings ist dann der Zeitpunkt der Übersendung des Entwurfs an das*

*Kabinett vorgezogen worden, sodass unsere Kritikpunkte an einer Reihe von Regelungen in der Kabinettsvorlage doch nicht mehr berücksichtigt wurden.*

An einer Sicherheitsüberprüfung ist nicht nur die Stelle beteiligt, die jemanden mit einer sicherheitsempfindlichen Tätigkeit betrauen möchte, sondern auch die Brandenburgische Verfassungsschutzbehörde. Veranlasst wird die Sicherheitsüberprüfung, durch die Stelle, bei der die sicherheitsempfindliche Tätigkeit auszuführen ist. Sie trägt die Verantwortung für die Betrauung oder ggf. Ablehnung der zu überprüfenden Person. Im Gesetzentwurf ist sie als zuständige Stelle bezeichnet. Die Aufgaben der zuständigen Stelle werden von einem dort zu bestellenden Geheimschutzbeauftragten wahrgenommen, der dazu auch die im Gesetz geregelten Befugnisse der zuständigen Stelle hat. Dies sollte der Entwurf klarer stellen.

Die Verfassungsschutzbehörde erhebt die für die Überprüfung erforderlichen Informationen über die zu überprüfende Person und ihr Umfeld. Sie bewertet auch die gesammelten Erkenntnisse über den Betroffenen und stellt fest, ob ein Sicherheitsrisiko vorliegt. Die als Ergebnis der Sicherheitsüberprüfung zu treffende Entscheidung, ob der überprüften Person die sicherheitsempfindliche Tätigkeit übertragen wird, fällt jedoch nicht in ihren Verantwortungsbereich. Sie wirkt bei Sicherheitsüberprüfungen nur mit und wird daher im Gesetz als mitwirkende Stelle bezeichnet.

Sicherheitsüberprüfungen sind ein tiefer Eingriff in die Persönlichkeitsrechte der überprüften Personen. Sie müssen ihre berufliche und private Vergangenheit einschließlich ihrer Beziehungen zu anderen Personen offenlegen. Auch wenn Sicherheitsüberprüfungen hinzunehmen sind, weil bestimmte Tätigkeiten im Interesse der Allgemeinheit nur von solchen Personen ausgeübt werden sollten, die ein hohes Maß an Sicherheit gewährleisten, kann niemand dazu gezwungen werden, die Teilnahme ist freiwillig. Derjenige, der entscheiden soll, ob er die Prozedur auf sich nehmen will, muss vorher wissen, auf was er sich dabei einlässt. Die Ausübung der Entscheidungsfreiheit setzt eine umfassende Unterrichtung voraus.

Die Regelungen des Entwurfs über die Rechte und Pflichten der zu überprüfenden und einzubeziehenden Personen tragen dem ausreichend Rechnung. Die zuständige Stelle ist vor der Durchführung einer Sicherheitsüberprüfung verpflichtet, die zu überprüfende Person über die Überprüfung als solche sowie die dazu erforderlichen Datenverarbeitungsmaßnahmen umfassend zu unterrichten. Weiterhin ist klargestellt, dass eine Sicherheitsüberprüfung nur mit Zustimmung des Betroffenen erfolgen kann.

Sowohl die zuständige als auch die mitwirkenden Stellen sind befugt, ohne Wissen des Betroffenen andere geeignete Personen oder Stellen zu befragen, wenn die Datenerhebung bei der zu überprüfenden Person nicht ausreicht. Damit wird das Prinzip der Sicherheitsüberprüfung durchbrochen, demgemäß die zu überprüfende Person in allen Phasen Herrin des Verfahrens sein soll, das ohne ihre Einwilligung nicht durchgeführt werden kann und die daher vor anderen zu befragen ist.

Auch wenn es nicht von der Hand zu weisen ist, dass sich bei der Durchführung einer Sicherheitsüberprüfung im Einzelfall Sachverhalte ergeben können, die eine Befragung Dritter ohne Wissen der zu überprüfenden Person erforderlich erscheinen lassen, bleibt doch fraglich, ob beide Sicherheit überprüfenden Stellen die Befugnis zur Befragung Dritter ohne Wissen des Betroffenen erhalten müssen. Wir sind der Auffassung, dass es ausreichend wäre, wenn nur die mitwirkende Stelle verdeckte Datenerhebungsmaßnahmen durchführen darf, da sie von vornherein weitergehendere Datenerhebungsbefugnisse, wie z. B. die Befragung von Referenzpersonen hat, als die zuständige Stelle. Es steht daher zu erwarten, dass die mitwirkende Stelle dadurch Sachverhalte ohne darüber hinausgehende Befragungen anderer Personen, d. h. ohne weitere Grundrechtseingriffe klären kann.

Ungeachtet der Frage der Befugniszuweisung sind die Voraussetzungen, unter der die zuständige Stelle vom Grundsatz der Datenerhebung beim Betroffenen abweichen kann, nicht normenklar. Hier sollte zumindest auf die Angaben über nahestehende Personen, frühere Wohnsitze, Berufsausbildung und -ausübung in der Sicherheitserklärung, die die zu überprüfende Person abgeben muss und die Tatsache, dass ihre Angaben im Einzelfall durch die Befragung anderer Personen verifiziert werden können, verwiesen werden.

Das Akteneinsichtsrecht der Überprüften in die anlässlich der Sicherheitsüberprüfung bei der zuständigen und bei der mitwirkenden Stelle angelegten Sicherheits- und Sicherheitsüberprüfungsakte ist in dem Entwurf zu eng geregelt. Nach der Brandenburgischen Verfassung hat jeder ein Recht auf Einsicht in Akten und sonstige amtliche Unterlagen, soweit sie ihn betreffen, und Rechte Dritter nicht entgegenstehen. Hier ist die Gewährung der Akteneinsicht an die Voraussetzung geknüpft, dass der Antragsteller ein rechtliches Interesse an der Akteneinsicht darlegt.

Mit der Brandenburgischen Verfassung wäre eine Einsichtsverweigerung nur vereinbar, wenn dadurch die öffentliche Sicherheit oder das Wohl des Bundes oder eines Bundeslandes gefährdet, die berechtigten Interessen Dritter verletzt sowie in Ausnahmefällen die Aufgabenerfüllung der zuständigen oder der mitwirkenden Stelle gefährdet würde. Das Grundrecht des Einzelnen auf Zugang zu den Unterlagen, die ihn betreffen, muss sich auch im Brandenburgischen Sicherheitsüberprüfungsgesetz widerspiegeln.

## 4.3 Ausländer

### Zweierlei Maß im Schengener Informationssystem und im Informationssystem der Polizei

*Mehrere im europäischen Ausland lebende Staatsangehörige aus Drittländern (Nichtmitglieder der Europäischen Union) wollten in Erfahrung bringen, ob sie im Schengener Informationssystem (SIS) und im deutschen Informationssystem der Polizei (INPOL) registriert sind. Diese Personen waren in der Vergangenheit nach Brandenburg eingereist und, nachdem ihnen hier ein Aufenthaltsrecht verweigert worden war, in einen anderen Mitgliedsstaat der Europäischen Union gezogen. Die Ausschreibung im SIS und INPOL hat zur Folge, dass der Betroffene bei jeder Personalienkontrolle innerhalb "Schengenlands" (europäische Staaten, die dem Schengener Durchführungsabkommen - SDÜ - beigetreten sind) oder beim Passieren der Außengrenzen mit einer Festnahme bis zur Klärung des Sachverhalts rechnen muss.*

Ausländer, die keine Aufenthaltsgenehmigung erhalten, werden von den Ausländerbehörden zur Ausreise aufgefordert und nach Ablauf der festgesetzten Ausreisefrist zur Einreiseverweigerung im SIS und INPOL ausgeschrieben. Bei Personen, die ausgewiesen werden können, deren Aufenthalt aber unbekannt ist oder die bereits ausgereist sind, sowie bei Abgeschobenen wird ebenso verfahren.

Rechtsgrundlage für die Ausschreibung ist Artikel 96 Schengener Durchführungsübereinkommen (SDÜ), demgemäß die Mitgliedstaaten die personenbezogenen Daten von Drittausländern zur Einreiseverweigerung im SIS speichern dürfen. In Artikel 102 SDÜ ist festgelegt, dass die ausschreibende Behörde nach drei Jahren prüfen muss, ob es weiterhin erforderlich ist, den Betroffenen die Wiedereinreise im Schengen-Raum zu verweigern und die Daten daher nicht gelöscht werden können. Die Speicherungsfrist kann dann um weitere drei Jahre verlängert werden. Wenn den Betroffenen in einem anderen Schengenmitgliedsstaat der Aufenthalt gestattet wird, muss die ausschreibende Ausländerbehörde die Löschung des Datensatzes im SIS veranlassen, weil der Ausschreibungsgrund entfallen ist.

Davon erfährt die Behörde aber meist nur, wenn der Betroffene Löschung verlangt, weil im Schengen-Verbund kein Rückmeldeverfahren vorgesehen ist. Eine Weiterspeicherung aus anderen Gründen, z. B. weil der Betroffene die durch die Ausschreibung entstandenen Kosten noch nicht beglichen hat, ist unzulässig. Dies gilt jedoch nicht für die Speicherung in dem INPOL-Fahndungssystem. In Brandenburg ist die Zentrale Ausländerbehörde in Eisenhüttenstadt für die Ausschreibungen zuständig. Das Landeskriminalamt nimmt die Datenverarbeitung in den beiden Fahndungssystemen vor.

Aufgrund unserer Intervention hat die Zentrale Ausländerbehörde in allen Fällen die Ausschreibung der Petenten im SIS löschen lassen. Die Löschung in der INPOL-Personenfahndung ist nicht immer erfolgt.

Wenn einem Drittausländer der Aufenthalt in einem Mitgliedsland des Schengener Durchführungsabkommens gestattet wird, entfällt in der Regel der Ausschreibungsgrund nach Artikel 96 SDÜ mit der Folge, dass der Datensatz des Betroffenen im SIS zu löschen ist. Auf die Speicherung im INPOL-Personenfahndungssystem hat die Aufenthaltsgenehmigung in einem anderen Schengenstaat keine Auswirkungen, sodass diese Ausschreibung bestehen bleiben kann.

## 4.4 Meldewesen

### 4.4.1 Privatanschriften für alle - das Melderegister im Internet

*Noch bevor der Bundesgesetzgeber das Zweite Gesetz zur Änderung des Melderechtsrahmengesetzes (MRRG) verabschiedet hat, hat sich eine Arbeitsgruppe von Bund und Ländern unter Federführung des Bundesministeriums des Innern mit einem Dritten Änderungsgesetz des MRRG befasst. Das Melderecht soll den modernen Informations- und Kommunikationstechniken angepasst werden. Dazu lagen uns erste Entwürfe des Bundesministeriums des Innern vor, die auch aus Sicht des Datenschutzes bedeutsame Änderungen des Melderechts erwarten lassen.*

So bestand zunächst die Absicht, das Melderegister hinsichtlich bestimmter Daten wie Name, Vorname, Anschrift und akademischen Grad zu einem öffentlich zugänglichen Register zu machen. Dabei sollte auch für jedermann der elektronische Abruf - etwa über das Internet - dieser Daten möglich sein. Dies stößt auf erhebliche datenschutzrechtliche Einwände.

Wir haben grundsätzlich keine Bedenken, den elektronischen Abruf von Daten aus dem Melderegister zuzulassen. Allerdings dürfen solche Abrufe

auch in Zukunft nur nach den gleichen rechtlichen Voraussetzungen möglich sein wie bisher. Dies setzt zunächst voraus, das der Abrufende die gesuchte Person eindeutig identifizieren kann. Deshalb muss bei solchen Abrufen technisch sichergestellt werden, dass der elektronische Abruf nur unter Verwendung gesetzlich vorgeschriebener Suchmerkmale möglich ist, die zu einer eindeutigen Identifizierung des gesuchten Einwohners führen.

Es muss gewährleistet sein, dass auch bei einem elektronischen Abruf die schutzwürdigen Interessen des von der Suche betroffenen Einwohners berücksichtigt werden und eine Melderegisterauskunft unterbleibt. Bei einem elektronischen Abrufverfahren kann die Meldebehörde den Einzelfall nicht mehr prüfen, da sie einen Abruf überhaupt nicht bemerkt.

Zwischenzeitlich hat das Bundesinnenministerium in einem neueren Entwurf die Kritik der Datenschutzbeauftragten teilweise aufgegriffen und bezeichnet das Melderegister nicht mehr als "öffentlich". Nach wie vor sollen aber Auskünfte auch in einem noch nicht näher beschriebenen elektronischen Verfahren möglich sein.

Im Übrigen begrüßen wir, dass sowohl den Meldebehörden als auch den Bürgerinnen und Bürgern der Umgang mit dem Melderegister auch auf elektronischem Wege ermöglicht werden soll. So ist geplant, dass Änderungen des Wohnsitzes auch online erfolgen können. Voraussetzung hierfür ist allerdings die praktische Nutzung digitaler Signaturen, wofür die rechtlichen Voraussetzungen in Deutschland gegenwärtig geschaffen werden[37].

Der uns vorliegende Entwurf enthält schließlich noch weitere Vorschriften, die aus datenschutzrechtlicher Sicht ausdrücklich zu begrüßen sind. So sollen die Informationsrechte der betroffenen Einwohner gegenüber der Meldebehörde erweitert werden. Darüber hinaus ist geplant, dass man sich bei Umzügen im Inland nicht mehr bei der Meldebehörde am früheren Wohnsitz abmelden muss. Dies ist bisher nur bei Umzügen innerhalb des Landes Brandenburg möglich. Wegfallen soll auch die Hotelmeldepflicht für Deutsche bei einem Aufenthalt von weniger als drei Monaten.

Weiterhin sollen Melderegisterauskünfte an Parteien anlässlich von Wahlen und Plebisziten nur noch dann möglich sein, wenn die Einwohner ausdrücklich in diese Auskunft einwilligen. Damit würde eine schon seit langem bestehende Forderung der Datenschutzbeauftragten umgesetzt, das Melderegister nicht ohne Mitwirkung der Bürgerinnen und Bürger für

[37] s. Pkt. A 1.1

politische Zwecke zu nutzen[38].

Das Melderegister ist kein öffentliches Register. Abrufe von Meldedaten über das Internet sollten nur nach den gleichen Voraussetzungen möglich sein wie bisher schon. Es ist zu begrüßen, dass zukünftig Melderegisterauskünfte an Parteien nur noch mit Einwilligung der Betroffenen erfolgen sollen.

### 4.4.2 Zugriffe auf das Melderegister innerhalb von Gemeinden, Ämtern und kreisfreien Städten

*Im Berichtszeitraum haben wir in einer amtsfreien Gemeinde geprüft, unter welchen Voraussetzungen gemeinde-intern durch einzelne Ämter auf das Melderegister zugegriffen werden darf[39].*

In der von uns überprüften Gemeinde standen für den Zugriff auf das Melderegister mehrere Abfrageplätze zur Verfügung. Einige davon waren im Einwohnermeldeamt selbst untergebracht, die übrigen verteilten sich auf andere Ämter, wie z. B. das Steueramt. Der Umfang der Zugriffsrechte war nach Amt und Zweck differenziert. Nur das Einwohnermeldeamt verfügt über Schreib- und Änderungsrechte.

Die übrigen Ämter verfügen entsprechend ihrer Aufgaben nur über reduzierte Rechte. Alle Daten mit Auskunftssperren nach § 32 a Brandenburgisches Meldegesetz (BbgMeldeG) waren vom Zugriff ausgenommen.

---

[38] vgl. Tätigkeitsbericht 1998, Pkt. A 4.3

[39] *s. Tätigkeitsbericht 1999, Pkt. A 4.3.2*

Die in dieser Gemeinde vorgefundene Verteilung der internen Zugriffe auf das Melderegister halten wir aus datenschutzrechtlicher Sicht für akzeptabel. Wie bereits in unserem letzten Tätigkeitsbericht ausgeführt[40], halten wir es grundsätzlich für erforderlich, dass auch beim automatisierten Abruf von Daten aus dem Melderegister die interne Weitergabe der Datenübermittlung gleichgestellt wird. Dies hat zur Folge, dass dafür die Vorschrift des § 29 BbgMeldeG entsprechend angewendet werden müsste, die den automatisierten Abruf aus dem Melderegister vom Vorhandensein einer Rechtsvorschrift abhängig macht.

Die oben beschriebene Lösung ist dann datenschutzgerecht, wenn durch geeignete technische und organisatorische Maßnahmen sichergestellt wird, dass die Abrufe auf das im Einzelfall erforderliche Maß beschränkt werden. In technischer Hinsicht kann dies durch eine restriktive Vergabe von Zugriffsrechten in ausreichender Weise gewährleistet werden. In organisatorischer Hinsicht halten wir es für erforderlich, dass die jeweilige Gemeinde in einer Dienstanweisung festlegt, dass Zugriffe auf das Melderegister durch Ämter außerhalb des Einwohnermeldeamtes nur dann zulässig sind, wenn es im Einzelfall erforderlich ist, um z. B. die Anschrift einer Person zu erfahren.

Dessen ungeachtet sollten aber auch eindeutige Rechtsgrundlagen geschaffen werden.

Gemeindeinterne Zugriffe auf das Melderegister durch Fachämter außerhalb des Einwohnermeldeamtes sind aus datenschutzrechtlicher Sicht dann akzeptabel, wenn durch technische und organisatorische Maßnahmen sichergestellt werden kann, dass das Erforderlichkeitsprinzip beachtet wird. Der Gesetzgeber sollte eine ausdrückliche Regelung zur Zulässigkeit solcher Zugriffe im Brandenburgischen Meldegesetz treffen.

## 4.5 Personaldaten

### 4.5.1 Besserer Datenschutz für Arbeitnehmer - eine unendliche Geschichte?

[40] s. Tätigkeitsbericht 1999, Pkt. A 4.3.2

*Seit vielen Jahren weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass entsprechend den Forderungen des Bundesverfassungsgerichts endlich eine bereichsspezifische Regelung zum Datenschutz im Arbeitsverhältnis geschaffen werden muss[41]. Die seit 1998 regierenden Koalitionsparteien auf Bundesebene haben vereinbart, noch in der laufenden Legislaturperiode ein neues Arbeitnehmerdatenschutzgesetz zu schaffen. Wie der Presse zu entnehmen war, hat das Bundesministerium für Arbeit und Sozialordnung ein Eckpunktepapier für ein neues Arbeitnehmerdatenschutzgesetz vorgelegt.*

Wir halten es weiterhin dringend für erforderlich, dass angesichts der Vielzahl von speziellen datenschutzrechtlichen Fragen im Verhältnis zwischen Arbeitgebern und Arbeitnehmern ein spezielles Gesetz für den Arbeitnehmerdatenschutz geschaffen wird.

Aus den Plänen des Bundesministeriums für Arbeit und Sozialordnung ergeben sich eine Reihe von positiven Ansätzen, wie:

- Einhaltung der Zweckbindung,
- Beachtung der Grundsätze von Datensparsamkeit und Datenvermeidung,
- Sicherstellung der Richtigkeit und Aktualität gespeicherter Daten,
- Verbot der Diskriminierung,
- Verpflichtung auf das Datengeheimnis und
- Gewährleistung der Datensicherheit.

Personenbezogene Daten dürfen nur noch dann verarbeitet werden, wenn sie für Zwecke des konkreten Arbeitsverhältnisses erforderlich sind, Fragen nach Partei- oder Gewerkschaftszugehörigkeit sind nicht zulässig. Mit dem Datengeheimnis ist es nicht vereinbar, wenn beispielsweise ein Laptop auf einer Dienstreise mit der Möglichkeit einer Kenntnisnahme von Personaldaten durch Dritte benutzt wird. Die Datensicherheit gebietet es, Arbeitnehmerdaten nicht unverschlüsselt über das Internet zu übertragen.

Auch der Umgang mit Daten aus dem Bewerbungsverfahren und dem eigentlichen Arbeitsverhältnis wird geregelt. So soll z. B. eine Genomanalyse im Einstellungsverfahren auch dann unzulässig sein, wenn die Einwilligung des Bewerbers vorliegt, da ein zu rechtfertigendes Interesse des Arbeitgebers an den Ergebnissen einer solchen Untersuchung nicht vorhanden sei.

Der Presse war zu entnehmen, dass ein Referentenentwurf möglicherweise

---

[41] *s. 5. Tätigkeitsbericht, Pkt. 13.1.1 und 6. Tätigkeitsbericht, Pkt. 13.1*

auch Regelungen zur privaten Nutzung von Internet und E-Mail beinhalten werde. Nach dem Willen des Bundesministers für Arbeit und Sozialordnung sollen die Arbeitnehmer grundsätzlich das Recht bekommen, privat am Arbeitsplatz im Internet zu surfen und E-Mails zu versenden. Dies soll jedenfalls so lange gelten, wie betriebliche Belange nicht beeinträchtigt werden. Eine Inhalts-kontrolle durch den Arbeitgeber darf in diesen Fällen selbstverständlich nicht stattfinden.

Besonders hervorzuheben ist die geplante Stärkung der Arbeitnehmer-position durch Benachrichtigungspflichten des Arbeitgebers, Auskunfts- und Akteneinsichtsrechte des Arbeitnehmers, Korrekturrechte des Arbeitnehmers und nicht zuletzt Schadensersatzansprüche bei unrechtmäßiger Datenverarbeitung durch den Arbeitgeber.

Schließlich enthält das geplante Arbeitnehmerdatenschutzgesetz auch Vor-schriften zum organisatorischen Datenschutz. Dies betrifft vor allem die Rechtsstellung und Kontrolle durch betriebliche Datenschutzbeauftragte, deren Zusammenarbeit mit dem Arbeitgeber und der Personalvertretung, aber auch Regelungen zu den Aufgaben von Aufsichtsbehörden und Sanktionen bei Rechtsverstößen.

Die rasante Entwicklung der Informations- und Kommunikationstechnologie macht normenklare Regelungen auf dem Gebiet der Arbeitnehmerdatenschutzrechte erforderlich.

### 4.5.2 Gehaltslisten an Privatunternehmen

*Die Gemeindevertretung einer amtsangehörigen Gemeinde plant die Privatisierung des gemeindlichen Bauhofes, um Kosten zu sparen. Im Auftrag der Gemeindevertretung fand deshalb im Amt ein Gespräch über die Privatisierung des Bauhofes mit dem Geschäftsführer eines privaten Unternehmens statt, das an der Übernahme des Bauhofes interessiert war. Das private Unternehmen, eine GmbH, hatte sich bereit erklärt, ein Grobkonzept zur Übernahme des Bauhofes mit verschiedenen Lösungs-ansätzen vorzubereiten. Im Rahmen der mit dem Amt vereinbarten Zu-arbeit wurde der GmbH u. A. eine Liste der Beschäftigten des Bauhofes zur Verfügung gestellt. Diese Liste enthielt zwar keine Namen, wohl aber das genaue Eintrittsdatum, den erlernten Beruf, das Lebensalter, die monatliche Vergütung, das Urlaubs- und Weihnachtsgeld, die Führer-scheinklasse sowie Angaben zu etwaigen Behinderungen. Das Amt hat die GmbH gebeten, diese Angaben vertraulich zu behandeln und nur für das zu erstellende Konzept zu verwenden.*

Bei der Übergabe der Liste der Mitarbeiter des Bauhofes an die GmbH

handelt es sich um eine Übermittlung personenbezogener Personaldaten. Auch wenn die Namen der Beschäftigten nicht genannt worden sind, kann nicht von einer Anonymisierung i. S. v. § 3 Abs. 3 Nr. 1 BbgDSG ausgegangen werden. Danach sind Daten erst dann anonym, wenn die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die geringe Zahl der Beschäftigten des Bauhofes sowie die sehr detaillierten Angaben zu Berufsabschluss, Alter, Vergütung usw. bringen es mit sich, dass der Personenbezug ohne Weiteres mit wenig Zusatzwissen hergestellt werden kann. Deshalb handelt es sich um personenbezogene Daten.

Da die GmbH eine Stelle außerhalb des öffentlichen Bereichs ist, ist eine Übermittlung von Personaldaten der Beschäftigten des Bauhofes nur unter den Voraussetzungen des § 29 Abs. 1 Satz 2 BbgDSG möglich. Diese Vorschrift lässt eine solche Übermittlung dann zu, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder die Betroffenen eingewilligt haben.

Im vorliegenden Fall lag keine der genannten Voraussetzungen vor. Selbstverständlich hat die GmbH als mögliche Übernehmerin des Bauhofes ein erhebliches Interesse, die mit dem Betrieb des Bauhofes zusammenhängenden Kosten zu erfahren. Dazu gehören auch und in erster Linie die Personalkosten. Zu dem Zeitpunkt der Übergabe der Liste stand jedoch offensichtlich noch nicht fest, ob die GmbH tatsächlich den Bauhof übernehmen würde. Vielmehr sollte erst ein Grobkonzept erarbeitet werden, auf dessen Grundlage sich die GmbH und die Gemeinde entscheiden wollten. Für diesen Zweck wäre es völlig ausreichend gewesen, die wesentlichen Grundzüge der Personalstruktur darzustellen, sowie die bisher durch die Gemeinde gezahlten Personalkosten zusammengefasst aufzuführen. In keinem Fall war es zu diesem Zeitpunkt erforderlich, weitere Personaldaten wie Alter, Beschäftigungszeitraum, Beruf, Führerschein und etwaige Behinderungen in die Liste aufzunehmen. Mit anderen Worten hätte es ausgereicht, nur Daten ohne Personenbezug zu übermitteln. Insofern bestand aus Sicht der GmbH weder ein rechtliches Interesse an der Kenntnis der Personaldaten noch hat der Dienstverkehr dies erfordert. Das rechtliche Interesse kann auch nicht dadurch hergestellt werden, dass sich die Gemeinde etwa zur Übermittlung der Listen in dieser Form möglicherweise vertraglich verpflichtet hat. Das rechtliche Interesse i. S. v. § 29 Abs. 1 Satz 2 BbgDSG hängt nicht allein vom Willen der beteiligten Stellen ab. Vielmehr muss die übermittelnde öffentliche Stelle (hier die Gemeinde) auch prüfen, ob die Übermittlung von Personaldaten für den beabsichtigten Zweck überhaupt erforderlich ist. Gerade dies war hier noch nicht der Fall. Ein rechtliches Inter-

esse bestünde selbstverständlich dann, wenn die GmbH als Erwerberin des Bauhofes feststeht und die Beschäftigten von ihr gem. § 613 a des Bürgerlichen Gesetzbuches übernommen werden. Da auch eine Einwilligung der Beschäftigten des Bauhofes nicht eingeholt wurde, war die Übermittlung der Mitarbeiterlisten, so wie sie hier stattgefunden hat, aus datenschutzrechtlicher Sicht unzulässig.

Bei der Privatisierung öffentlicher Aufgaben ist zu beachten, dass personenbezogene Personaldaten der Beschäftigten erst dann an einen Interessenten übermittelt werden, wenn dieser als Erwerber feststeht. Im Rahmen der Vorbereitung von Privatisierungsvorhaben ist in der Regel eine anonymisierte, zusammengefasste Form der Datenübermittlung ausreichend.

### 4.5.3 Einsicht in Personalakten durch den Amtsausschuss

*Ein bei einem Amt tätiger Beamter auf Probe hatte seine Probezeit beendet. Nunmehr sollte darüber entschieden werden, ob der Beamte in das Beamtenverhältnis auf Lebenszeit übernommen werden konnte. Das Amt hat uns um Mitteilung gebeten, unter welchen Voraussetzungen Mitglieder des Amtsausschusses Einsicht in die Personalakte des Betroffenen nehmen können.*

Nach § 7 Abs. 2 der Amtsordnung (AmtsO) ist der Amtsausschuss oberste Dienstbehörde der Bediensteten der Amtsverwaltung, somit also auch des hier betroffenen Beamten. Der Amtsdirektor ist gem. § 9 Abs. 7 Satz 1 AmtsO wiederum Dienstvorgesetzter der Beamten.

Nach § 61 Abs. 1 des Landesbeamtengesetzes (LBG) kann die Personalakte der obersten Dienstbehörde ohne Einwilligung des Beamten vorgelegt werden. Voraussetzung ist, dass dies für Zwecke der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Damit ist es grundsätzlich möglich, dass Mitglieder des Amtsausschusses Einsicht in die Personalakte ohne Einwilligung des betroffenen Beamten nehmen.

Ob Zwecke der Personalverwaltung oder Personalwirtschaft gegeben sind, ist in jedem Einzelfall gesondert zu prüfen. Bei der Umwandlung eines Beamtenverhältnisses auf Probe in ein solches auf Lebenszeit kann dieser Zweck für die oberste Dienstbehörde durchaus gegeben sein. Dies gilt vor allem dann, wenn der Amtsausschuss nicht von seiner Ermächtigung gem. § 16 Abs. 1 AmtsO i. V. m. § 73 Abs. 2 Satz 4 der Gemeindeordnung (GO) Gebrauch gemacht hat, dem Amtsdirektor die Entscheidung über Ernennungen oder Entlassungen von Beamten zu übertragen. In diesem Fall entscheidet gem. § 73 Abs. 2 Satz 2 GO der Amtsausschuss auf Vorschlag des Amtsdirektors über die Ernennung von Beamten selbst.

Falls die Vorlage der Personalakte gem. § 61 Abs. 1 LBG zulässig ist, so ist allerdings vorrangig gem. § 61 Abs. 1 Satz 5 LBG zu prüfen, ob eine bloße Auskunft aus der Personalakte für den speziellen Informationszweck ausreichend ist. Eine Vorlage der Akte darf dann nicht erfolgen.

Des Weiteren sind Vorlage und Auskunft gem. § 61 Abs. 3 LBG auf den erforderlichen Umfang zu beschränken. Eine Einsicht in die gesamte Personalakte wird in der Regel nicht erforderlich sein. Daraus folgt, dass der Amtsausschuss auch genau angeben muss, zu welchem konkreten Zweck er welche Informationen benötigt.

Schließlich muss auch bei der obersten Dienstbehörde gewährleistet sein, dass entsprechend § 57 Abs. 3 LBG nur Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, Zugang zu Personalakten haben dürfen. Übertragen auf den Amtsausschuss bedeutet dies, dass nicht alle Mitglieder des Amtsausschusses Einsicht nehmen sollten, sondern einzelne Mitglieder damit zu beauftragen sind.

Liegen die hier dargestellten Voraussetzungen nicht vor, ist eine Auskunft aus der Personalakte gem. § 61 Abs. 2 Satz 1 LBG nur mit Einwilligung des Beamten zulässig. Gem. § 61 Abs. 2 Satz 2 LBG sind in diesem Fall Inhalt und Empfänger der Auskunft dem Beamten schriftlich mitzuteilen.

Mitglieder kommunaler Vertretungskörperschaften können unter den Voraussetzungen des § 61 Abs. 1 LBG insbesondere dann Einsicht in Personalakten nehmen, wenn sie nach der Kommunalverfassung für personalrechtliche Entscheidungen zuständig sind. Der Zugang zu Personalakten ist auf den erforderlichen Umfang sowie auf einen möglichst kleinen Personenkreis zu beschränken.

### 4.5.4 Die Arztrechnung in der Stadtverordnetenversammlung

*Eine kreisfreie Stadt unterhält eine eigene Beihilfekasse für ihre Beamten. Im Gegensatz zu anderen Kommunen nutzt sie also hinsichtlich der Beihilfeangelegenheiten der aktiven Beamten nicht die Leistungen des Kommunalen Versorgungsverbandes Brandenburg.*

Nach § 73 Abs. 1 Satz 1 der Gemeindeordnung (GO) gelten für die Kommunalbeamten, soweit nichts anderes bestimmt ist, die landesrechtlichen Vorschriften, also vor allem das Landesbeamtengesetz (LBG). Legt ein Beamter der Stadt Widerspruch gegen einen Beihilfebescheid ein, so erlässt gemäß § 127 Abs. 3 Nr. 2 Satz 1 Landesbeamtengesetz (LBG) die oberste

Dienstbehörde den Widerspruchsbescheid. Oberste Dienstbehörde der Gemeindebeamten ist gemäß § 4 Abs. 1 Satz 1 Nr. 2 LBG die Gemeindevertretung, in kreisfreien Städten die Stadtverordnetenversammlung. Entsprechendes gilt für den Kreistag hinsichtlich der Beamten des Kreises und nach § 7 Abs. 2 Amtsordnung für den Amtsausschuss hinsichtlich der Beamten des Amtes. Die ehrenamtlich tätigen kommunalen Vertretungskörperschaften müssen somit auch in Beihilfeangelegenheiten die Widerspruchsbescheide erlassen.

Dies führt dazu, dass z. B. in der Stadtverordnetenversammlung über sensible gesundheitliche Daten der Beamten, zu denen beispielsweise Arztrechnungen gehören, verhandelt wird. Zwar haben die Stadtverordneten gemäß § 27 GO die Pflicht zur Amtsverschwiegenheit; außerdem wären solche Angelegenheiten selbstverständlich in nicht-öffentlicher Sitzung gemäß § 44 Satz 2 GO zu beraten. Die Praxis zeigt aber, dass dennoch häufig personenbezogene Daten an die Öffentlichkeit gelangen. Darüber hinaus ist schon allein der Personenkreis der Stadtverordnetenversammlung oder Gemeindevertretung, der Zugang zu sensiblen Gesundheitsinformationen hätte, sehr groß. Im Ergebnis machen die Beamten häufig von ihrem Widerspruchsrecht keinen Gebrauch, da sie zu Recht fürchten, dass die sensiblen Daten in unbefugte Hände geraten.

Wir halten den oben beschriebenen Zustand für sehr unbefriedigend. Er widerspricht zum einen dem Grundsatz in § 58 Satz 2 2. Halbs. LBG, dass Zugang zu Beihilfeakten nur Beschäftigte der Beihilfestelle haben dürfen, auch wenn die Vorschrift für behördliche Verfahren eine gewisse Öffnung dieses Grundsatzes zulässt. Zudem sehen die bestehenden Rechtsgrundlagen keine angemessenen Garantien zum Schutze des Rechts auf informationelle Selbstbestimmung vor, wie sie § 4 a Satz 1 Buchst. e des Brandenburgischen Datenschutzgesetzes vorschreibt.

Unabhängig von der Frage, ob das geltende Recht in den oben beschriebenen Fällen zu Verstößen gegen datenschutzrechtliche Grundsätze führt, kann jedenfalls faktisch kein effektiver Rechtsschutz gewährleistet werden.

Aus unserer Sicht müssten die Vorschriften daher dringend geändert werden. Wir halten es für unabdingbar, dass der Erlass von Widerspruchsbescheiden in Beihilfeangelegenheiten kommunaler Beamter nicht mehr in die Zuständigkeit der kommunalen Vertretungen fällt und haben deshalb das Ministerium des Innern gebeten, entsprechende gesetzliche Änderungen ins Auge zu fassen.

Das Ministerium des Innern teilt unsere Auffassung und hat sich eine Änderung des Landesbeamtengesetzes vorgemerkt.

Widerspruchsbescheide in Beihilfeangelegenheiten kommunaler Beamter sollten künftig nicht mehr durch die kommunalen Vertretungen erlassen werden, da auf diese Weise eine größere Zahl von Personen Zugang zu sensiblen Gesundheitsdaten, wie beispielsweise Arztrechnungen, erhalten würde. Wir begrüßen die Absicht des Ministeriums des Innern, die gesetzlichen Bestimmungen in diesem Punkt zu ändern.

## 4.6 Statistik

### 4.6.1 Testgesetz zur Volkszählung

*Die Bundesregierung beabsichtigt, zukünftige Volkszählungen, die auch im Rahmen der Europäischen Union gefordert werden, nicht mehr durch primäre Vollerhebungen, sondern durch die Nutzung von Verwaltungsregistern zu realisieren. Um die Tauglichkeit dieser Register für die Statistik zu erproben, wurde ein Zensusvorbereitungsgesetz (Testgesetz) erar-beitet, auf dessen Grundlage voraussichtlich im Herbst 2001 oder im Frühjahr 2002 Testerhebungen erfolgen sollen. Diese werden sowohl mit Hilfe von Verwaltungsregistern als auch durch die Befragung von Bürgern durchgeführt. Es sollen Stichprobenerhebungen bei Meldebehörden und bei Personen in ausgewählten Gebäuden, eine Gebäude- und Wohnungsstichprobe in ausgewählten Gemeinden und eine Stichprobe bei der Bundesanstalt für Arbeit durchgeführt werden. Die Melderegister sollen auf Mehrfachmeldungen zentral abgeglichen und personenbezogene Daten zusammengeführt werden.*

Dass für den angestrebten Methodenwechsel bei Volkszählungen Testerhebungen in Form von Stichproben stattfinden sollen und hierfür ein spezielles Testgesetz entwickelt wird, ist ausdrücklich zu begrüßen. Es sollte grundsätzlich möglich sein, noch andere Erhebungsarten für zukünftige Zensen anzuwenden, z. B. eine modernisierte postalische Primärerhebung. Viele Fachstatistiker und Datenschutzbeauftragte ziehen bei Volkszählungen ohnehin Primärerhebungen unter Einsatz von Zählern aufgrund der dann höheren Genauigkeit des Ergebnisses vor. Allerdings wäre es wünschenswert, auch die Möglichkeit einer Erhöhung des Anteils an freiwillig zu beantwortenden Fragen zu erproben.

Ein registergestützter Zensus ist zudem nur vordergründig bürgerfreundlicher als eine herkömmliche Zählung. Datenschutzrechtlich ist die Übernahme und Verknüpfung von Daten unterschiedlicher Verwaltungsregister nicht das

mildere Eingriffsmittel[42], sondern stellt vielmehr einen erheblichen Eingriff in die Persönlichkeitsrechte der Betroffenen dar, hinter deren Rücken die Daten zusammengeführt werden.

Nach dem Entwurf des Zensustestgesetzes soll das Statistische Bundesamt zur zentralen Überprüfung der sog. Mehrfachfälle (Personen sind in mehreren Bundesländern gemeldet) alle personenbezogenen Melderegisterdaten im Umfang einer ca 1,2%igen Stichprobe erhalten. Ein solches Verfahren ist datenschutzrechtlich insbesondere dann sehr bedenklich, wenn es bei zukünftigen Zensen für den Abgleich aller Einwohnermelderegister der Bundesrepublik angewendet werden sollte. Ein solches zentralisiertes Verfahren zur automatisierten Verarbeitung von Statistikdaten würde zudem die Länderhoheit außer Acht lassen.

Es sollten Pseudonyme für die identifizierenden Hilfsmerkmale im Rahmen der Testerhebungen erprobt werden und dazu starke kryptographische Sicherheitssoft- oder -hardware eingesetzt werden. Zusätzlich sollte eine Vertrauensstelle eingerichtet werden, die die unverschlüsselten Hilfsmerkmale für eine gewisse Zeit aufbewahrt, damit in Einzelfällen die Klärung der sog. Mehrfachfälle durch Nachfrage der Statistischen Landesämter bei den betroffenen Auskunftspflichtigen möglich ist.

Die geplanten Testerhebungen für zukünftige Volkszählungen und die Erstellung eines Zensustestgesetzes sind grundsätzlich zu begrüßen. Falls bei zukünftigen Volkszählungen auf einen zentralistischen Abgleich aller Melderegister tatsächlich nicht verzichtet werden sollte, sind zusätzliche Maßnahmen wie Pseudonymisierung und Verschlüsselung zu ergreifen, um die Eingriffe in das Persönlichkeitsrecht der Bürger auf das erforderliche Maß zu beschränken.

### 4.6.2 Umwandlung des Landesamtes für Datenverarbeitung und Statistik in einen Landesbetrieb

*Das Brandenburgische Landesamt für Datenverarbeitung und Statistik (LDS) wurde zum 1. Januar 2001 in einen Landesbetrieb umgewandelt. Sind hierdurch Gefahren für die Wahrung des Statistikgeheimnisses entstanden?*

[42] BVerfGE 65, S. 57

In der Geschäftsanweisung aus dem Errichtungserlass des Ministeriums des Innern[43] heißt es, dass für den neuen Landesbetrieb die Rechts- und Verwaltungsvorschriften wie für eine Landesoberbehörde gelten, soweit in der Geschäftsanweisung nichts anderes bestimmt ist. § 13 Landesorganisationsgesetz[44] regelt, dass Landesbetriebe rechtlich unselbständige, organisatorisch abgesonderte Teile der Landesverwaltung sind, deren Tätigkeit erwerbswirtschaftlich oder zumindest auf Kostendeckung ausgerichtet ist.

Der Landesbetrieb besteht aus den Betriebsteilen Informatikzentrum und Statistikzentrum. Als Statistikzentrum führt er weiter die hoheitlichen Aufgaben der amtlichen Statistik und Informationsbereitstellung durch und fungiert damit als statistisches Landesamt. In dieser Funktion ist der Landesbetrieb den Grundsätzen der Neutralität, Objektivität, wissenschaftlichen Unabhängigkeit und statistischen Geheimhaltung (§ 3 Abs. 2 Geschäftsanweisung) wie bisher verpflichtet. Andererseits führt der Landesbetrieb seine Aufgaben mit dem Ziel durch, seine Selbstkosten zu decken und sein Betriebsvermögen zu erhalten. Insgesamt ist seine Tätigkeit nicht auf Gewinnerzielung ausgerichtet (§ 8 Abs. 3 Geschäftsanweisung).

Da der Landesbetrieb Teil der Landesverwaltung bleibt, ist er öffentliche Stelle im Sinne des § 2 Abs. 1 Brandenburgisches Datenschutzgesetz und unterliegt der Kontrolle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht. Der Schutz der Bürgerdaten wird also auch beim Landesbetrieb in gleicher Weise wie bisher gewährleistet; das Statistikgeheimnis bleibt gewahrt. Eine Privatisierung des LDS, also die Umwandlung in eine private Rechtsform, stieße dagegen an rechtliche Grenzen, weil die Durchführung von Erhebungen der amtlichen Statistik zu den Kernaufgaben des Staates gehört.

Bei zukünftigen statistischen Erhebungen durch den Landesbetrieb für Datenverarbeitung und Statistik sollten die Auskunftspflichtigen durch zusätzliche Aufdrucke auf den Erhebungsbögen oder durch besondere Anschreiben über die Rolle des Landesbetriebes aufgeklärt werden.

Gegen die Umwandlung des LDS in einen Landesbetrieb bestehen keine datenschutzrechtlichen Bedenken.

### 4.6.3 Zur Durchführung der Agrarstatistik im Land Brandenburg

*Ein Landwirt beschwerte sich darüber, dass er seine Berichtsbögen zur*

---

[43] ABl. 2000, S. 1189

[44] i. d. F. des Haushaltsstrukturgesetzes 2000, GVBl. I, S. 97

*Agrarstatistik nach dem Agrarstatistikgesetz (AgrStatG) nicht an das Landesamt für Datenverarbeitung und Statistik (LDS), sondern an das Landwirtschaftsamt des Kreises schicken sollte. Er äußerte die Vermutung, dass damit das geltende und verfassungsrechtlich begründete Prinzip der Trennung von Statistik und Verwaltungsvollzug umgangen würde und dass seine statistischen Erhebungsdaten mit den bei der Landwirtschaftsverwaltung vorliegenden Agrarförderungsdaten des Integrierten Verwaltungs- und Kontrollsystems (InVeKoS) der Europäischen Union abgeglichen werden sollten. Auch sei der PC der Erhebungsstelle in das lokale Behördennetz des Landwirtschaftsamtes eingebunden, sodass solche Abgleiche sogar automatisiert erfolgen könnten.*

Erhebungsstellen für die Agrarstatistik sind nach § 95 Abs. 1 AgrStatG in den Kreisverwaltungen eingerichtet worden und sollen nur die Agrarstatistikerhebungen durchführen. Die Auswertung selbst erfolgt dann im Landesbetrieb für Datenverarbeitung und Statistik (§ 12 Abs. 1 Brandenburgisches Statistikgesetz - BbgStatG).

Solche örtlichen Erhebungsstellen müssen zur Wahrung des Statistikgeheimnisses räumlich, organisatorisch und personell vom Verwaltungsvollzug getrennt sein[45].

Im vorliegenden Fall hatte das Landwirtschaftsamt die beiden Bereiche nicht räumlich getrennt. Inzwischen ist dieser Mangel behoben. Zudem war vorgesehen, die Erhebungsbögen nicht, wie vorgeschrieben an die Agrarstatistikstellen oder an das LDS direkt, sondern an das Landwirtschaftsamt des Kreises zu übersenden.

Das LDS hat uns mitgeteilt, im Land Brandenburg würden bis auf Weiteres die InVeKoS-Anträge für die Agrarstatistik nicht verwendet. Dies liege daran, dass sich die Agrarverwaltung in Brandenburg gegenwärtig außer Stande sieht, die Daten zu den für die Bundesstatistik geforderten Terminen zu liefern, ohne dass die Zahlungstermine der Fördermittel, Prämien und Beihilfen für die Landwirte gefährdet würden.

Ferner werden in eingeschränktem Umfang Daten aus den InVeKoS-Förderanträgen zulässigerweise genutzt, um beim LDS das Betriebsregister Landwirtschaft zu führen (§ 97 AgrStatG i. V. m. § 4 Abs. 2 BbgStatG).

Die geschilderte Eingabe werden wir zum Anlass nehmen, das Erhebungsverfahren zur Agrarstatistik erneut auch bei anderen Kreisverwaltungen zu

---

[45] vgl. dazu 3. Tätigkeitsbericht 1994 Pkt. 3.9.5

untersuchen, um uns bei Kontrollen vor Ort ab dem kommenden Jahr ein umfassendes Bild über die praktische Durchführung der Agrarstatistik im Land Brandenburg machen zu können.

Nur eine für die Dauer der Verarbeitung von statistischen Einzelangaben sicher abgeschottete örtliche Erhebungsstelle der Agrarstatistik kann das Vertrauen der Landwirte in die Wahrung des Statistikgeheimnisses rechtfertigen. Eine schriftliche Dienstanweisung über die Abschottung der Erhebungsstelle ist dringend zu empfehlen, damit das Erhebungsverfahren für die auskunftspflichtigen Landwirte transparent wird.

## 4.7 Kommunalrecht

### 4.7.1 Besseres Datenschutzrecht im kommunalen Bereich

*Die Landesregierung hat am 11. Juli 2000 Leitlinien für die künftige Gemeindestruktur in Brandenburg beschlossen[46]. Sie hat sich dabei zum Ziel gesetzt, durch eine Reform der Gemeindestrukturen leistungsstarke amtsfreie Gemeinden und Ämter mit leistungsfähigen Mitgliedsgemeinden zu schaffen und gleichzeitig die kommunale Selbstverwaltung zu stärken.*

Bei der Zusammenarbeit unserer Dienststelle mit den Landkreisen, Ämtern und Gemeinden ergeben sich häufig wiederkehrende Fragen, die mit dem allgemeinen Datenschutzrecht in der Praxis oft nur schwer zu beantworten sind. Gerade in kleinen Verwaltungen und erst recht im Rahmen der ehrenamtlichen Tätigkeit von Gemeindevertretern oder ehrenamtlichen Bürgermeistern zeigen sich häufig Unsicherheiten beim Umgang mit dem Datenschutzrecht.

Wir halten es daher für erforderlich, bestehende Vorschriften mit datenschutzrechtlichem Bezug in der Kommunalverfassung, insbesondere der Gemeindeordnung (GO), zu überarbeiten und für bestimmte Fälle neue bereichsspezifische Datenschutzbestimmungen zu schaffen:

[46] *Leitlinien der Landesregierung für die Entwicklung der Gemeindestruktur im Land Brandenburg, LT-Drs. 3/1482*

- Der Umgang mit personenbezogenen Daten von Einwohnern bei Einwohneranträgen nach § 19 GO bzw. bei Bürgerbegehren und Bürgerentscheiden nach § 20 GO bedarf einer normenklaren gesetzlichen Regelung. Insbesondere ist festzulegen, wie mit Unterschriftenlisten der Bürger umzugehen ist und dass für diese Daten eine strenge Zweckbindung gilt[47].

- Immer wieder treten Schwierigkeiten bei der Anwendung des § 36 GO auf. Häufig besteht Streit darüber, inwieweit die Einsichtnahme in personenbezogene Daten durch Gemeindevertreter zulässig ist bzw. in welchem Umfang die Verwaltung in solchen Fällen eine Akteneinsicht oder Auskunft verweigern darf oder sogar muss. Schließlich sollte in § 36 GO ein Anspruch auf Überlassung von Kopien verankert werden, um das Akteneinsichtsrecht gerade bei komplexen Vorgängen nicht leerlaufen zu lassen [48].

- Es sollten Vorschriften zum Umgang mit personenbezogenen Daten durch die Gemeindevertretung, die Fraktionen und die Ausschüsse geschaffen werden. In diesem Zusammenhang könnte im § 44 GO festgelegt werden, dass in den entsprechenden Sitzungen grundsätzlich keine personenbezogenen Daten verarbeitet werden sollten. Ist dies nicht möglich, muss grundsätzlich die Öffentlichkeit von der Sitzung ausgeschlossen werden[49].

- Schließlich halten wir es für notwendig, dass Vorschriften zur Verarbeitung personenbezogener Daten der Gemeindevertreter durch die Gemeindeverwaltungen aufgenommen werden. So ist beispielsweise zunehmend zu beobachten, dass Kommunalverwaltungen personenbezogene Daten der Gemeindevertreter bzw. Stadtverordneten in das Internet einstellen, ohne die datenschutzrechtlichen Vorschriften zu beachten[50].

Wir haben unsere Vorschläge dem Ministerium des Innern unterbreitet und ihm die Zusammenarbeit mit unserer Dienststelle bei der konkreten Umsetzung unserer Vorschläge angeboten.

Das Ministerium des Innern hat zugesagt, bei der beabsichtigten zweiten Stufe der umfassenden Novellierung der Kommunalverfassung Mitte 2001 unsere Vorschläge zu prüfen.

---

[47] vgl. 6. Tätigkeitsbericht, Pkt. 12.6.1.2

[48] vgl. Tätigkeitsbericht 1999, Pkt. 4.6.1

[49] vgl. 6. Tätigkeitsbericht, Pkt. 12.6.1

[50] vgl. Pkt. A 4.7.2

Es ist erforderlich, dass in die Kommunalverfassung bereichsspezifische Vorschriften zum Datenschutz aufgenommen werden, um den Umgang mit dem Datenschutzrecht in den Kommunen unseres Landes zu erleichtern.

### 4.7.2 Kommunen im Internet - Daten der Gemeindevertreter weltweit verfügbar?

*Ein Gemeindevertreter einer amtsfreien Gemeinde beschwerte sich bei uns darüber, dass er im Internet-Angebot seiner Gemeinde auf der Website der Gemeindevertretung nicht nur seine eigene Privatanschrift, sondern die sämtlicher Gemeindevertreter lesen konnte. Keiner der Gemeindevertreter hatte in diese Veröffentlichung eingewilligt. Die Gemeindevertreter wurden darüber nicht einmal informiert. Die Gemeindevertretung wurde lediglich allgemein darüber informiert, dass die Gemeinde im Internet vertreten sei.*

Wir haben diese Eingabe zum Anlass genommen, die Internet-Auftritte weiterer Kommunen zu überprüfen. Bei einer Reihe von ihnen stellte sich heraus, dass auch hier die Privatanschriften der Gemeindevertreter veröffentlicht waren, ohne dass diese eingewilligt hatten.

Für den Umgang mit personenbezogenen Daten der Gemeindevertreter existieren keine speziellen Vorschriften. Deshalb sind die Regelungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) anzuwenden.

Stellt eine öffentliche Stelle personenbezogene Daten in das Internet ein, so kann potentiell weltweit jeder Kenntnis von diesen Informationen erlangen. Deshalb ist hier eine Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs i. S. v. § 16 und 12 BbgDSG und zudem an ausländische Stellen nach § 17 BbgDSG gegeben.

Gemeindevertreter sind nur in einem örtlich sehr eingeschränkten Umfeld tätig. Es ist nicht ersichtlich, weshalb ihre personenbezogenen Daten ohne ihre informierte Einwilligung über diesen Bereich hinaus verbreitet werden sollten.
Wir haben mehrere Kommunen darauf hingewiesen, dass sie von jedem Gemeindevertreter eine nach § 4 Abs. 2 BbgDSG wirksame Einwilligung einholen müssen, wenn sie deren Privatanschriften im Internet veröffentlichen wollen. Dazu gehört auch eine Information über die Risiken der Veröffentlichung im Internet. Die Veröffentlichung der Adresse des Gemeindebüros ist selbstverständlich ohne Einwilligung zulässig.

Beabsichtigt eine Kommune, die Anschriften ihrer Gemeindevertreter im Internet zu veröffentlichen, so ist dies nur mit einer informierten Einwilligung zulässig. Wir empfehlen, für die Erreichbarkeit der Gemeindevertreter die Anschrift eines Gemeindebüros zu veröffentlichen.

### 4.7.3 Vertrauliches im dörflichen Schaukasten

*Ein Einwohner einer kleinen Gemeinde beantragte bei der unteren Straßenverkehrsbehörde, verkehrsbeschränkende Maßnahmen an der an seinem Grundstück vorbeiführenden Straße anzuordnen. Die Begründung dieses Antrages enthielt zahlreiche personenbezogene Daten, darunter auch Gesundheitsdaten des Bürgers und weiterer Anlieger der Straße. Die Behörde übergab den Antrag u. a. der Gemeinde zum Zweck der Stellungnahme. Die Gemeindevertretung befasste sich daraufhin in öffentlicher Sitzung mit dem Antrag. Er wurde kontrovers diskutiert, allerdings auch wegen der darin enthaltenen sensiblen Daten nicht verlesen. Im Ergebnis hat der Bürgermeister der Gemeinde in einem offenen Brief mitgeteilt, dass der genaue Wortlaut des Antrages an die Straßenverkehrsbehörde im Schaukasten am Gemeindehaus nachzulesen sei und den Antrag des Bürgers daraufhin tatsächlich im Originalwortlaut ausgehängt.*

Der Aushang bedeutet eine Preisgabe personenbezogener Daten, für die keine gesetzliche Grundlage ersichtlich ist.

Der Antrag auf Verkehrsberuhigung ist keine allgemein zugängliche Quelle, sondern ein Schreiben, das zunächst nur an die Straßenverkehrsbehörde gerichtet war. Zugang zu den dort enthaltenen personenbezogenen Daten dürfen nur diejenigen Personen oder Stellen haben, die im Rahmen ihrer Aufgabenerfüllung damit befasst sind. Dies ist neben der Straßenverkehrsbehörde nur die Gemeinde selbst.

Ein solcher Aushang wäre zulässig, wenn er im öffentlichen Interesse läge oder hierfür ein berechtigtes Interesse geltend gemacht würde und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hätte. Die Diskussion über die Anordnung einer verkehrsbeschränkenden Maßnahme für eine öffentliche Straße liegt zwar sicher im öffentlichen Interesse der Bürgerinnen und Bürger. Diese müssen selbstverständlich, beispielsweise im Rahmen der Gemeindevertretersitzungen, die Möglichkeit haben, sich mit Anträgen auf Verkehrsberuhigung oder -beschränkung auseinander setzen zu können. Dieses öffentliche Interesse wird allerdings dadurch erfüllt, dass die Gemeindevertretersitzung über diese Vorhaben berät. Dafür ist es ausreichend, wenn die Bürgerinnen und Bürger über das Ziel des Antrages sowie seine tragenden Gründe informiert werden. Ein

Bezug zu einzelnen im Antrag genannten Personen ist gerade angesichts der im Antrag enthaltenen sensiblen Daten für die Öffentlichkeit nicht relevant. Somit besteht kein öffentliches Interesse, das einen Aushang rechtfertigen würde.

Zusammenfassend ist festzuhalten, dass für die mit dem Aushang im Schaukasten verbundene Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs keine Rechtsgrundlage gegeben ist. Angesichts der mit dem Aushang im Schaukasten verbundenen Prangerwirkung ist dieser Verstoß so schwerwiegend, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht eine förmliche Beanstandung gem. § 25 Abs. 1 BbgDSG ausgesprochen hat.

### 4.7.4 Schüleradressen im Stadtmagazin

*Eine Gemeinde gibt - unter Beteiligung des ehrenamtlichen Bürgermeisters - ein Stadtmagazin heraus, das monatlich erscheint. Die Einschulung der Erstklässler nahm das Stadtmagazin zum Anlass, den Kindern und Eltern zur Einschulung zu gratulieren. Dabei waren alle eingeschulten Kinder namentlich mit ihrer jeweiligen Privatanschrift aufgeführt. Die Veröffentlichung der Privatanschriften war allerdings nur versehentlich erfolgt. Die Eltern waren über die Veröffentlichungen vorher nicht informiert worden und hatten daher auch nicht eingewilligt.*

Die Veröffentlichung von Namen und Anschriften der Erstklässler im Stadtmagazin ohne Einwilligung der Eltern ist aus datenschutzrechtlicher Sicht eine unzulässige Übermittlung personenbezogener Daten.

Die Meldebehörden sind gem. § 5 der Meldedatenübermittlungsverordnung (MeldDÜV) zwar befugt, den Schulverwaltungsbehörden bestimmte Daten der im folgenden Jahr jeweils schulpflichtig werdenden Kinder zu übermitteln. Zu diesen Daten gehören auch der vollständige Name sowie die Anschrift. Diese nach dem Melderecht übermittelten Daten dürfen nach § 28 Abs. 5 des Brandenburgischen Meldegesetzes (BbgMeldeG) aber nur für solche Zwecke verarbeitet werden, zu deren Erfüllung sie auch übermittelt worden sind. Die Meldebehörde übermittelt diese Daten hier ausschließlich zu dem Zweck, die Erfüllung der Schulpflicht zu sichern.
Da die Daten der Kinder von der Schule weitergegeben werden, gelten darüber hinaus das Brandenburgische Schulgesetz (BbgSchulG) sowie die Datenschutzverordnung Schulwesen. Auch nach diesen Vorschriften ist eine Weitergabe von Namen und/oder Anschriften von Erstklässlern ohne Einwilligung der Eltern nicht zulässig. Gem. § 65 Abs. 3 BbgSchulG dürfen Schulbehörden und Schulträger personenbezogene Daten von Schülerinnen und Schülern und ihren Eltern nur verarbeiten, soweit dies zur Erfüllung der in

ihrer Zuständigkeit liegenden Aufgaben der Schulplanung, der Schulorganisation und der Schulaufsicht erforderlich ist. Das sicher gut gemeinte Anliegen, die Namen und Anschriften der Erstklässler zu veröffentlichen, um so die Besonderheit des Beginns eines neuen Lebensabschnittes zu würdigen, ist von diesen Aufgaben der Schulbehörden und Schulträger nicht umfasst. Daher kann eine Veröffentlichung auch nicht auf diese Rechtsgrundlagen gestützt werden.

Personenbezogene Daten von Schülerinnen und Schülern dürfen zum Zwecke der Gratulation zur Einschulung, aber auch z. B. zum Abitur, nur öffentlich bekannt gemacht werden, wenn Eltern oder Schülerinnen und Schüler (soweit sie einwilligungsfähig sind) eingewilligt haben.

### 4.7.5 Ist der Datenschutz auf den Hund gekommen?

*In der Annahme, dass zahlreiche Hundehalter ihre Tiere nicht beim kommunalen Steueramt anmelden, gehen immer mehr Kommunen dazu über, Hundebestandsaufnahmen durchzuführen. Ein privates Unternehmen soll im Auftrag der Kommune nicht angemeldete Hunde ermitteln. Mitarbeiter des Unternehmens suchen dann die Haushalte auf, um festzustellen, in welchen Haushalten ein Hund gehalten wird. Dazu überlassen die Kommunen in vielen Fällen den privaten Auftragnehmern Listen mit Namen und Anschriften von Bürgern. Aus den Verträgen geht oft nicht hervor, ob die Daten aus dem Melderegister stammen oder beispielsweise aus dem Steueramt selbst.*

Das Durchführen einer Hundebestandsaufnahme durch einen privaten Auftragnehmer ist eine Datenverarbeitung im Auftrag gem. § 11 Brandenburgisches Datenschutzgesetz (BbgDSG). Deshalb bedürfen die entsprechenden Verträge der Genehmigung des Ministeriums des Innern. Über die Auftragsvergabe ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht zu unterrichten.

Sollen personenbezogene Daten der bereits gemeldeten Hundehalter an den Auftragnehmer übergeben werden, so ist zu berücksichtigen, dass diese Angaben dem Steuergeheimnis unterliegen. Eine Offenbarungsbefugnis nach § 30 Abs. 4 Abgabenordnung (AO) besteht hier nicht. Im Übrigen wäre eine Weitergabe dieser Daten auch nicht sinnvoll, da sich anhand der Daten nur feststellen lässt, wer bereits einen Hund angemeldet hat, nicht jedoch die Personen ermittelt werden können, die ihrer Pflicht nicht nachgekommen sind.

Auch für die Weitergabe der Daten aller volljährigen Einwohner aus dem Melderegister innerhalb der Gemeinde (z. B. an die Kämmerei) gilt der Er-

forderlichkeitsgrundsatz. Es ist damit zu rechnen, dass der weitaus größte Teil der Einwohner entweder keinen Hund hält oder diesen angemeldet hat. Damit würde der Auftragnehmer die Adressen von einer Vielzahl von Haushalten erfahren, ohne dass dies für die Aufgaben der Kämmerei erforderlich ist. Eine solche Datenweitergabe wäre deshalb unverhältnismäßig und damit unzulässig.

Eine erfolgreiche Hundebestandsaufnahme kann - wie praktische Erfahrungen zeigen - auch durchgeführt werden, wenn dem Auftragnehmer ein Straßenverzeichnis mit Hausnummern und Wohnungsangaben zur Verfügung gestellt wird.

Wir haben das Ministerium des Innern gebeten, unsere Rechtsauffassung künftig zu berücksichtigen und nur noch Verträge zu genehmigen, bei denen keine Listen mit personenbezogenen Daten übergeben werden. Das Ministerium des Innern ist unserer Auffassung bisher nicht gefolgt.

Lässt eine Kommune von einem privaten Auftragnehmer eine Hunde-bestandsaufnahme durchführen, so ist dies aus datenschutzrechtlicher Sicht nur dann zulässig, wenn dem Auftragnehmer keine Listen mit personenbezogenen Daten übergeben werden.

## 4.8 Allgemeines Ordnungsrecht

### 4.8.1 Novellierung der Hundehalterverordnung

*Aufgrund wiederholter Angriffe von gefährlichen Hunden auf Menschen hat das Ministerium des Innern die bereits bestehende Hundehalterverordnung (HundehV) novelliert und verschärft[51]. Nach der neuen Verordnung dürfen bestimmte Hunderassen nicht mehr gehalten oder gehandelt werden. Für das Halten einer Reihe weiterer Hunderassen bedarf der Hundehalter einer Genehmigung der Ordnungsbehörde, die nur erteilt wird, wenn der Hundehalter nachweist, dass der Hund keine gesteigerte Kampfbereitschaft, Angriffslust oder in ihrer Wirkung vergleichbare Eigenschaft aufweist. Darüber hinaus werden alle Personen, die einen Hund mit einer Widerristhöhe von mindestens 40 cm oder einem Gewicht von mindestens 20 kg halten, verpflichtet, dies der Ordnungsbehörde anzuzeigen und ihre Zuverlässigkeit nachzuweisen. Diese Hunde sind zudem auf Kosten des Halters dauerhaft mit einem Mikrochip-Transponder zu kennzeichnen. Dieser enthält eine Chip-Nummer, mit Hilfe derer die Hunde ihren Haltern zugeordnet werden können. Nach wie vor müssen alle Hunde ein*

[51] *Ordnungsbehördliche Verordnung über das Halten und Führen von Hunden (Hundehalterverordnung - HundehV) vom 25. Juli 2000, GVBl. II, S. 235*

*Halsband mit Namen und Adresse des Hundehalters tragen.*

### 4.8.1.1 Die Adresse am Halsband

Die neue Hundehalterverordnung ist in mehreren Punkten datenschutzrechtlich problematisch. Die Verpflichtung in § 2 Abs. 3 Satz 1 HundehV, dass alle Hunde außerhalb des befriedeten Besitztums ein Halsband mit Namen und Adresse des Hundehalters tragen müssen, hätte zu Gunsten einer pseudonymen Kennzeichnung aufgegeben werden sollen[52]. So könnte beispielsweise zumindest bei den Hunden, die ohnehin anzeigepflichtig sind, eine Nummer auf der Steuermarke angebracht werden, mit deren Hilfe das Ordnungsamt beispielsweise den Hund und seinen Halter eindeutig identifizieren kann. Auch angesichts der zusätzlichen Identifikationsmöglichkeit bei Hunden mit Transponder-Chip besteht jedenfalls insoweit kein Bedarf an einer zusätzlichen namentlichen Kennzeichnung.

Eine Petentin, die sich bei uns über die "Adresspflicht am Halsband" beschwerte, machte geltend, dadurch würden potentielle Einbrecher erfahren, welches Haus oder welche Wohnung gerade unbewacht sei. Dieser Sicherheitseinwand ist nicht völlig von der Hand zu weisen. Dennoch konnten wir die Petentin nur auf die bestehende Rechtslage hinweisen.

### 4.8.1.2 Das Führungszeugnis für Hundehalter

Ob die Pflicht zur Vorlage eines Führungszeugnisses ein verhältnismäßiges, insbesondere geeignetes Mittel ist, muss ebenfalls bezweifelt werden. Einerseits enthält das Führungszeugnis Überschussinformationen, andererseits gibt es über bestimmte Straftaten, die für die Prüfung der Zuverlässigkeit nach § 12 HundehV relevant sind, keine Auskunft. Bestimmte Straftaten wie z. B. Hausfriedensbruch dürfen bereits drei Jahre nach Verurteilung nicht mehr im Führungszeugnis erscheinen, sollen aber nach der Hundehalterverordnung fünf Jahre lang die Zuverlässigkeit ausschließen.

[52] vgl. 6. Tätigkeitsbericht, Pkt. 8.2.3

Um die Umsetzung der Hundehalterverordnung für die Ordnungsbehörden zu erleichtern, hat das Ministerium des Innern am 30. August 2000 eine Verwaltungsvorschrift zur Durchführung der Hundehalterverordnung erlassen[53]. Auch hinsichtlich dieser Verwaltungsvorschrift haben wir datenschutzrechtliche Bedenken.

Dieser sind als Anlagen Muster für die verschiedenen Anzeigen, Anträge und zu erteilenden Bescheide beigefügt. Anlage 1 ist ein Muster für die Anzeige der Hundehaltung gem. § 6 HundehV. Dabei werden vom Hundehalter Informationen abgefragt, die aus unserer Sicht für die Durchführung der Hundehalterverordnung nicht erforderlich sind. So können wir insbesondere nicht feststellen, warum die Staatsangehörigkeit des Hundehalters für die Durchführung der Hundehalterverordnung irgendeine Rolle spielen soll.

Unsere Kritik an der novellierten Hundehalterverordnung und an der Verwaltungsvorschrift zur Hundehalterverordnung haben wir in unseren Stellungnahmen zu den Vorschriften gegenüber dem Ministerium des Innern geäußert. Das Ministerium des Innern ist auf keinen dieser Punkte eingegangen. Trotz unserer Bitte erfolgte nicht einmal eine Antwort des Ministeriums. Zudem war eine ausführliche und abschließende datenschutzrechtliche Stellungnahme zu beiden Vorschriften nicht möglich, da uns das Ministerium des Innern jeweils nur eine Frist von einem Tag zur Stellungnahme eingeräumt hat. Zwar haben wir großes Verständnis dafür, dass die Landesregierung die verschärften Vorschriften für die Haltung gefährlicher Hunde zügig umsetzen wollte. Unter solchen Umständen wird jedoch das Recht des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht auf Anhörung gem. § 7 Abs. 2 BbgDSG zur Farce.

### 4.8.1.3 Transpondersysteme zur Kennzeichnung von Hunden

Ein Transponder besteht aus einer etwa 12 x 2 mm großen Bioglaskapsel und enthält einen Microchip sowie eine winzige Spule, die als Antenne dient. Der Transponder-Chip wird dem Tier vom Tierarzt unter die Haut injiziert. Transponder sind passive Sender, dass heißt, sie arbeiten ohne Stromversorgung. Mit Hilfe eines speziellen Lesegerätes wird ein elektromagnetisches Feld erzeugt, wodurch der Transponder eine 15-stellige Chipnummer sendet, die in der Anzeige des Lesegerätes erscheint. Derartige Lesegeräte sind in vielen Tierarztpraxen, Tierheimen sowie in den Ordnungsämtern vorhanden.

[53] ABl. 2000, S. 645

Die im Transponder-Chip gespeicherte 15-stellige Chipnummer ist in der ISO-Norm 11784 (Elektronische Identifizierung von Tieren mit HF-Technik - Codestruktur) definiert. Sie besteht aus einer 12-stelligen, weltweit einmaligen Identifikationsnummer und einem 3-stelligen Ländercode (z. B. DEU für Deutschland). Die Zuordnung der Identifikationsnummer zum jeweiligen Hundehalter kann nur durch das zuständige Ordnungsamt erfolgen. Die technischen Anforderungen an ein Transpondersystem zur Kennzeichnung von Tieren werden in der ISO-Norm 11785 (Elektronische Identifizierung von Tieren mit HF-Technik - Technisches Konzept) festgelegt. Für die Erstellung einer landesweiten Datei gefährlicher Hunde und ihrer Halter gibt es keine rechtliche Grundlage.

Sowohl die novellierte Hundehalterverordnung des Landes Brandenburg als auch die dazu erlassene Verwaltungsvorschrift stoßen in einigen Punkten auf datenschutzrechtliche Bedenken. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird sich aufgrund der bisherigen Erfahrungen für datenschutzrechtliche Verbesserungen im Detail einsetzen.

### 4.8.2 Umsetzung der Hundehalterverordnung - Steuerdaten für das Ordnungsamt?

*Bei der Umsetzung der Hundehalterverordnung stellte sich als Problem heraus, diejenigen Hundehalter zu ermitteln, die ihrer Meldepflicht nicht nachkommen.*

Die Hundehalter sind von sich aus verpflichtet, das Halten bestimmter Hunde beim Ordnungsamt anzuzeigen. Dennoch machen sich viele Ordnungsämter darüber Gedanken, wie sie diejenigen Hundehalter ermitteln können, die entweder aus Unkenntnis oder bewusst ihrer Meldepflicht nicht nachgekommen sind. Dabei wurde vereinzelt der Wunsch geäußert, die im Steueramt gespeicherten Daten über die Hundesteuer zu nutzen.

Die Daten der Hundehalter einschließlich ihrer Namen und Anschriften unterliegen dem Steuergeheimnis. Eine allgemeine Offenbarungsbefugnis für ordnungsbehördliche Zwecke ist nicht vorgesehen. Eine Durchbrechung des Steuergeheimnisses ist nur bei bestehendem zwingenden öffentlichen Interesse an einer Offenbarung i. S. v. § 30 Abs. 4 Nr. 5 Abgabenordnung (AO) möglich. In der Norm sind nur drei Fallgruppen eines zwingenden öffentlichen Interesses ausdrücklich geregelt. Dabei zeigt sich, dass sogar kriminelles Verhalten nicht durchgehend als schwerer Nachteil für das allgemeine Wohl im Sinne dieser Norm zu werten ist. Ein Vergleich des mit der Hundehalterverordnung verfolgten Zwecks der Gefahrenabwehr mit den in § 30 Abs. 4 Nr. 5 AO genannten Fällen wie z. B. der Verfolgung von Straftaten gegen Leib und Leben zeigt, dass hier nicht von einem zwingenden

öffentlichen Interesse an der Offenbarung der Hundesteuerdaten ausgegangen werden kann.

Zulässig wäre es allerdings, wenn das Steueramt selbst die vom Ordnungsamt erstellten Vordrucke zur Anmeldung gefährlicher Hunde an die steuerpflichtigen Hundehalter versendet. Die Hundehalter, die nach der Hundehalterverordnung anzeigepflichtig sind, können dann die ausgefüllten Vordrucke unmittelbar an die Ordnungsämter zurückschicken. Dabei würden keine Steuerdaten vom Steueramt an das Ordnungsamt übermittelt.

Bei der Durchführung der Hundehalterverordnung durch die Ordnungsämter ist darauf zu achten, dass nur solche Daten der Hundehalter verarbeitet werden, die dafür erforderlich sind. Das Steuergeheimnis darf nicht für ordnungsbehördliche Zwecke durchbrochen werden.

# 5 Justiz und Europaangelegenheiten

## 5.1 Benachrichtigung in Nachlasssachen

*Die Suche nach einem Testament oder einer anderen Verfügung von Todes wegen, z. B. einem Erbvertrag, führt nicht selten zu Verzögerungen und Schwierigkeiten bei der Feststellung der Erben und der Abwicklung der Erbschaft. Um dem abzuhelfen, besteht ein Benachrichtigungssystem zwischen Gerichten und Notaren, die Testamente und ähnliche Urkunden aufbewahren, und den Standesämtern, bei denen ein Todesfall registriert wird.*

Gerichte und Notare, vor denen ein Testament in der gesetzlich vorgeschriebenen Form errichtet, Erbverträge geschlossen, die Änderung der Erbfolge bewirkende Erklärungen beurkundet bzw. eigenhändige Testamente in besondere amtliche Verwahrung genommen werden, benachrichtigen die Standesämter von der Existenz und der Verwahrung solcher Urkunden. Darüber hinaus wird das Geburtsstandesamt von dem Standesamt, das den Sterbefall beurkundet, von dem Todesfall benachrichtigt. So kann das Standesamt seinerseits die das Testament verwahrende Stelle von dem Eintritt des Todes- und Erbfalls informieren. Ausgenommen davon sind die sog. eigenhändigen Testamente, d. h. solche Testamente, die der Betroffene selbst ohne Mitwirkung eines Notars verfasst, wenn der Verfasser sie nicht in besondere amtliche Verwahrung gibt, sondern privat aufbewahrt.

Aus datenschutzrechtlicher Sicht stellt sich bei der Benachrichtigung an die Standesämter das Problem, dass es gegenwärtig für die Datenübermittlung zwischen verwahrender Stelle und Standesämtern keine Rechtsgrundlage

gibt. Bisher ist das Verfahren in Form einer Verwaltungsvorschrift als allgemeine Verfügung an die Landesjustiz- und Innenverwaltungen geregelt. Dies genügt dem Erfordernis eines formellen Gesetzes nicht. Dies gilt auch und erst recht in Hinblick auf eine geplante Errichtung einer bundesweiten zentralen Testamentskartei.

Als Rechtfertigung für die Datenübermittlung und -registrierung genügt die Annahme des - mutmaßlichen - Interesses des Verfassers nicht, dass seine Verfügung von Todes wegen im Todes- und Erbfall bald aufgefunden und die Erben ermittelt werden sollen. Um sicher zu gehen, dass die Übermittlung der Daten an die Standesämter im jeweiligen Fall auch tatsächlich im Interesse der Betroffenen erfolgt, bedürfte es der informierten Einwilligung des Verfassers. Zumindest aber müsste er über die beabsichtigte Übermittlung aufgeklärt werden, was in der Praxis ohne unverhältnismäßig hohen Aufwand zu bewerkstelligen ist.

Wer ein Testament verfassen möchte, sollte wissen, dass er nicht verpflichtet ist, dieses in öffentliche Verwahrung zu geben. Die Vermeidung einer Benachrichtigung ist nach der derzeitigen Lage nämlich nur möglich, wenn das Testament privat verwahrt wird. Dies birgt jedoch die Gefahr, dass der dokumentierte letzte Willen des Verfassers nicht oder nur schwer aufgefunden werden kann.

Bis zur erforderlichen Schaffung einer gesetzlichen Grundlage sollen die Benachrichtigungen in Nachlasssachen zwischen verwahrender Stelle und Standesamt und die Registrierung der verwahrten letztwilligen Verfügungen nur mit Einwilligung, zumindest aber mit Kenntnis des Betroffenen erfolgen.

## 5.2 Prüfung der Telefonabhörmaßnahmen bei einer Staatsanwaltschaft

*Im Berichtszeitraum haben wir erneut die Telefonüberwachungsmaßnahmen bei einer Staatsanwaltschaft datenschutzrechtlich geprüft[54]. Ziel war es, die Einhaltung der in den §§ 100 a und 100 b sowie 101 Strafprozessordnung (StPO) vorgeschriebenen Verfahrensschritte zu kontrollieren. Durch Nutzungs- und strikte Vernichtungsregelungen der durch Abhören gewonnenen Erkenntnisse sowie durch die Verpflichtung der Staatsanwaltschaft, die abgehörten Personen zu benachrichtigen, soll gewährleistet werden, dass die Betroffenen keine über das erforderliche Maß hinausgehenden Eingriffe in das Grundrecht auf das Fernmeldegeheimnis (Artikel 10 Grundgesetz) hinnehmen müssen. Bei der geprüften Staatsanwaltschaft ist von 1997 bis 1999 in insgesamt 23*

[54] s. 5. Tätigkeitsbericht, Pkt. 4.4.1

*abgeschlossenen Ermittlungsverfahren abgehört worden.*

Während die staatsanwaltschaftlichen Anträge bei den Amtsgerichten den Anforderungen der Strafprozessordnung entsprachen, war bei einer Reihe von richterlichen Anordnungen aus dem Jahre 1997 festzustellen, dass sie als Beginn der Telefonüberwachungsmaßnahmen (TÜ-Maßnahmen) lediglich den Vermerk "ab Tag der Schaltung" enthielten. Eine solche Festsetzung erschwert die Berechnung der dreimonatigen Höchstfrist einer Abhörmaßnahme mit dem Risiko, dass Verlängerungsanträge zu spät gestellt werden und so ohne richterliche Anordnung abgehört wird. Wir waren daher immer der Auffassung, dass für die Fristenberechnung nicht der Zeitpunkt ausschlaggebend ist, an dem die Überwachung eines Telefonanschlusses technisch realisiert worden ist, sondern das Datum, das der anordnende Richter bestimmt. Unsere Auffassung ist unterdessen durch eine Entscheidung des Bundesgerichtshofes[55] bestätigt worden. In den seither ergangenen richterlichen Anordnungen wird ein genaues Datum für den Beginn der Überwachungsmaßnahme festgesetzt.

Des Weiteren ergab die Prüfung, dass sowohl die TÜ-Unterlagen als auch die Beweis- und Arbeitsbänder länger als erforderlich aufgehoben worden sind. In zwei Fällen waren sie erst unmittelbar vor unserer datenschutzrechtlichen Prüfung vernichtet worden. In einem Fall waren die Betroffenen nicht informiert worden. Die ebenfalls erforderliche Benachrichtigung der Beteiligten stand in allen überprüften Fällen noch aus.

Wir hatten schon früher angeregt, die TÜ-Unterlagen in einer Sonderakte abzulegen, um so die Umsetzung des unverzüglichen Vernichtungsgebotes zu erleichtern. Dem ist das Brandenburgische Justizministerium mit einer Änderung der brandenburgischen Aktenordnung gefolgt. Entsprechend waren in den geprüften Ermittlungsverfahren Sonderakten für die TÜ-Unterlagen angelegt worden, die jedoch zusammen mit den anderen Akten lange über den Zeitpunkt ihrer gebotenen Vernichtung hinaus aufbewahrt wurden.

Zwar verstößt die zu lange Aufbewahrung der TÜ-Unterlagen gegen die grundrechtssichernden gesetzlichen Vorschriften. Die Staatsanwaltschaft hat jedoch bereits vor der Prüfung die bei der Zusammenstellung der Ermittlungsfälle festgestellten Mängel - soweit es möglich war - beseitigt. Sie hat zugesichert, für eine baldige Vernichtung der in Rede stehenden Unterlagen sowie für die Benachrichtigung der Beteiligten Sorge zu tragen.

## 5.3 Die Hinzuziehung "geeigneter" sachverständiger Zeugen

[55] 3 StR 181/98 vom 11. November 1998

*Ein öffentlich bestellter Vermessungsassessor beschwerte sich, weil im Verlauf eines gegen ihn geführten strafrechtlichen Ermittlungsverfahrens wegen des Verdachts der Urkundenfälschung im Amt nicht nur Innenministerium und Landesvermessungsamt über Sachverhalte und Fortgang des Ermittlungsverfahrens früher informiert waren als er, sondern letzteres darüber hinaus auch an einer im Zuge des Ermittlungsverfahrens durchgeführten Hausdurchsuchung beteiligt worden war.*

Das Ministerium des Innern war als oberste Fachaufsichtsbehörde über das Ergebnis einer vom Landesvermessungsamt beim Petenten durchgeführten Geschäftsführungsprüfung unterrichtet worden. Nach § 6 Abs. 2 Landesorganisationsgesetz können sich Landesoberbehörden wie das Landesvermessungsamt und Ministerien als Fachaufsichtsbehörden gegenseitig über ihre Ausübung der Fachaufsicht informieren.

Nachdem durch die Geschäftsführungsprüfung Unregelmäßigkeiten festgestellt worden waren, hatte das Landesvermessungsamt wegen des Verdachts der Falschbeurkundung im Amt und der Beihilfe zum Betrug gegen den Petenten Strafanzeige erstattet. Als obere Landesbehörde ist das Landesvermessungsamt zuständig für die Einhaltung der Berufsordnung der Öffentlich bestellten Vermessungsingenieure[56] im Land Brandenburg und kann - wie im Übrigen jedermann - im Rahmen seiner Aufgabenerfüllung auch Strafanzeige stellen. Zulässig war auch, dass die Staatsanwaltschaft das Landesvermessungsamt über den Gang des von ihm veranlassten Ermittlungsverfahrens und die bevorstehende Anklageerhebung informiert hatte. § 14 Einführungsgesetz zum Gerichtsverfassungsgesetz sieht die Übermittlung von Daten aus Ermittlungsverfahren gegen öffentlich Bedienstete an die Aufsichtsbehörden vor. Dass der Betroffene erst nach dem Landesvermessungsamt Kenntnis von der bevorstehenden Anklageerhebung erhielt, beruht auf den unterschiedlichen Mitteilungszuständigkeiten. Nach § 201 Strafprozessordnung (StPO) teilt nicht die Staatsanwaltschaft, sondern das Gericht dem Beschuldigten die Anklageerhebung mit und informiert ihn über die Klageschrift.

Zwar kann die Staatsanwaltschaft in allen Phasen des Ermittlungsverfahrens, also auch bei einer Hausdurchsuchung, Gutachter hinzuziehen (§ 73 StPO) und sich auch bei der Auswertung der anlässlich einer Hausdurchsuchung sichergestellten Unterlagen sachverständiger Zeugen bedienen (§ 110 StPO). Gutachter bzw. sachverständige Zeugen sollten jedoch nicht aus dem Kreis

[56] GVBl. I vom 18.10.2000, S. 142

der Geschädigten selbst kommen, um den Anschein der Parteilichkeit zu vermeiden. Es muss Zweifel an der Objektivität der gutachterlichen Beratung wecken, wenn die sachverständigen Zeugen als Mitarbeiter der geschädigten, Anzeige erstattenden Stelle in eigener Sache tätig werden.

Der Betroffene muss die mit einer Durchsuchung seiner Wohnung verbundenen Grundrechtseingriffe nur hinnehmen, wenn und soweit die Kenntnisnahme seines Privatbereichs durch Andere im überwiegenden Allgemeininteresse an der Tataufklärung erforderlich ist. Durch die Hinzuziehung von Mitarbeitern der Anzeige erstattenden Stelle als sachverständige Zeugen wird der Kreis der Einblicknehmenden auf ungeeignete Personen erweitert. Dies verletzt das Verhältnismäßigkeitsprinzip. Dem Geschädigten und Anzeigeerstatter muss der Betroffene seine privaten Lebensumstände nicht so weitgehend offenlegen, wie das gegenüber den Beteiligten einer Hausdurchsuchung und im Verlauf der anschließenden Auswertung der sichergestellten Unterlagen geschieht.

Vor diesem Hintergrund halten wir es für unzulässig, dass die Staatsanwaltschaft Mitarbeiter des Landesvermessungsamts an der Durchsuchung der Wohnräume des von diesem angezeigten Petenten und der anschließenden Auswertung der sichergestellten Unterlagen beteiligt hat. Zulässig wäre es jedoch gewesen, wenn die Staatsanwaltschaft das Landesvermessungsamt gebeten hätte, ihr unabhängige sachverständige Zeugen für die beabsichtigte Hausdurchsuchung zu nennen. Die Staatsanwaltschaft hat sich schließlich auch dieser Auffassung angeschlossen und zugesichert, in zukünftigen Fällen die oben dargelegten Erwägungen zu beachten.

Die Staatsanwaltschaft kann Sachverständige als Zeugen zu einer Hausdurchsuchung und zu der Auswertung der dabei sichergestellten Unterlagen hinzuziehen. Wegen der gebotenen Unvoreingenommenheit des staatsanwaltschaftlichen Ermittlungsverfahrens sollte sie jedoch nur auf unabhängige, nicht aus dem Kreis der Geschädigten oder der Anzeigeerstatter kommende Sachverständige zurückgreifen.

# 6 Bildung, Jugend und Sport

## 6.1 Novellierung des Brandenburgischen Schulgesetzes

*Im Rahmen seiner Bildungsoffensive hat das Ministerium für Bildung, Jugend und Sport einen Entwurf zur Änderung des Brandenburgischen Schulgesetzes vorgelegt.*

Um die Qualität von Schule zu verbessern, ist eine Evaluation des Unterrichts

vorgesehen, die die Einbeziehung der Schülerinnen und Schüler sowie deren Eltern erfordert. Anstatt, wie vorgesehen, im Schulgesetz eine Pflicht zur Teilnahme festzuschreiben, gehen wir davon aus, dass das Ziel der Qualitätssicherung und -verbesserung eher erreicht werden kann, wenn die Schülerinnen und Schüler sowie deren Eltern für eine freiwillige Beteiligung gewonnen werden können.

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen war bisher nur mit Einwilligung der oder des Betroffenen zulässig. Dies führte in der Praxis häufig zu unbefriedigenden Lösungen. Beispielsweise durften die Oberstufenzentren keine Klassenlisten ihrer Schüler an einen überbetrieblichen Ausbildungsbetrieb übermitteln, obwohl für diesen die Kenntnis der Daten zur Aufgabenerfüllung erforderlich war. Wir haben aus diesem Grunde ausdrücklich begrüßt, dass unser Vorschlag, Ausbildungsstätten im dualen System wie öffentliche Stellen zu behandeln und damit nicht mehr auf die Einwilligungslösung zurückgreifen zu müssen, nach dem neuesten Entwurf des Ministeriums aufgegriffen werden soll.

Die gegenwärtige Regelung des Einsichts- und Auskunftsrechtes, wonach das Recht für minderjährige Schülerinnen und Schüler durch deren Eltern ausgeübt wird, halten wir vor dem Hintergrund des Grundrechts auf Datenschutz (Art. 11 der Landesverfassung) für zu eng gefasst. Minderjährige Schülerinnen und Schüler sollten dann, wenn sie grundrechtsmündig sind, also ab dem vollendeten 14. Lebensjahr, ein eigenes gesetzliches Einsichts- und Auskunftsrecht erhalten.

Das Ministerium hat unsere Vorschläge bisher insoweit aufgegriffen, als der Abstimmungsentwurf die Datenübermittlung an Einzelpersonen oder private Einrichtungen zur Rechtsverfolgung zulässt sowie für minderjährige Schülerinnen und Schüler ein eigenes Einsichts- und Auskunftsrecht enthält.

## 6.2 Medienoffensive „Schulen ans Netz“

Im Rahmen des Projekts "Brandenburgische Informationsstrategie" (BIS 2006) begann eine Ausstattungs- und Qualifizierungsoffensive - genannt "m.a.u.s" (Medien an unsere Schulen) - an allgemein bildenden Schulen in öffentlicher Trägerschaft. Ziel ist es, den Einsatz neuer Medien zu forcieren und allen Schulen einen Internetanschluss zur Verfügung zu stellen.

Dazu hat das Pädagogische Landesinstitut Brandenburg (PLIB) eine Reihe von Qualifizierungsmaßnahmen für Lehrerinnen und Lehrer im Rahmen der Medienoffensive angeboten. Auch unsere Behörde hat im PLIB mehrere Work-shops zu technisch-organisatorischen Maßnahmen beim Anschluss von Netzen an das Internet sowie über rechtliche Vorgaben der Tele- und

Mediendienstegesetze durchgeführt.

Aus Sicht des Datenschutzes sollten insbesondere folgende Punkte beim Anschluss von Schulen an das Internet berücksichtigt werden:

- Datenverarbeitungsgeräte der Verwaltung dürfen nicht mit im Unterricht verwendeten Datenverarbeitungsgeräten vernetzt werden (§ 4 der Datenschutzverordnung Schulwesen - DSV).

- Die Veröffentlichung von Lehrer- oder Schülerdaten im Internet ist nur mit der informierten Einwilligung des Betroffenen zulässig.

- Präsentiert sich die Schule mit einem eigenen WWW-Angebot im Internet, so besteht gem. § 6 Teledienstegesetz (TDG) und § 6 Mediendienste-Staatsvertrag (MDStV) die Pflicht zur Anbieterkennzeichnung.

- Die Erstellung von Nutzerprofilen ist nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 Teledienstedatenschutzgesetz - TDDSG - und § 13 Abs. 4 MDStV).

- Protokolldateien auf den WWW-Servern dürfen nur in anonymisierter Form gespeichert werden.

- Bei eigenen Angeboten sollte auf den Einsatz von Cookies verzichtet werden.

- Bei der Gestaltung von Websites sollte man aus Sicherheitsgründen auf aktive Inhalte (u. a. Java-Applets, ActiveX-Controls) verzichten.

- Anbieter von eigenen Inhalten im Netz sind für diese verantwortlich (§ 5 Abs. 1 TDG).

- Anbieter sind für fremde Inhalte, die sie (z. B. über Links) zur Nutzung bereithalten, nur dann verantwortlich, wenn sie diese Inhalte kennen und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern (§ 5 Abs. 2 TDG).

Es wird außerdem entscheidend darauf ankommen, die Schülerinnen und Schüler in den "Computerkabinetten" und "Medienecken" darauf vorzubereiten, was sie im Netz erwartet. Eine intensive medienpädagogische Arbeit ist nötig - was wiederum nachhaltige Anstrengungen in der Lehrerfortbildung

voraussetzt -, um zum einen die Chancen des weltweiten Netzes zu nutzen, ohne andererseits die Risiken zu unterschätzen.

Auch datenschutzrechtliche Aspekte sind beim Internetanschluss an Schulen zu berücksichtigen. Daneben muss den Schülerinnen und Schülern eine Medienkompetenz vermittelt werden, damit sie die Chancen des Internets bei gleichzeitiger Beherrschung der Risiken nutzen können.

## 6.3 Videoüberwachung von Schülerinnen und Schülern

### 6.3.1 Videoüberwachung in öffentlichen Verkehrsmitteln, insbesondere in Schulbussen

*Ein Landkreis und eine amtsfreie Gemeinde führen gegenwärtig ein Pilotprojekt zur Videoüberwachung in Bussen durch, die überwiegend oder ausschließlich zur Schülerbeförderung eingesetzt werden. Ziel dieser Maßnahmen soll es vor allem sein, das Verhalten der Schülerinnen und Schüler positiv zu beeinflussen, um Unfallgefahren zu vermeiden und Sachbeschädigungen aufzuklären. Unklar ist dabei noch, durch welche Stellen in welcher Art und Weise die Auswertung des aufgezeichneten Bildmaterials erfolgen soll.*

Ob und unter welchen Voraussetzungen der Einsatz von Videoüberwachung ein verhältnismäßiges Mittel ist, um die Sicherheit in Schulbussen zu erhöhen, muss sorgfältig abgewogen werden. Grundsätzlich stellt die Beobachtung durch Videokameras und die Aufzeichnung und Speicherung der Bilder einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler und der übrigen Fahrgäste dar. Das gilt nicht nur für Kameras in Schulbussen, sondern auch für die Videoüberwachung im öffentlichen Personenverkehr insgesamt. Anders als bei der Beobachtung durch das Begleitpersonal ist für die Betroffenen bei der Videoaufzeichnung nicht nachvollziehbar, wer zu welchem Zeitpunkt ihr Verhalten registriert. Der Begleitung durch Aufsichtspersonal oder Begleitpersonen ist wegen des geringeren Grund rechtseingriffs im Regelfall der Vorzug zu geben, zumal sie auch die Gewähr bietet, dass in einer konkreten Gefahrensituation eingegriffen werden kann. Eine Videoüberwachung sollte deshalb nur in Ausnahmefällen in Betracht kommen.

Da das Thema der Videoüberwachung im öffentlichen Nahverkehr bundesweit an Bedeutung gewinnt, haben die Datenschutzbeauftragten des Bundes und der Länder gemeinsam mit dem Verband Deutscher Verkehrsunternehmen (VDV) und dessen Mitgliedsunternehmen eine Arbeitsgruppe gebildet, die sich mit der Thematik befasst. Als erstes Ergebnis

der Arbeitsgruppe konnte eine Reihe von Voraussetzungen entwickelt werden, unter denen der Einsatz von Videoüberwachung auch durch die Datenschutzbeauftragten für hinnehmbar gehalten wird. Diese gelten grundsätzlich auch für die Beförderung von Schülerinnen und Schülern durch öffentliche Verkehrsmittel. Dabei handelt es sich um folgende Punkte:

- Videoüberwachung in öffentlichen Verkehrsmitteln setzt zunächst grundsätzlich voraus, dass sie der Gewährleistung der öffentlichen Sicherheit bei der Beförderung dient, sie zu diesem Zweck erforderlich ist und die Rechte der Fahrgäste auf informationelle Selbstbestimmung nicht unverhältnismäßig beeinträchtigt werden,

- die Videobeobachtung (ohne Aufzeichnung) kann durchgeführt werden, wenn zugleich sichergestellt werden kann, dass in konkreten Gefahrsituationen zur Sicherheit der Fahrgäste auch eingegriffen werden kann,

- eine Videobeobachtung ist in der Regel dann verhältnismäßig, wenn die Fahrgäste in geeigneten Fällen die Möglichkeit haben, unbeobachtet fahren zu können,

- eine Videoaufzeichnung ist zulässig, wenn ein Anlass dazu besteht, etwa weil Ereignisse festgestellt werden, die die Gewährleistung der Sicherheit beeinträchtigen,

- die Auswertung aufgezeichneter Bilder darf nur zu dem Zweck erfolgen, zu dem sie aufgezeichnet worden sind und nur durch die dazu befugten Personen vorgenommen werden; nicht benötigte Bilder müssen unverzüglich gelöscht werden,

- an den Verkehrsmitteln ist auf die Beobachtung und Aufzeichnung sowie auf die verantwortliche Stelle deutlich unter Angabe der Telefonnummer hinzuweisen; wird personenbezogen ausgewertet, sind die Betroffenen grundsätzlich zu benachrichtigen,

- die notwendigen Sicherheitsmaßnahmen sind in einer Betriebs- bzw. Dienstanweisung festzulegen,

- die Videoüberwachung ist hinsichtlich ihrer Erforderlichkeit und der Datenschutzvorkehrungen kontinuierlich zu prüfen.

Konkret für die Schülerbeförderung bedeutet dies Folgendes:

Als Rechtsgrundlage für die Videoüberwachung kommen sowohl § 33 c des Brandenburgischen Datenschutzgesetzes (BbgDSG) als auch das Bundesdatenschutzgesetz (BDSG) in Betracht. Dies hängt davon ab, ob die Schülerbeförderung als hoheitliche Aufgabe der Landkreise im Sinne von § 2 Abs. 1 Satz 3 BbgDSG begriffen wird, führt aber in der Bewertung nicht zu unterschiedlichen Ergebnissen.

Nach § 33 c Abs. 1 BbgDSG ist die Videoüberwachung öffentlich zugänglicher Räume, also auch in öffentlichen Verkehrsmitteln, zulässig, soweit dies zur Erfüllung der Aufgaben erforderlich ist und überwiegende schutzwürdige Interessen Betroffener nicht beeinträchtigt werden.

Hierbei ist insbesondere an diejenigen Fahrgäste zu denken, die sich während der Fahrt ordnungsgemäß verhalten. In deren Persönlichkeitsrechte wird erheblich eingegriffen, ohne dass sie selbst eine Gefahr für die sichere Beförderung darstellen. Deshalb kann Videoüberwachung nur dann eingesetzt werden, wenn die Gefahren und Störungen ein Ausmaß erreicht haben, das die schutzwürdigen Interessen der sich ordnungsgemäß verhaltenden Fahrgäste in den Hintergrund treten lässt.

Schließlich ist zu differenzieren, ob eine bloße Beobachtung ohne Aufzeichnung erfolgt oder auch eine Aufzeichnung und Speicherung von Bildern. An die bloße Beobachtung sind geringere Anforderungen zu stellen, da diese lediglich als "verlängerter Rückspiegel" des Fahrpersonals dient. Die Aufzeichnung sollte erst dann erfolgen, wenn sich eine erhebliche Gefährdung für eine sichere Beförderung ergibt. Durch den Einsatz von Ringspeichern ist es technisch möglich, auch solche Bilder zu speichern, die bereits vor dem Ereignis aufgenommen worden sind. Erfahrungen großer Verkehrsunternehmen zeigen, dass die Verkehrssicherheit nicht beeinträchtigt wird, wenn das Fahrpersonal über einen Monitor das Wageninnere beobachtet und bei entsprechenden ähnlichen Anlässen eine Aufzeichnungstaste drückt. Darüber hinaus sind Erziehungs- und Ordnungsmaßnahmen der Schule denkbar. Zu diesem Zweck kann das Verkehrsunternehmen im Einzelfall schülerbezogene Angaben übermitteln.

Für die Auswertung der Aufzeichnungen ist in einer Dienstanweisung des jeweiligen Landkreises festzulegen, wie die Auswertung zu erfolgen hat. Der Kreis derjenigen, die auf die aufgezeichneten Bilder zugreifen können, ist so gering wie möglich zu halten.

Werden bei der Auswertung Ordnungswidrigkeiten oder Straftaten festgestellt, so ist es zulässig, Anzeige zu erstatten und den

Ermittlungsbehörden die Aufzeichnungssequenz zur Verfügung zu stellen. Das Personenbeförderungsrecht lässt auch einen - vorübergehenden - Ausschluss von der Schülerbeförderung bei gravierendem Fehlverhalten zu.

Ob darüber hinaus bei Aufnahmen von Schülerinnen und Schülern eine Übermittlung an den Schulpsychologischen Dienst zulässig ist, erscheint uns zweifelhaft. Dessen Befugnisse sind abschließend in § 14 der Datenschutzverordnung Schulwesen geregelt. Danach können Daten entweder nur beim Betroffenen selbst erhoben werden oder durch Einsicht in die Schülerakte. Diese Voraussetzungen sind hier nicht erfüllt.

Das Ministerium für Bildung, Jugend und Sport teilt unsere Auffassung nicht in allen Punkten, hat aber Gesprächbereitschaft signalisiert.

Die Videoüberwachung bei der Schülerbeförderung stellt einen erheblichen Eingriff in die Persönlichkeitsrechte der Betroffenen, aber auch des Fahr- und Begleitpersonals dar. Dieser ist nur unter sehr strengen Voraussetzungen zulässig.

### 6.3.2 Videoüberwachung auf dem Schulgelände

*Auf dem Gelände einer Schule sollte eine Videoüberwachungsanlage installiert werden, um die Verantwortlichen für Zerstörungen und Verunstaltungen zur Rechenschaft ziehen zu können.*

Die Videoüberwachung bedeutet unabhängig davon, ob Aufzeichnungen hergestellt werden, einen Eingriff in die Rechte der Betroffenen (also aller Personen, die in das Visier der Kamera geraten).

Bei der Erhebung von Daten von Schülerinnen und Schülern sind die Vorschriften des § 65 des Brandenburgischen Schulgesetzes (BbgSchulG) sowie der darauf basierenden Datenschutzverordnung Schulwesen (DSV) zu beachten. Die Videoüberwachung ist dort nicht geregelt.

Demgegenüber enthält § 33 c BbgDSG eine allgemeine Vorschrift zur Videoüberwachung durch öffentliche Stellen. Diese Norm ist jedoch nur auf schulfremde Personen anwendbar, weil die Datenverarbeitung in der Schule, soweit sie Personen betrifft, die dem Schulgesetz unterliegen, dort abschließend geregelt ist.

Nach § 33 c Abs. 1 Satz 1 BbgDSG ist eine Videoüberwachung zwar zulässig, wenn sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist. Weitere Voraussetzung ist aber, dass

überwiegende schutzwürdige Interessen Betroffener nicht beeinträchtigt werden. Daran bestanden im vorliegenden Fall erhebliche Zweifel. Die Videoüberwachung sollte dem Zweck dienen, Beschädigungen und Verunstaltungen zu verhindern. Wir sind davon ausgegangen, dass solche Taten nur von einer geringen Zahl von Schülerinnen und Schülern begangen werden, gleichwohl werden jedoch alle Schülerinnen und Schüler überwacht. Auch und gerade auf dem Schulgelände muss grundsätzlich die Möglichkeit und das Recht bestehen, sich frei und unbeobachtet bewegen zu können. Dieses schutzwürdige Interesse wird durch eine Videoüberwachung auf unverhältnismäßige Weise eingeschränkt.

Wir haben dem Schulträger deshalb empfohlen, von dem geplanten Vorhaben abzusehen und stattdessen den Hausmeister z. B. durch Mitglieder des Lehrerkollegiums bei der Aufsicht unterstützen zu lassen. Eine Beaufsichtigung der Schülerinnen und Schüler durch Personen halten wir in jedem Fall für Erfolg versprechender als eine automatisierte Überwachung durch Videokameras. Der Schulträger hat uns mitgeteilt, dass er noch keine abschließende Entscheidung zur Installierung einer Videoüberwachungsanlage gefällt habe.

Die Videoüberwachung eines Schulgeländes ist aus datenschutzrechtlicher Sicht nicht zulässig und stellt eine unverhältnismäßige Einschränkung der Persönlichkeitsrechte der Schülerinnen und Schüler dar.

## 6.4 Polizeibefragung in einer Gesamtschule - ohne Wissen der Eltern

*Im Rahmen eines Projekts zur Gewaltprävention wurden in den Klassen 4 bis 6 einer Gesamtschule in Zusammenarbeit mit einer Polizeilichen Beratungsstelle Fragebögen verteilt und anschließend schülerbezogen erfasst, ohne dass die Eltern davon Kenntnis hatten. Die in den Klassen ausgefüllten Fragebögen wurden an die Polizeiliche Beratungsstelle weitergeleitet. Auf einer nachfolgenden Elternversammlung erhielten die Eltern einen entsprechenden Fragebogen, der dann mit dem ihres Kindes verglichen wurde und durchaus Aufschluss über die jeweilige Familiensituation gab. Einer der Fragen lautete beispielsweise: "Was magst du an deiner Mutter/deinem Vater am Wenigsten?".*

Bei einer solchen Fragebogenaktion handelt es sich um eine personenbezogene Datenerhebung über minderjährige Schüler. Dafür gibt es keine Rechtsgrundlage, sodass die Erhebung und Verarbeitung der Daten nur auf der Basis einer Einwilligung i. S. v. § 4 Brandenburgisches Datenschutzgesetz (BbgDSG) erfolgen kann. Im Falle der Minderjährigkeit der Schülerinnen und Schüler müssen auch die Sorgeberechtigten (i. d. R.

die Eltern) einwilligen. Vor der schriftlichen Einwilligungserklärung sind sie über den Sinn und Zweck der Umfrage, die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis zu informieren. Sie dürfen die Einwilligung ohne Nachteile verweigern oder für die Zukunft widerrufen. Ebenso sollte darüber informiert werden, wie lange die Fragebögen aufbewahrt werden. Um die Tragweite ihrer Einwilligungserklärung transparent zu machen, sollte vorher Einblick in die Fragebögen gewährt werden. Dessen ungeachtet ist die Teilnahme auch für die Schülerinnen und Schüler freiwillig.

Sowohl die betreffende Gesamtschule als auch das zuständige Polizeipräsidium haben unsere Hinweise akzeptiert. Die Fragebögen sind inzwischen vernichtet worden.

Fragebogenaktionen an Schulen dürfen nur mit Einwilligung der Eltern minderjähriger Schülerinnen und Schüler sowie der Befragten selbst durchgeführt werden.

## 6.5 Zeitkarte für Schüler - ein Sammelsurium von Daten

*Der Vorsitzende einer Elternkonferenz hatte erhebliche Zweifel an der Zulässigkeit der Erhebung personenbezogener Daten in einem Antrag auf eine Schülerbeförderungszeitkarte. Fraglich war auch, welche für die Schülerbeförderung erforderlichen Daten das Schulverwaltungsamt an das jeweilige Verkehrsunternehmen übermitteln darf.*

Mit dem Antragsformular soll ermittelt werden, ob die Voraussetzungen für die Schülerfahrtkostenerstattung gem. § 112 Brandenburgisches Schulgesetz (BbgSchulG) vorliegen. Zuständig für die Schülerbeförderung sind die Landkreise und kreisfreien Städte, in denen sich die Wohnung oder die Ausbildungs- oder Arbeitsstelle befindet. Sie nehmen die Aufgaben und die Finanzverantwortung wahr. Sie bestimmen in der Satzung die Mindestentfernung zwischen Wohnung und Schule, ab der ein Beförderungs- oder Erstattungsanspruch besteht.

In dem betroffenen Landkreis variierte die festgelegte Entfernungsgrenze je nach Schuljahr des Schülers. Maßgeblich ist daher nicht das Geburtsdatum, sondern die Klassenstufe des Antrag stellenden Schülers. Zur Ermittlung der Erstattungsvoraussetzungen ist die Kenntnis der Anschriften der Schule und des Antragstellers erforderlich.

Das zuständige Schulverwaltungsamt vertrat die Auffassung, dass aus Gründen der besseren Zuordnung für die Bearbeitung der jeweiligen Anträge das Geburtsdatum der Schüler erforderlich sei. Es begründete dies damit, dass

Fälle aufgetreten seien, in denen Kinder mit gleichem Namen und gleicher Wohnanschrift die gleiche Klasse einer Schule besuchten. Unseren Vorschlag, eine Differenzierung bzw. Zuordnung mit Hilfe der unterschiedlichen Vornamen vorzunehmen und damit auf das Geburtsdatum der Schüler zu verzichten, hat das Schulverwaltungsamt aufgegriffen und wird künftig auf die Erhebung des Geburtsdatums verzichten.

Das Schulverwaltungsamt übermittelt die aus seiner Sicht zur Erstellung der Fahrausweise notwendigen personenbezogenen Daten an das zuständige Verkehrsunternehmen. Dies sind Name, Vorname, Wohnanschrift, Klassenstufe, Ein- und Ausstiegshaltestelle, Zeitraum, Schülerpassnummer und derzeit besuchte Schule. Die Übermittlung der Adressen aller Schüler ist nicht erforderlich. Das Schulverwaltungsamt hat sie mit der Ausstellung der beantragten Fahrausweise begründet. Außerdem benötige das Verkehrsunternehmen die Anschriften, um Verstöße gegen die Beförderungsbedingungen zu verfolgen und zu ahnden.

Es ist jedoch nicht nachvollziehbar, weshalb die Adresse des Schülers im Gegensatz zu anderen Fahrgästen auf dem Fahrausweis vermerkt sein muss. Zur Identifizierung des jeweiligen Schülers genügt in der Regel das Lichtbild. Ein- und Ausstiegshaltestelle bestimmen den Beförderungsweg eindeutig. Die Angabe des Namens und der Anschrift auf der Zeitkarte sollte freiwillig erfolgen, um im Falle des Verlustes die Karte dem Besitzer wieder zuleiten zu können.

Die Landkreise und kreisfreien Städte dürfen nur die für die Schülerfahrtkostenerstattung erforderlichen personenbezogenen Daten der Schülerinnen und Schüler verarbeiten. Die Übermittlung der Adresse der Betroffenen an die jeweilige Verkehrsgesellschaft ist für die Ausstellung der Zeitkarte nicht erforderlich und damit unzulässig.

## 6.6 Zu viele Daten für einen Kita-Platz?

*Mit dem neuen Kindertagesstättengesetz hat das Land Brandenburg den Rechtsanspruch des Kindes auf Erziehung, Bildung, Betreuung und Versorgung in Kindertagesstätten hinsichtlich der Altersgruppen und des zeitlichen Umfangs eingeschränkt. Zum Nachweis des Rechtsanspruchs gem. § 1 Abs. 2 und 3 Kindertagesstättengesetz (KitaG) wurden und werden von den Ämtern und Gemeinden Fragebögen entwickelt, die jedoch den datenschutzrechtlichen Anforderungen entsprechen sollten. Wir haben die am häufigsten aufgetretenen Probleme in einem Merkblatt zusammengefasst, das wir den Landkreisen und kreisfreien Städten zur Verfügung gestellt haben, um eine datenschutzgerechte Praxis in den*

*Ämtern und Gemeinden sicherzustellen.*

Auf folgende grundsätzliche Probleme haben wir hingewiesen:

- Nach § 62 Abs. 2 Achtes Buch Sozialgesetzbuch (SGB VIII) sind die Betroffenen über die Rechtsgrundlage der Erhebung, den Erhebungszweck und den Zweck der Verarbeitung oder Nutzung der Daten aufzuklären. Dies kann in geeigneter Weise entweder in einem Anschreiben zum Fragebogen oder auch auf dem Erhebungsbogen selbst erfolgen. Die Rechtsgrundlage ergibt sich in diesem Zusammenhang aus § 62 Abs. 1 SGB VIII i. V. m. § 1 Abs. 2 und 3 KitaG in der ab dem 01. Juli 2000 geltenden Fassung.

- Es muss deutlich werden, dass die Frage zur familiären Situation nur dann zu beantworten ist, wenn das Kind entweder das zweite Lebensjahr noch nicht vollendet hat, die fünfte oder sechste Schuljahrsgangsstufe besucht und/oder eine längere Betreuungszeit als vier Stunden (Hort) bzw. sechs Stunden (bis zur Einschulung) gewünscht wird.

- Bei der Frage nach der Erwerbstätigkeit der Personensorgeberechtigten ist es nicht erforderlich, nach der Art der Tätigkeit zu differenzieren. Lediglich die Frage nach der Befristung ist zulässig.

- Wird die Erwerbstätigkeit/Aus- und Fortbildung vom Arbeitgeber/der Bildungsstätte bestätigt, so sollte dies für jedes Elternteil auf getrennten Formularen erfolgen.

Darüber hinaus wollten viele Gemeinden weit mehr Daten erheben, als zur Anspruchsprüfung erforderlich waren. Ursache hierfür war eine erhebliche Unsicherheit bei der Auslegung unbestimmter Rechtsbegriffe wie "familiäre Situation" oder "besonderer Erziehungsbedarf". Beispielsweise wurden die Vorlage des Personalausweises sowie Einwilligungserklärungen verlangt. Mit letzteren sollten die Eltern der Datenverarbeitung zu anderen Zwecken wie der Beantragung von Bundeserziehungsgeld bzw. dem Datenabgleich zwischen Jugend- und Meldeamt zustimmen. Die Verknüpfung solch weitreichender Einwilligungen mit dem Antrag auf einen Kita-Platz, aber auch die Aufforderung zur Vorlage eines Personalausweises ist unverhältnismäßig.

Insgesamt kommt es aus datenschutzrechtlicher Sicht darauf an, dass nur die Daten von den Betroffenen erhoben werden, die für die Aufgabenerfüllung (Prüfung des Rechtsanspruchs) erforderlich sind. Erforderlich kann im Einzelfall die Vorlage einer Arbeitgeberbescheinigung über den Beschäftigungsumfang sein, wenn es um den Anspruch auf verlängerte Betreuung eines Kindes geht.

Weiter hatten wir die Frage zu prüfen, inwieweit eine Gemeinde ab dem 1. Januar 2001 verpflichtet ist, die Prüfung des Rechtsanspruchs auf Betreuung in einer Kindertagesstätte und die damit verbundene Datenverarbeitung selbst vorzunehmen. Mitunter wurde die Auffassung vertreten, dass es zu den Kompetenzen und zur Verantwortung eines freien Trägers gehöre, auf der Grundlage des Kindertagesstättengesetzes die erforderlichen Daten und Nachweise zur Feststellung des Rechtsanspruchs auf einen Kita-Platz zu erheben.

Dazu haben wir festgestellt, dass den Gemeinden ab dem 1. Januar 2001 die Verpflichtung obliegt, den Rechtsanspruch auf Kindertagesbetreuung zu überprüfen. Rechtsgrundlage dafür ist § 12 Abs. 1 Satz 1 KitaG, in der ab dem 1. Januar 2001 geltenden Fassung. Mit dieser Anspruchsprüfung ist die im Rahmen des § 1 KitaG erforderliche Datenverarbeitung verbunden. Die Rechtsanspruchsprüfung ist gem. § 1 KitaG dem Leistungsverpflichteten übertragen worden. Soweit eine Gemeinde jedoch der Auffassung ist, dass die Datenerhebung im Rahmen der Anspruchsprüfung für sie mit einem zusätzlichen personellen Aufwand verbunden ist, kann dem freien Träger eine solche Auftragsdatenvereinbarung nach § 80 SGB X übertragen werden. Dabei ist jedoch zu bedenken, dass der Träger der Einrichtung die erforderlichen Daten nur erheben und an den Leistungsverpflichteten weitergeben kann. Die Gemeinde, gegen die sich der Anspruch richtet, bleibt in der Verpflichtung, den entsprechenden Bescheid zu erlassen.
Die Gemeinden dürfen zur Prüfung des Rechtsanspruchs auf Kitabetreuung von den Betroffenen nur die erforderlichen Daten erheben. Sie müssen darauf achten, den Erhebungsbogen datenschutzgerecht zu gestalten. Zu dieser Thematik kann ein Merkblatt bei uns angefordert werden.

## 6.7 Einsicht in Jugendamtsakten zu Ausbildungszwecken?

*Ein Angestellter eines Gesundheitsamtes, der eine Amtsarztausbildung absolvierte, bat das Jugendamt, in bestimmte Jugendamtsakten für seine wissenschaftliche Arbeit mit dem Thema "Zusammenarbeit zwischen dem Gesundheitsamt und dem Jugendamt" einzusehen. Das Jugendamt hatte dabei datenschutzrechtliche Bedenken.*

Gem. § 64 Abs. 1 SGB VIII dürfen Sozialdaten zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind. Ausnahmsweise ist nach § 67 c Abs. 3 Satz 2 SGB X zu Ausbildungs- und Prüfungszwecken eine Nutzung unabhängig vom Erhebungszweck des Absatzes 1 Satz 1 und vom Speicherungszweck des Absatzes 1 Satz 2 zulässig. Dies gilt aber nur unter der Voraussetzung, dass keine schutzwürdigen Interessen des Betroffenen entgegenstehen.

Die Nutzung sollte nicht durch die speichernde Stelle - das Jugendamt -, sondern durch einen Mitarbeiter des Gesundheitsamtes zu Ausbildungszwecken erfolgen. Unabhängig von der Klärung der Frage, ob dieser Mitarbeiter im Rahmen seiner wissenschaftlichen Arbeit in irgendeiner Form dem Jugendamt zuzurechnen sein könnte, ist im Rahmen einer Interessenabwägung zu berücksichtigen, dass es sich um sehr sensible Daten handelt, die zum Teil auch dem besonderen Vertrauensschutz des § 65 SGB VIII und der durch § 203 Strafgesetzbuch strafbewehrten beruflichen Schweigepflicht unterliegen. Sollen solche Unterlagen für Ausbildungszwecke genutzt werden, sind sie zu anonymisieren. Dies gilt auch dann, wenn Auszubildende zur Verschwiegenheit verpflichtet sind. Soweit eine Anonymisierung aus organisatorischen Gründen nicht in Betracht kommt, ist eine Akteneinsicht nur nach Einwilligungserklärung der jeweiligen Betroffenen bzw. der Sorgeberechtigten möglich. Im Übrigen scheidet eine Akteneinsicht aus.

Sollen Jugendamtsakten für Ausbildungszwecke genutzt werden, sind sie vorab zu anonymisieren. Ist dies nicht möglich, ist eine Akteneinsicht nur mit der Einwilligung des Betroffenen bzw. Personensorgeberechtigten möglich.

## 7 Wissenschaft, Forschung und Kultur

### Unvollständige Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten von Studierenden

*Im Zusammenhang mit der chipkartengestützten Verarbeitung personenbezogener Daten von Studierenden stellte sich die Frage, ob das Brandenburgische Hochschulgesetz hierzu ausreichende Regelungen trifft oder ob zusätzlich noch eine Rechtsverordnung erlassen werden muss.*

Das Brandenburgische Hochschulgesetz (BbgHSG) regelt die Voraussetzungen der Verarbeitung der (personenbezogenen) Daten von Studierenden (§ 5). Hiernach dürfen Hochschulen die Angaben verarbeiten, die insbesondere für die Immatrikulation, die Rückmeldung, die Teilnahme an Lehrveranstaltungen, Prüfungen, die Nutzung von Hochschuleinrichtungen und für die Hochschulplanung erforderlich sind. Das für die Hochschulen zuständige Mitglied der Landesregierung kann durch Rechtsverordnung bestimmen, welche Daten für diese Zwecke verarbeitet werden dürfen.

Nach unserer Rechtsauffassung bedeutet dies, dass die Hochschulen erst mit dem Erlass einer konkretisierenden Rechtsverordnung befugt werden, die Daten der Studierenden zu verarbeiten. Das Gesetz selbst grenzt also

lediglich die Zwecke und Bereiche ein, für die die Regierung anstelle des Parlaments eine Regelung treffen darf, aufgrund derer ein Eingriff in die Rechte der Betroffenen erlaubt sein soll.

Das Ministerium für Wissenschaft, Forschung und Kultur vertritt demgegenüber die Auffassung, dass eine Rechtsverordnung zwar erlassen werden kann, dies aber nicht geschehen muss. Vielmehr genüge die in § 5 Satz 1 BbgHSG vorgenommene Aufzählung der Zwecke als Grundlage für die Datenverarbeitung der Brandenburgischen Hochschulen. Die Möglichkeit zum Erlass von Verordnungen sei für den Fall gedacht, dass der Gesetzgeber eine weitere Notwendigkeit der Zulässigkeit einer Datenverarbeitung übersehen hätte. In diesem Fall könnte flexibel ohne langwierige Gesetzgebungsverfahren durch den Erlass einer Rechtsverordnung reagiert werden, um auch in Zukunft bei veränderten Anforderungen eine rechtmäßige Datenverarbeitung im Hochschulbereich zu garantieren.

Dieser Ansatz verkennt jedoch, dass es immer noch Aufgabe des Parlaments ist, die Reichweite von Grundrechtseingriffen selbst zu bestimmen. Eine Ermächtigung der Exekutive zum Erlass einer Rechtsverordnung muss hinreichend konkret und begrenzt sein. Keinesfalls kann eine Befugnis zum Erlass einer Rechtsverordnung dazu dienen, künftige, zum Zeitpunkt der Verabschiedung des Gesetzes noch nicht erkannte Regelungsnotwendigkeiten auszufüllen. Die Ermächtigung zum Erlass von Rechtsverordnungen bedeutet gerade nicht den Verzicht auf gesetzgeberische Befugnisse.

Soweit für die Verarbeitung der Daten von Studierenden eine ausreichende Rechtsgrundlage besteht, ist der Einsatz von Chipkarten nach Maßgabe des § 5 Abs. 3 BbgDSG zulässig. Dabei hat die Hochschule sicherzustellen, dass die Datenverarbeitung (auch auf der Chipkarte) für den Betroffenen transparent verläuft und er seine Rechte (z. B. auf Berichtigung oder Löschung) mit vertretbarem Aufwand ausüben kann. Eine Verpflichtung zur Verwendung der Chipkarte setzt eine entsprechende Regelung in einer Rechtsvorschrift, etwa einer Hochschulsatzung, voraus.

Die zulässige Verarbeitung personenbezogener Daten durch brandenburgische Hochschulen bedarf einer Rechtsverordnung. Darüber hinaus bleibt es allein dem Gesetzgeber vorbehalten, festgestellte Gesetzeslücken zu schließen. Beim Einsatz von Chipkarten müssen die Betroffenen ihre Rechte in der gleichen Weise geltend machen können wie bei einem Verzicht auf diese Technik.

# 8 Arbeit, Soziales, Gesundheit und Frauen

## 8.1 Soziales

### 8.1.1 Interne Geltung des Sozialgeheimnisses bei Leistungsträgern

*In einer Landesbehörde hatten sich die zuständigen Leistungssachbearbeiter in einer Angelegenheit, die einen ihrer Kollegen betraf, für befangen erklärt. Über die Befangenheit sollte der Leiter der Behörde entscheiden.*

Das Erste Buch des Sozialgesetzbuches (SGB I) schreibt vor, dass die Sozialleistungsdaten der Beschäftigten und ihrer Angehörigen solchen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten an diesen Personenkreis weitergegeben werden dürfen. Hätte der Leiter der Behörde über die Befangenheit entschieden, hätte er zugleich auch Kenntnis über den Sozialleistungsantrag des Mitarbeiters und dessen nähere Gründe erhalten. Dem steht jedoch das Sozialgeheimnis entgegen.

Bereits früher[57] hatten wir auf verschiedene organisatorische Maßnahmen zum Schutz des Sozialgeheimnisses für Mitarbeiter des Sozialleistungsträgers hingewiesen. Der dargestellte Fall gibt Anlass, diese Hinweise zu ergänzen.

Über die Befangenheit hat grundsätzlich entweder der Behördenleiter oder ein von ihm Beauftragter zu entscheiden. Im geschilderten Fall darf der Leiter der Behörde wegen des Sozialgeheimnisses jedoch ausnahmsweise nicht mit der Entscheidung befasst werden. Diese muss vielmehr einem Beauftragten überlassen werden. Bei der Auswahl des Beauftragten ist darauf zu achten, dass dieser nicht zu dem Personenkreis zählt, der Personalentscheidungen trifft oder daran mitwirken kann.

[57] s. 6. Tätigkeitsbericht, Pkt. 7.1.2.1

Organisatorisch muss von Sozialleistungsträgern Vorsorge dafür getroffen werden, dass im Fall der Entscheidung über die Befangenheit der zuständigen Leistungssachbearbeiter das Sozialgeheimnis auch für Sozialdaten der Beschäftigten und ihrer Angehörigen gewahrt bleibt. Da das Sozialgesetzbuch den Behördenleiter bezüglich seiner Mitarbeiter von dieser Entscheidung ausschließt, muss für solche Fälle ein Beauftragter bestellt werden, der weder Personalentscheidungen trifft, noch an ihnen mitwirken kann.

### 8.1.2 Sozialhilfe

#### 8.1.2.1 Einsatz von Sozialhilfeermittlern

*Bei einer Hilfeempfängerin mit mehreren Kindern war ca. ein Vierteljahr lang durch einen sog. Sozialhilfeermittler die Überwachung des Wohnhauses und des umliegenden Parkraums erfolgt, um eine nicht eheliche Lebensgemeinschaft mit dem vermutlichen Vater des jüngsten Kindes nachzuweisen. Die Hilfeempfängerin hatte vor und während der Ermittlungen verschiedene Anträge gestellt und dazu teilweise Widerspruchsverfahren oder Verfahren auf einstweiligen Rechtsschutz eingeleitet, die letztlich alle erfolglos waren. Sie scheiterte dabei stets an Gründen, die nichts mit der vermuteten eheähnlichen Lebensgemeinschaft zu tun hatten. Eine nicht eheliche Partnerschaft konnte ihr trotz aller Ermittlungen des Sozialleistungsträgers nicht nachgewiesen werden. Dabei leitete die Behörde sogar Datenerhebungen über den potentiellen Lebensgefährten ein, die sowohl dessen Meldeanschrift als auch die von ihm benutzten Pkw‘s betrafen.*

Sozialdaten sind grundsätzlich beim Betroffenen selbst mit dessen Kenntnis - also offen und nicht verdeckt - zu erheben. Darüber hinaus ist darauf hinzuweisen, dass das Gesetz nur Halteranfragen zum Hilfeempfänger selbst, nicht aber über andere Personen oder zu einem bestimmten amtlichen Kennzeichen vorsieht.

Auch ist jemand, der nicht selbst Hilfeempfänger ist, grundsätzlich nicht verpflichtet, dem Sozialamt Auskunft über seine Lebenssituation zu erteilen. Ein möglicher nicht ehelicher Lebenspartner wird im Bundessozialhilfegesetz (BSHG) nicht unter den ausnahmsweise Auskunftspflichtigen genannt. Eine Zeugnispflicht nach dem SGB X scheidet für ihn ebenfalls aus, weil sie voraussetzt, dass die Aussage unabweisbar für die Entscheidung des Sozialamtes ist. Solange der Hilfeempfänger selbst über den Tatbestand der eheähnlichen Gemeinschaft ebenso gut Angaben machen kann und insoweit auch eine Mitwirkungspflicht hat, kann die Aussage des evtl. Lebensgefährten nicht als unabweisbar angesehen werden. Ohne seine Einwilligung durfte

keine Datenerhebung bei Dritten, wie z. B. bei der Meldebehörde, stattfinden. Allenfalls könnte durch eine Meldeanfrage geklärt werden, ob unter der Anschrift des Hilfeempfängers weitere Personen gemeldet sind.

Der Fall machte es eindrucksvoll deutlich, dass ein Auftrag an einen Sozialhilfeermittler zum Selbstläufer werden kann, wenn sich der Auftraggeber keine Rechenschaft darüber ablegt, für welches konkrete Verfahren die Ermittlungen erfolgen und ob sie überhaupt für seine Entscheidung notwendig sind. Außerdem fand nach dem Beginn der Ermittlungen auch keine laufende Prüfung statt, ob die Ermittlungen, die sich fast ein Vierteljahr hinzogen, überhaupt geeignet und noch erforderlich waren.

Wir konnten bei der Kontrolle des Sozialhilfeermittlers eines anderen Sozialleistungsträgers feststellen, dass dieser sich im Wesentlichen an unsere Empfehlungen hielt. Die Tätigkeit des Sachbearbeiters im Außendienst ist dort durch eine interne Dienstanweisung geregelt. Nach ihr besteht eine strenge Bindung des Sachbearbeiters im Außendienst an Prüfaufträge des jeweils zuständigen Sozialamtssachbearbeiters. Auf eigene Verantwortung unternimmt der Mitarbeiter im Außendienst keine Ermittlungen. Beim Fehlschlag von Ermittlungen entscheidet stets die Ansprechperson im Amt über das weitere Vorgehen. Datenerhebungen nimmt der Ermittler grundsätzlich nur beim Betroffenen selbst oder mit dessen Kenntnis vor. Anfragen bei Dritten unterbleiben in der Regel. Ebenso werden verdeckte Ermittlungen beim Betroffenen abgelehnt. Bei Datenabgleichen mit der Kfz-Meldestelle wird lediglich nach der Haltereigenschaft des Hilfeempfängers gefragt, wie es das BSHG zulässt. Der Sozialhilfeträger brachte zum Ausdruck, mit diesem datenschutzgerechten Verfahren zufrieden zu sein.
Es ist durchaus möglich, den Einsatz von Sozialhilfeermittlern so auszugestalten, dass er effektiv und datenschutzgerecht ist. Ermittlungen, die gegen Datenschutzvorschriften verstoßen und sich zudem als ungeeignete Maßnahme erweisen, sind nicht nur eine Verschwendung von Ressourcen, sondern auch rechtswidrig.

#### 8.1.2.2 Erschwerter Zugang zu den eigenen Sozialhilfedaten

*Ein Betroffener bemüht sich seit mehreren Jahren, Akteneinsicht in sowie Kopien aus seiner Sozialhilfeakte zu erhalten. Darüber hinaus stellte sich im Laufe unserer Ermittlungen heraus, dass die früher beteiligten Außendienstmitarbeiter außerhalb der Akten sog. Handbücher geführt hatten, die inzwischen jedoch vernichtet worden waren. Erst bei einer Akteneinsicht unter unserer Beteiligung wurde festgestellt, dass noch ein weiterer Vorgang existieren muss, der bereits ins öffentliche Archiv abgegeben worden war, obwohl er zeitlich nach Dokumentationen*

*entstanden war, die noch im Sozialamt aufbewahrt wurden. Das Sozialamt verweigerte zunächst ein Anfertigen von Kopien aus der Sozialhilfeakte unter Hinweis darauf, dass es keine Gebührenordnung gebe. Dies war verwunderlich, weil der Betroffene gerade bei einem anderen Amt der Behörde Kopien gegen Kostenersatz hatte herstellen können.*

Streng genommen kennt das Sozialgesetzbuch ein Akteneinsichtsrecht nur für Beteiligte an einem laufenden Verfahren, soweit diese die Kenntnis der Akten zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen benötigen. Jederzeit kann ein Betroffener demgegenüber Auskunft über die zu seiner Person gespeicherten Sozialdaten, deren Herkunft oder Empfänger und den Zweck der Speicherung verlangen. Das Sozialamt bestimmt dabei das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. So kann das Sozialamt statt der Auskunftserteilung auch eine Akteneinsicht gewähren oder dem Betroffenen Kopien aus dem Vorgang überlassen. Da die Vorschrift auch im Lichte des Grundrechts auf informationelle Selbstbestimmung zu sehen ist, muss es dem Wunsch des Betroffenen nachkommen, wenn es nicht gewichtige Gründe gegen die gewünschte Form der Auskunftserteilung vorbringen kann. Grundsätzlich hat ein Betroffener daher nicht nur jederzeit ein Recht auf Auskunftserteilung aus seiner Akte, sondern auch auf Einsichtnahme oder auf das Anfertigen von Kopien.

Das Sozialgesetzbuch sieht vor, dass ein Antragsteller die Daten, um die es ihm geht, näher bezeichnen soll. Wenn sie in Akten gespeichert sind, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen.

Ist infolge der unvollständigen Angaben des Betroffenen das Sozialamt nicht in der Lage, ihm die gewünschte Auskunft zu erteilen, so ist dies allein dem Verantwortungsbereich des Antragstellers zuzuweisen. Wird das Auffinden der Daten allerdings durch die Aktenführung des Sozialamtes selbst erschwert, so kann dies nicht gelten. So muss ein Betroffener nicht damit rechnen, dass das Sozialamt einzelne Angaben nicht zur Akte speichert, sondern diese in Handbüchern der Mitarbeiter aufbewahrt. Insoweit wird von einer Verwaltung erwartet, dass sie Notizen dann, wenn sie für den Vorgang relevant sind, zur Akte nimmt, oder sie anderenfalls unverzüglich vernichtet. Ein Aufbewahren nicht aktenrelevanter Notizen über einen längeren Zeitraum hinweg führt dazu, dass diese Notizen auch als Akten gelten. Sie sind daher bei Auskunftsbegehren des Betroffenen zu berücksichtigen und in sie ist

Einsicht zu gewähren[58].

Eine landesweite Umfrage zum Führen von Handbüchern bei Sozialämtern ergab, dass ca. bei jedem dritten Sozialhilfeträger zumindest die Außendienstmitarbeiter solche Handbücher verwandten. Wir haben den Behörden empfohlen, ihre Praxis umgehend zu ändern. Zum Teil wurde dem schon von einzelnen Sozialleistungsträgern entsprochen.

Das Fehlen einer Gebührensatzung kann nicht dazu führen, dass das Recht auf informationelle Selbstbestimmung beschränkt wird. Dieses Recht könnte sonst von der Verwaltung einfach dadurch ausgehebelt werden, dass sie für bestimmte Leistungen keine Gebührenregelungen trifft. Für die Auskunft an Betroffene ist ausdrücklich festgelegt, dass sie unentgeltlich erfolgt. Im Übrigen ist nach dem Sozialgesetzbuch grundsätzlich davon auszugehen, dass von Hilfeempfängern weder Gebühren noch Auslagen erhoben werden.

Das Sozialgesetzbuch nimmt vom Auskunftsanspruch Sozialdaten aus, die nur deshalb noch gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen. Selbstverständlich ist die Verwaltung aber jederzeit berechtigt, dem Betroffenen auch eine Akteneinsicht in archivierte Unterlagen zu gewähren. Solche archivierten Daten unterliegen ausnahmsweise dann einem Akteneinsichtsanspruch, wenn die Verwaltung das Recht auf informationelle Selbstbestimmung des Betroffenen zu einem Zeitpunkt unzulässigerweise beschränkt hat, zu dem eine Archivierung noch nicht erfolgt war.

Der Betroffene hat nach dem Sozialgesetzbuch grundsätzlich ein Recht darauf, seinem Wunsch entsprechend Akteneinsicht, Auskünfte oder Kopien zu ihn betreffenden Vorgängen kostenfrei zu erhalten. Das Fehlen einer Gebührensatzung darf nicht zu einer Beschränkung dieses Rechts führen.

Bei der Suche nach ihn interessierenden eigenen Sozialdaten hat der Betroffene die Behörde zu unterstützen. Zu vage Angaben oder Irrtümer des Antragstellers können sich dabei zu seinen Lasten auswirken.

Archivierte Unterlagen sind in der Regel dem Zugriff des Betroffenen entzogen. Es sei denn, die Behörde ist bereit, ihm auch solche Sozialdaten zu offenbaren, oder hat seine diesbezüglichen Rechte früher unzulässigerweise beschränkt.

[58] vgl. Pkt. A 8.3.1

### 8.1.3 Sozialversicherung

## Abrechnungsverfahren bei Schwangerschaftsabbrüchen

*Im Mai 1996 wurde zwischen dem Land Brandenburg und verschiedenen Landesverbänden von Krankenkassen eine Verwaltungsvereinbarung abgeschlossen, die das Verfahren der Kostenerstattung nach dem Gesetz zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen regelt. Darin war u. a. vorgesehen, dass die gesetzlichen Krankenkassen dem für die Kostenerstattung zuständigen Landesamt für Soziales und Versorgung die Kopien der Abrechnungsbelege der Krankenhäuser und Ärzte, auf deren Grundlage sie die Kosten verauslagt haben, übersenden.*

In anderen Bundesländern wird teilweise mit anonymisierten oder pseudonymisierten Daten abgerechnet. Trotz Nachfragen gab das Ministerium für Arbeit, Soziales, Gesundheit und Frauen uns dazu gegenüber zwei Jahre lang keine Stellungnahme ab. Wir nahmen daraufhin Mitte 1999 mit den Krankenkassen im Land Kontakt auf. Diese waren zum Teil bereit, in den Abrechnungen die Namen bis auf die Initialen zu schwärzen, sodass immerhin eine geringfügige Anonymisierung erreicht werden konnte. Eine gesetzliche Krankenversicherung teilte mit, dass sie noch bis vor kurzem eine fallbezogene Abrechnung, bei der lediglich die Krankenversicherungsnummer offenbart wurde, durchführen konnte, inzwischen aber vom Landesamt die Angabe des Namens, des Geburtsdatums und der Anschrift der Patientin verlangt werde.

Einige Krankenkassen waren bereit, mit dem Landesamt für Soziales und Versorgung in Verhandlungen einzutreten, wie sie ihre Abrechnungsqualität verbessern und insbesondere doppelte Bezahlungen vermeiden könnten, sodass für das Landesamt eine stärkere Anonymisierung des Kostenerstattungsverfahrens haushaltsrechtlich noch akzeptabel sein könnte. Mitte 2000 hat eine Krankenkasse eine Zusatzvereinbarung mit dem Land geschlossen. Nach dieser sind nur noch die Forderungsbuchnummer der Krankenkasse, ggf. eine Kennzeichnung von Nachberechnungen zum Fall, der Tag des Schwangerschaftsabbruchs, Postleitzahl und Wohnort der Betroffenen, ein Kennzeichen für stationäres oder ambulantes Verfahren, ein Kennzeichen für einen operativen oder medikamentösen Eingriff sowie der Erstattungsbetrag mitzuteilen. Dafür erhielt das Landesamt für Soziales und Versorgung ein Prüfrecht bei der Krankenkasse für die abgerechneten Fälle.

Es ist deutlich datenschutzgerechter, ein regelmäßiges Abrechnungsverfahren mit Pseudonymen durchzuführen und für Einzelfälle eine

Einsichtnahme in die Belege zu gewähren, als Kopien dieser Dokumente der anderen Stelle bei jeder Abrechnung personenbezogen zu übersenden.

## 8.2 Gesundheit

### 8.2.1 Gesundheitsämter: Einsatz von "Handbüchern"

*In einigen Gesundheitsämtern tragen einzelne Mitarbeiter beispielsweise des Sozialpsychiatrischen Dienstes personenbezogene Angaben über Patienten, die sie bei einem Beratungsgespräch am Telefon oder bei einem Hausbesuch erfahren, fortlaufend in ein gebundenes Notizbuch ein. Dementsprechend finden sich dort nacheinander zu verschiedenen Betroffenen personenbezogene Daten. In manchen Fällen begreifen die Mitarbeiter diese sog. Handbücher als ihr Privateigentum, in das niemand außer ihnen Einblick nehmen darf. In der Regel ist eine "Löschung" der Bücher erst dann vorgesehen, wenn das Buch vollgeschrieben ist oder der jeweilige Mitarbeiter seine Zuständigkeit für die bisherigen Aufgaben verliert. Die Löschung wird nicht davon abhängig gemacht, ob zu der Handbucheintragung eine Reinschrift für die jeweilige Akte gefertigt wird.*

Nach dem Brandenburgischen Datenschutzgesetz ist eine Akte jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht den Dateibegriff erfüllt. Nicht als Akten verstanden werden allerdings Vorentwürfe und Notizen, die nicht Bestandteil eines Vorganges werden sollen und alsbald vernichtet werden. Notizen, die über einen längeren Zeitraum aufbewahrt werden, sind damit als Teil der Akte zu begreifen. Mithin erstrecken sich Akteneinsichtsrechte der Betroffenen, Aufsichts- und Kontrollrechte von Vorgesetzten und Kontrollbehörden sowie die Aufforderungen der Gerichte, die gesamte Akte vorzulegen, auch auf diese Unterlagen. Vielen der genannten Stellen und Personen wird jedoch gar nicht bekannt sein, dass solche weiteren Aktenteile existieren, sodass sie ihre diesbezüglichen Rechte nicht ausüben können. Hinzu kommt, dass durch das fortlaufende Notieren personenbezogener Daten verschiedener Betroffener darauf geachtet werden müsste, jeweils nur die einen bestimmten Fall betreffenden Angaben offenzulegen. Dies bedeutet einen ziemlichen Aufwand, wenn es zu einer Anforderung der Akte und damit auch der Dokumentation aus dem Handbuch kommen sollte.

Darüber hinaus werden bei dieser Verfahrensweise die allgemeinen Löschungsvorschriften nicht eingehalten. Nach Anfertigen einer Reinschrift müsste die Notiz vernichtet werden, um eine doppelte Datenspeicherung zu vermeiden. Eine Löschung hätte aber auch dann zu erfolgen, wenn die An-

gaben im Handbuch als nicht relevant für den jeweiligen Vorgang beurteilt werden.

Ein Gesundheitsamt hat auf unsere Umfrage zu dieser Problematik hin sofort das weitere Führen der Handbücher untersagt. Für erforderliche Notizen werden dort Einzelblätter benutzt. Diese werden dann der Akte beigefügt oder nach einer Reinschrift vernichtet. Die bisherigen Handbücher sollen nach Fertigstellung der Akte noch im Jahr 2000 vernichtet werden.

Im Bereich des Sozialpsychiatrischen Dienstes kann es dazu kommen, dass ein Patient einen Mitarbeiter des Gesundheitsamtes nicht lediglich als Behördenvertreter, sondern als Vertrauensperson über bestimmte Lebenssachverhalte zu seiner Person informiert. Im Hinblick auf die besondere berufliche Schweigepflicht nach dem Strafgesetzbuch empfiehlt sich für solche persönlich anvertrauten Daten eine gesonderte Dokumentation. Diese kann z. B. in einem verschlossenen Umschlag bei der jeweiligen Patientenakte des Sozialpsychiatrischen Dienstes aufbewahrt werden. Auf Wunsch des Betroffenen könnte dann auch ein Vertreter des zuständigen Mitarbeiters diese Notizen zur Kenntnis nehmen.

Das fortlaufende Eintragen von personenbezogenen Notizen zu verschiedenen Betroffenen in ein einziges Handbuch des Sachbearbeiters erscheint auf den ersten Blick praktisch, wirft aber datenschutzrechtliche Probleme auf, die bei getrennten Einzelnotizen nicht bestehen.

### 8.2.2 Heilberufskammern: Auswahl von Teilnehmern an einer Arzneimittelstudie durch ein Call-Center

*Die Ethik-Kommission der Landesärztekammer Brandenburg hatte sich mit einem Studienantrag zu befassen, bei dem Patienten über Zeitungsanzeigen geworben werden sollten. Anschließend war eine Vor-Auswahl durch ein Call-Center mit Hilfe eines Fragebogens vorgesehen. Nach allgemeinen Fragen zur Eignung des Anrufers für die Studie sollten konkrete Fragen zur Erkrankung und ihrer Behandlung sowie nach der Identität des Betroffenen gestellt und ggf. ein Untersuchungstermin in einem der Studienzentren vereinbart werden. Entscheidet sich der Betroffene am Ende der Befragung gegen eine Teilnahme an der Untersuchung, werden die Unterlagen vernichtet.*

Wir kamen zu dem Ergebnis, dass der geplante Einsatz von Call-Centern für Arzneimittelstudien aus datenschutzrechtlichen Gründen nicht geeignet ist. Zum einen hat sowohl eine Einwilligungserklärung für die Teilnahme an der Studie und die damit verbundenen Dokumentationen und Datenflüsse nach dem Arzneimittelgesetz als auch nach dem Bundesdatenschutzgesetz schrift-

lich zu erfolgen. Gerade aus dem Vergleich mit der Vorschrift des Arzneimittelgesetzes geht hervor, dass im konkreten Fall auch keine Ausnahme vom Grundsatz der Schriftlichkeit nach dem Bundesdatenschutzgesetz gemacht werden kann. Die notwendige Voraussetzung der Wirksamkeit einer Einwilligungserklärung ist die vorherige Aufklärung des Betroffenen. Es war aber nicht ersichtlich, dass potentiellen Studienteilnehmern Hinweise in dieser Richtung zu Beginn der Befragung gegeben wurden. Auch ein datenschutzrechtlicher Hinweis erfolgte erst nach der Datenerhebung.

Der Aufbau des Fragebogens war an vielen Stellen problematisch. Bei vielen Fragen war es nicht nachvollziehbar, weshalb diese statt durch einen Prüfarzt, der einer besonderen Schweigepflicht unterliegt, bereits durch Mitarbeiter des Call-Centers erhoben werden sollten, zumal der Schutz der personenbezogenen Daten bei einem Telefonat auch noch deutlich geringer ist als bei einem persönlichen Gespräch.

Im Ergebnis wurde die Aufgabe des Call-Centers von dem Forschungsinstitut völlig verändert. Es soll nunmehr nur noch anrufenden Interessenten Anschriften von Prüfärzten in deren Nähe zur Verfügung stellen. Die Angaben des Betroffenen brauchen und dürfen vom Call-Center nicht dokumentiert werden. Die eigentliche Befragung führen nach der erforderlichen Aufklärung und schriftlichen Einwilligung die benannten Ärzte durch.

Es ist verständlich, dass für eine Arzneimittelstudie geeignete Probanden möglichst rasch und mit möglichst wenig Aufwand ausgewählt werden sollen. Dies darf jedoch nicht auf Kosten des Datenschutzes und des Schutzes von Patientengeheimnissen durch die ärztliche Schweigepflicht geschehen.

### 8.2.3 Landeskliniken: "Unabhängige Expertenkommission Maßregelvollzug"

*Nach der Flucht eines Sexualstraftäters aus dem Maßregelvollzug wollte das Ministerium für Arbeit, Soziales, Gesundheit und Frauen als Fachaufsichtsbehörde die Umstände, die die Entweichung ermöglicht hatten, untersuchen, aber auch generell organisatorische und strukturelle Abläufe in den betroffenen Einrichtungen überprüfen. Ziel war es, das Ministerium in die Lage zu versetzen, erforderliche Verbesserungen im Maßregelvollzug vorzunehmen. Hierzu wurde eine "Unabhängige Expertenkommission Maßregelvollzug" berufen, die aus zwei Landesbediensteten und zwei auswärtigen Mitgliedern besteht. Diese Kommission sollte selbst entscheiden, welche Unterlagen und Informationen sie benötigt, und wen sie zu ihrer Unterstützung heranzieht. Das Ministerium bat uns um eine Beurteilung der Frage, ob die Kommission Einsicht in Patientenakten nehmen darf.*

Eine Übermittlung der erforderlichen personenbezogenen Daten von den Landeskliniken an das Gesundheitsministerium zu Aufsichtszwecken halten wir für vertretbar. Allerdings ist eine eindeutige Klarstellung des Gesetzgebers zu den Grenzen der ärztlichen Schweigepflicht in diesem Zusammenhang zu befürworten.

Die Zulässigkeit einer Übermittlung zu Aufsichtszwecken an das Gesundheitsministerium bedeutet allerdings nicht, dass auch der von ihm eingesetzten Kommission dieselben Daten offenbart werden dürfen. Eine Vorschrift, die eine Übermittlung von Patientendaten an die Kommission ermöglichen würde, existiert genauso wenig wie ein Gesetz, in dem die Errichtung der Kommission überhaupt vorgesehen ist. Sie als bloße Verwaltungshelferin des Ministeriums zu betrachten, scheidet aus, weil die Kommission ihre Aufgaben gerade unabhängig von Weisungen wahrnehmen soll.

Patientendaten, bei denen über datenschutzrechtliche Vorschriften hinaus noch auf die besondere berufliche Schweigepflicht Rücksicht zu nehmen ist, dürfen der Kommission deshalb erst recht nicht offenbart werden. Ein Vergleich mit der im Brandenburgischen Psychisch-Kranken-Gesetz vorgesehenen Besuchskommission zeigt, dass selbst diese gesetzlich vorgesehene Stelle nur mit Einwilligung der Betroffenen in deren Patientenakten Einsicht nehmen kann. Soweit die Kommission mit anonymisierten Daten arbeiten kann, ist dies datenschutzrechtlich unproblematisch.

Es ist nachvollziehbar, dass das Ministerium bestrebt ist, wahrscheinlich bestehende Mängel im System des Maßregelvollzugs durch Hinzuziehung externer Experten untersuchen und Vorschläge zu ihrer Behebung machen zu lassen. Auch außerhalb Brandenburgs sind in jüngster Vergangenheit in ähnlichen Situationen wiederholt "Sonderermittler" damit beauftragt worden, problematische Vorgänge in der Verwaltung aufzuklären. Dies kann aber - soweit dabei personenbezogene Daten verwendet werden sollen - immer nur unter Beachtung des geltenden Datenschutzrechts geschehen.

Das Ministerium als Fachaufsichtsbehörde kann zur Wahrnehmung seiner Aufgaben die erforderlichen personenbezogenen Daten verarbeiten, indem es sich geeignete Beamte anderer Behörden abordnen lässt und ihnen zeitweise einen Dienstposten mit klarem Arbeitsauftrag und mit allen dienstrechtlichen Pflichten überträgt. Zumindest für die beiden Mitglieder der Expertenkommission, die Landesbedienstete sind, dürfte dies ein gangbarer Weg sein.

Das Ministerium hat uns mitgeteilt, ein Mitglied der Kommission sei ärztlicher Landesbediensteter im Geschäftsbereich des Ministeriums und werde die Patientenakten sichten, um den übrigen Kommissionsmitgliedern unter Wahrung der ärztlichen Schweigepflicht über seine Erkenntnisse zu möglichen organisatorischen und anderen Mängeln im System des Maßregelvollzuges und im Verfahren der Vollzugslockerungen zu berichten.

Ergänzend haben wir darauf hingewiesen, dass Bedienstete des Ministeriums oder Mitarbeiter in Einrichtungen, die zu einem möglichen eigenen Fehlverhalten befragt werden sollen, zuvor über die weitere Verwendung ihrer Angaben in einem späteren Disziplinarverfahren und darüber aufzuklären wären, dass sie die Aussage verweigern können.

Wir hatten bereits 1997 datenschutzrechtliche Verbesserungen im Psychisch-Kranken-Gesetz angeregt[59]. Dieser Fall sollte auch zum Anlass genommen werden, das Gesetz zu überarbeiten und um eine Vorschrift zu ergänzen, die nach dem Vorbild des Strafvollzugsgesetzes die Hinzuziehung externer Fachleute und ihre Ausstattung mit bestimmten Befugnissen ausdrücklich vorsieht.

Personenbezogene Daten dürfen nur von solchen Personen und Stellen verwendet werden, die aufgrund ihrer dienstlichen Stellung oder einer besonderen gesetzlichen Bestimmung dazu befugt sind. Das gilt auch bei der Untersuchung von Missständen in der Verwaltung.

# 9 Wirtschaft

## Geöffnete Post für Gewerbeämter

*Die zentrale Poststelle einer Stadtverwaltung öffnete die Post, die erkennbar an das Gewerbeamt der Stadt adressiert war und leitete diese im geöffneten Zustand an das Gewerbeamt weiter.*

Üblicherweise werden Posteingänge von der - zentralen - Poststelle geöffnet, sortiert, mit dem Eingangsstempel versehen und nach dem Geschäftsverteilungsplan auf die Abteilungen verteilt.

Gem. § 14 Abs. 5 Brandenburgisches Datenschutzgesetz (BbgDSG) dürfen personenbezogene Daten innerhalb einer öffentlichen Stelle nur weitergegeben werden, soweit dies der rechtmäßigen Erfüllung der Aufgaben

[59] s. 6. Tätigkeitsbericht, Pkt. 7.2.1.6

des Absenders oder des Empfängers dient (sog. Prinzip der informationellen Gewaltenteilung). Auch wenn man die zentrale Poststelle einer Stadtverwaltung als Teil des jeweiligen Fachamtes ansieht, an das die Post gerichtet ist, ist das Öffnen der Post streng genommen nur für die Registrierung der eingehenden Post nicht erforderlich. Hierzu wäre es auch ausreichend, den geschlossen Umschlag mit einem Eingangsstempel oder -vermerk zu versehen. Dieses - in einer anderen kreisfreien Stadt praktizierte - Verfahren ist zugleich das datenschutzfreundlichste. Wer sicherstellen will, dass stets so verfahren wird, kann das, indem er sein Schreiben persönlich an den Leiter des Gewerbeamtes (oder eines anderen Amtes) oder an den Sachbearbeiter adressiert.

Problematisch ist bei einer Öffnung in der zentralen Poststelle insbesondere, dass Post an Gewerbeämter auch sehr sensible Daten enthalten kann, die Ermittlungsverfahren betreffen oder dem Sozialgeheimnis unterliegen. In diesem Fall hat der Empfänger von Sozialdaten, hier das Gewerbeamt, diese nach § 78 Abs. 1 Zehntes Sozialgesetzbuch (SGB X) in gleicher Weise zu schützen wie die Stelle, von der er sie erhalten hat. Schon bei der behörden-internen Übermittlung muss die Kenntnisnahme Unbefugter daher durch den Einsatz von Verschlussmappen erschwert werden.

Soweit Bürgerinnen und Bürger ihre Schreiben persönlich an einen bestimmten Bediensteten (z. B. einen Amtsleiter) adressieren, sind die Schreiben ungeöffnet dem Adressaten zu übergeben. Ist das Schreiben an ein bestimmtes Amt (z. B. das Gewerbeamt) gerichtet, kann die Postverteilung datenschutzfreundlich so organisiert werden, dass auch dieses Schreiben ungeöffnet registriert und weitergeleitet wird. Bei einer Öffnung der nicht persönlich adressierten Eingänge durch die zentrale Poststelle ist sicherzustellen, dass die geöffneten Eingänge bei der internen Weiterverteilung nicht ohne Weiteres durch unbefugte Dritte zur Kenntnis genommen werden können. Das ist beispielsweise durch den Einsatz von Verschlussmappen zu gewährleisten.

## 10 Landwirtschaft, Umweltschutz und Raumordnung

### 10.1 Datenübermittlung zwischen Zweckverbänden

*Bürger sind häufig irritiert, wenn sie vermeintlich in ein und derselben Angelegenheit (Wasserver- und Abwasserentsorgung) Gebühren-bescheide von verschiedenen Zweckverbänden erhalten. Handelt es sich dabei um einen datenschutzrechtlichen Verstoß?*

In Brandenburg sind viele Zweckverbände nur entweder für die Trinkwasser- ver- oder die Abwasserentsorgung zuständig. Die Datenübermittlung zwischen den Zweckverbänden ist nach dem Brandenburgischen Datenschutzgesetz (§ 14) zulässig, soweit die rechtmäßige Aufgabenerfüllung des Empfängers sie erfordert. Der für die Abwasserentsorgung zuständige Zweckverband benötigt für die Gebührenerhebung Name, Adresse und Trinkwasserverbrauchsmengen. Die Trinkwasserverbrauchsmengen sind deshalb relevant, weil nach den Satzungen für die Abwassergebühren in der Regel der Frischwassermaßstab gilt. Die Entsorgungsgebühr wird nach der Schmutzwassermenge bemessen, die in die Grundstücksentwässerungsanlage gelangt und diese Menge wird anhand des entnommenen Frischwassers errechnet.

Die Zweckverbände sollten in ihre Gebührenbescheide einen Hinweis aufnehmen, woher und auf welcher Rechtsgrundlage sie die Verbrauchsdaten erhalten haben.

Zur rechtmäßigen Aufgabenerfüllung, insbesondere zur Errechnung der Entwässerungsgebühren, dürfen Zweckverbände nach § 14 BbgDSG die erforderlichen personenbezogenen Daten von Bürgern übermitteln. Eine entsprechender Hinweis in den Gebührenbescheiden ist zu empfehlen.

## 10.2 Zugang zu Umweltinformationen

*Eine Bürgerin bemühte sich vergeblich, Einsicht in umweltrelevante Unterlagen einer Kläranlage zu nehmen. Sie rief den Geschäftsführer des betreffenden Wasser- und Abwasserzweckverbandes an, der sie nach ihrer Legitimation befragte, eine mündliche Auskunft ablehnte und einen schriftlichen Antrag für erforderlich hielt. Der Anspruch auf freien Zugang zu Umweltinformationen war dem Zweckverband unbekannt.*

Nach dem Umweltinformationsgesetz hat jeder einen Anspruch auf freien Zugang zu Informationen über die Umwelt, ohne seine Identität bzw. sein Interesse nachweisen oder glaubhaft begründen zu müssen.

Das Verfahren nach dem Umweltinformationsgesetz ist ein Antragsverfahren; die Behörde muss auf einen Antrag hin tätig werden. Die Schriftform ist hier nicht erforderlich. Der Antrag kann schriftlich, telegrafisch, per Telefax, Fernschreiben, elektronisch, per Diskette, zur Niederschrift der Behörde, mündlich, telefonisch oder auf sonstige Weise gestellt werden. Er muss jedoch hinreichend bestimmt sein, d. h. die Behörde muss erkennen können, welche konkreten Informationen abgefragt werden sollen. Das Einsichtsbegehren ist innerhalb einer Frist von zwei Monaten zu bescheiden.

Der Europäische Gerichtshof hat den Zugang zu Umweltinformationen gestärkt, indem er mehrere Regelungen des deutschen Umweltinformationsgesetzes für nicht mit dem Gemeinschaftsrecht vereinbar hielt[60]. Die Bundesregierung hat nun einen Gesetzentwurf[61] vorgelegt, der die entsprechende Anpassung des Umweltinformationsgesetzes vorsieht.

Mitte des Jahres 2000 legte die Europäische Kommission zudem den Entwurf einer Richtlinie über den Zugang zu Umweltinformationen vor, die die Richtlinie über den freien Zugang zu Informationen über die Umwelt aus dem Jahre 1990 ersetzen soll. Der Umweltinformationszugang soll durch folgende Maßnahmen weiter erleichtert werden:

- die Bereitstellung von Umweltinformationen für eine breite Öffentlichkeit insbesondere mittels neuer Informationstechnologien,

- eine weitergefasste Definition des Behördenbegriffs,

- eine auf einen Monat verkürzte Frist für die Erteilung der beantragten Informationen,

- präzisere Bestimmungen über die Gebühren für die Bereitstellung von Informationen,

- ein bürgerfreundliches Rechtsbehelfsverfahren.

Informationsbegehren sind oft auf Umweltdaten gerichtet und deshalb nach dem Umweltinformationsgesetz zu prüfen. Das Recht auf Zugang zu Umweltinformationen wird aufgrund europäischer Vorgaben gegenwärtig erweitert.

# 11 Stadtentwicklung, Wohnen und Verkehr

## 11.1 Planfeststellungsverfahren Großflughafen Schönefeld - Weitergabe aller Einwendungen mit Personenbezug

*Das Brandenburgische Landesamt für Bauen, Verkehr und Straßenwesen hat im Rahmen des Planfeststellungsverfahrens als Anhörungsbehörde für das Vorhaben "Ausbau des Flughafens Berlin-Schönefeld" sämtliche Einwendungen in personenbezogener Form an die Vorhabenträgerin übermittelt. Darüber haben sich mehrere Bürgerinnen und Bürger bei uns beschwert. Außerdem hat das*

[60] vgl. Tätigkeitsbericht 1999, Pkt. A 10.1

[61] BR-Drs. 674/00 vom 10. November 2000

*Landesamt drei Unternehmen in anderen Bundesländern als Verwaltungshelfer mit der Abwicklung des Verfahrens beauftragt.*

Sinn und Zweck des Planfeststellungsverfahrens ist es, die gegen ein Vorhaben erhobenen Bedenken der Betroffenen soweit wie möglich auszuräumen und einen Ausgleich der öffentlichen und privaten Interessen zu erreichen. Zu den Aufgaben der Anhörungsbehörde gehört dabei, sämtliches für die Abwägung relevante Material zu sammeln - so auch die erhobenen Einwendungen der Bürgerinnen und Bürger -, sie zu bündeln und gemeinsam mit dem Vorhabenträger, den zuständigen Behörden, den Betroffenen und den Einwendern zu erörtern (§ 73 Abs. 6 Verwaltungsverfahrensgesetz). Dies geschieht im sog. Erörterungstermin.

Es ist durchaus nachvollziehbar, dass eine Anhörungsbehörde bestrebt ist, den mit solchen Großverfahren verbundenen erheblichen Aufwand weitgehend auf den Vorhabenträger abzuwälzen, der die Planfeststellung beantragt hat. Die Träger des Vorhabens "Flughafen Berlin-Brandenburg International" haben zu diesem Zweck eine eigene Gesellschaft, die "Flughafen Berlin-Schönefeld GmbH" gegründet, die den Erörterungstermin vorbereiten und dazu auch sämtliche Einwendungen sichten soll. Dies tut sie unabhängig von Weisungen der Behörde und damit nicht als deren Auftragnehmer im datenschutzrechtlichen Sinn. Das Landesamt für Bauen, Verkehr und Straßenwesen hat als Anhörungsbehörde dieses Verfahren in Anlehnung an vorangegangene Planungsverfahren für Großflughäfen im Bundesgebiet gewählt.

Dabei war zunächst durchaus zweifelhaft, ob das geltende Verwaltungsverfahrensrecht die ungeprüfte Übermittlung aller Einwendungen in personenbezogener Form an die Vorhabenträger zulässt. Zweifel sind aus Gründen des Datenschutzes insbesondere in den Fällen angebracht, in denen Einwender, die bei einem Vorhabenträger beschäftigt sind, geltend machen, dass eine vorhandene, aber noch nicht bekannte Erkrankung bei ihnen durch das Vorhaben verschlimmert werden könnte. Wären sie gezwungen, diesen Einwand personenbezogen dem Vorhabenträger bekannt zu geben, so müssten sie arbeitsrechtliche Nachteile bis hin zur Kündigung befürchten. Andererseits könnte sie dieser Offenbarungszugang davon abhalten, berechtigte Einwendungen im Planfeststellungsverfahren zu erheben, was auch die Qualität des Abwägungsergebnisses beeinträchtigen könnte.

Zur Frage, inwieweit personenbezogene Daten der Einwender an Vorhaben-

träger weitergegeben werden dürfen[62], liegt inzwischen eine Entscheidung des Bundesverwaltungsgerichts vor[63]. Im Regelfall hat danach eine Übermittlung der Einwendungen in personenbezogener Form zu erfolgen. Nach Auffassung des Bundesverwaltungsgerichts ist das Planfeststellungsverfahren mit einem gerichtlichen Verfahren zu vergleichen, sodass der Vorhabenträger nach dem Grundsatz des rechtlichen Gehörs prinzipiell Anspruch auf vollständige Kenntnis der Einwendungen habe. Gleichwohl hält das Gericht Fälle für denkbar, in denen ein Einwender darlegen kann, " ... dass ihm durch die Weitergabe seiner nicht anonymisierten Einwendungen besondere und unzumutbare und mithin von der Funktion des Anhörungsverfahrens nicht mehr gedeckte Nachteile entstehen, die es gebieten, das Verfahrens- und Rechtsverfolgungsinteresse der Vorhabenträgerin ausnahmsweise hinter dem Recht auf informationelle Selbstbestimmung zurücktreten zu lassen"[64]. Dazu zählt insbesondere der geschilderte Fall, dass ein Arbeitnehmer nicht gezwungen werden darf, Einwendungen aufgrund seines Gesundheitszustandes gegen ein Vorhaben seines Arbeitgebers in personenbezogener Form zu machen.

Daher war die ungeprüfte, pauschale Übermittlung von Einwendungen, die personenbezogene Daten beinhalten, nicht zulässig, da stets untersucht werden muss, ob besondere von den Einwendern vorgebrachte Einzelfallumstände vorliegen, die eine Anonymisierung erforderlich machen.

Dessen ungeachtet lehnte das Brandenburgische Landesamt für Bauen, Verkehr und Straßenwesen eine Einzelfallprüfung unter Hinweis auf die praktischen Probleme eines Massenverfahrens generell ab. Es übermittelte alle vorgebrachten Einwendungen ohne vorherige Prüfung in personenbezogener Form an die Flughafen Berlin-Schönefeld GmbH als Tochtergesellschaft der Vorhabenträger.

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dies gegenüber dem Ministerium für Stadtentwicklung, Wohnen und Verkehr förmlich beanstandet.

Das Ministerium hat aufgrund unserer Beanstandung und der damit verbundenen Empfehlungen für einen datenschutzgerechten Umgang mit den Einwendungen in der Zukunft die Planungsgesellschaft "Flughafen Berlin-Schönefeld GmbH" zu der Zusicherung veranlasst, dass personenbezogene Einwendungen nur den mit den Ausbauvorhaben befassten

---

[62] s. Tätigkeitsbericht 1998, Pkt. A 10.1.1

[63] Beschluss v. 14.08.2000 - 11 VR 10.00 -

[64] Beschluss vom 14. August 2000, BVerwG 11 VR 10.00

Personen zugänglich gemacht und nicht dem Personalbereich, der Geschäftsleitung oder anderen Gesellschaften der "Berlin-Brandenburg Flughafen Holding GmbH" zur Kenntnis gegeben werden. Durch diese Verpflichtung zur abgeschotteten Bearbeitung der Einwendungen und zu deren Löschung bei Rücknahme oder nach Abschluss des Verfahrens kann der festgestellte erhebliche datenschutzrechtliche Mangel zwar nicht behoben, aber in seinen praktischen Auswirkungen doch weitgehend ausgeglichen werden. Es wird zu überprüfen sein, ob die Einwendungen im weiteren Verlauf des Planfeststellungsverfahrens entsprechend diesen Zusicherungen datenschutzgerecht verarbeitet werden.

Gegen die - datenschutzrechtlich mögliche - Beauftragung von drei Unternehmen als Verwaltungshelfer bestanden im Ergebnis keine Bedenken, nachdem sichergestellt war, dass diese der Kontrolle durch die örtlich zuständigen Aufsichtsbehörden, die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen und das Innenministerium Baden-Württemberg unterliegen.

Im Planfeststellungsverfahren ist die personenbezogene Weitergabe von Einwenderdaten an die Vorhabenträger grundsätzlich zulässig. Es bedarf dabei aber einer Prüfung, ob im Einzelfall Einwendungen geltend gemacht wurden, die aufgrund der besonderen Situation der Einwender nur anonymisiert weitergegeben werden dürfen.

## 11.2 Planfeststellungsverfahren - Auslegung des Plans mit Namen und Adressen der Grundstückseigentümer

*Ein Petent fand seinen Namen und die vollständige Adresse in den Plänen für den Ausbau einer Bundesstraße, die zur Durchführung des Anhörungsverfahrens im Rahmen des Planfeststellungsverfahren öffentlich auslagen. Zur besseren Zuordnung der betroffenen Grundstücke hat die Anhörungsbehörde zudem die Grunderwerbsverzeichnisse ausgelegt.*

Die Auslegung des Plans im Rahmen des Planfeststellungsverfahrens dient vorrangig der Information der Betroffenen über den Umfang des Vorhabens. Ob die Eigentümerdaten zulässig offenbart werden, bedarf der Ermessensausübung durch die Behörde (§ 73 Abs. 1 S. 3 Verwaltungsverfahrensgesetz -VwVfG). Diese muss dabei berücksichtigen, dass die Planauslegung grundsätzlich ohne personenbezogene Daten Dritter zu erfolgen hat. In Fällen, in denen die Zuordnung der Grundstücke nur sehr schwer möglich ist, kann die Angabe des Namens und der Anschrift der Eigentümer der betroffenen Grundstücke jedoch zulässig sein. Das gilt beispielsweise, wenn ein Grundstück aufgrund seiner Abgelegenheit

(außerhalb geschlossener Ortschaften) nicht eindeutig bestimmt werden kann. Auf diese Auslegung des Verwaltungsverfahrensrechts hatten wir uns bereits 1997 mit dem zuständigen Ministerium verständigt[65].

Bei den Planungen zum Ausbau des Flughafens Berlin-Schönefeld haben die zuständigen Behörden auf die Nennung der Eigentümerdaten insgesamt verzichtet und sie nur verschlüsselt ausgelegt. Das ist zu begrüßen.

In dem geschilderten Fall wurden jedoch alle Eigentümerdaten sehr weitgehend veröffentlicht. Die Anhörungsbehörde nannte Namen und Anschrift der Eigentümer sämtlicher vom Vorhaben betroffenen Grundstücke, ohne für jedes Grundstück jeweils die Erforderlichkeit zu prüfen.

Das Ministerium für Stadtentwicklung, Wohnen und Verkehr hat uns zugesichert, die nachgeordneten Behörden auf die notwendige restriktive Handhabung bei der Auslegung von Eigentümerdaten hinzuweisen.

Grundsätzlich hat die Planauslegung ohne personenbezogene Daten der Grundstückseigentümer zu erfolgen. Lediglich in Ausnahmefällen ist die Nennung ihrer Namen und Anschriften zulässig. Dies gilt aber nur für einzelne Grundstücke und nicht pauschal für ein gesamtes Planungsvorhaben.

## 11.3 Knöllchen von freiberuflichen "Outsideworkerinnen"

*Unter der Überschrift "Jagdszenen um Falschparker in Brandenburg" hat eine Zeitung über die in einem Amt geübte Praxis berichtet, Parkverstöße von freiberuflichen - also privaten - sog. "Outsideworkerinnen" feststellen zu lassen. Dem Landkreis war die Privatisierung bereits Anfang des vergangenen Jahres durch eine Rechnungsprüfung bekannt geworden. Das Amt ist jedoch den seinerzeitigen Aufforderungen der Kommunalaufsicht, die Praxis zu beenden, zunächst nicht nachgekommen. Auch wir haben gefordert, die private Form der Parkverstoßahndung einzustellen.*

Rechtsgrundlage für die Verfolgung von Verstößen im ruhenden Verkehr ist das Ordnungswidrigkeitenrecht. Als hoheitliche Aufgabe kann sie gem. Art. 33 Abs. 4 Grundgesetz nicht ohne Weiteres auf Private übertragen werden. Für den erforderlichen Beleihungsakt bedarf es einer Rechtsgrundlage. Ein entsprechender Änderungsvorschlag des einschlägigen § 26 Abs. 2 Straßenverkehrsgesetz (StVG) fand wegen verfassungsrechtlicher Bedenken 1996 auf Bundesebene keine Mehrheit.

---

[65] s. 6. Tätigkeitsbericht, Pkt. 2.2

Somit gilt nach wie vor, dass die Überwachung des ruhenden Verkehrs als hoheitliche Tätigkeit nach § 26 Abs. 1 StVG der Polizei bzw. den von der Landesregierung bestimmten Behörden zugewiesen ist. Nach § 1 Abs. 1 der Verordnung zur Bestimmung der für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständigen Verwaltungsbehörden (Verkehrsordnungswidrigkeitenzuständigkeitsverordnung - VOwiZustV GVBl. 1994 S. 74) obliegt die Verfolgung und Ahndung von Parkverstößen den örtlichen Ordnungsbehörden, die ihre Zuständigkeit nur selbst ausüben können.

Das Amt hat mitgeteilt, dass es das Verfahren unterdessen eingestellt hat und Parkverstöße nur noch von fest angestellten Ordnungskräften verfolgen lassen will. Allerdings hat es auch angekündigt, in einem Modellversuch "ausloten" zu wollen, ob und wie sich mittels digitaler Fotografien die Beweissicherung vollständig von hoheitlichen Aufgaben abkoppeln lasse. Dabei wird zu berücksichtigen sein, dass schon die Beweissicherung zu der hoheitlichen Aufgabe der Verfolgung von Ordnungswidrigkeiten gehört.

Die Beauftragung Privater mit der Verfolgung und Ahndung von Ordnungswidrigkeiten im ruhenden Straßenverkehr ist mangels einer gesetzlichen Ermächtigung rechtswidrig. Das gilt für das gesamte Verfahren von der Feststellung eines falsch geparkten Autos bis zum Abschluss des Bußgeldverfahrens gegen den Halter.

# 12 Finanzen

## 12.1 Zentrale Fördermitteldatenbank für das Land Brandenburg

*Für bessere Entscheidungsgrundlagen von Legislative und Exekutive sowie bessere interne und externe Kontrollmöglichkeiten soll eine zentrale, beim Ministerium der Finanzen eingerichtete Förderdatenbank sorgen, in der landesweit alle Daten über Förderprogramme und geförderte Projekte registriert werden. Derzeit ist noch offen, ob die Daten anonym oder personenbezogen verarbeitet werden sollen.*

Rechtsgrundlage für die Errichtung dieser Fördermitteldatenbank ist Art. 18 Abs. 3 Buchst. e) der Verordnung (EG) Nr. 1260/1999 des Rates vom 21. Juni 1999 mit allgemeinen Bestimmungen über die Strukturform, wonach ein computergestützter Austausch der zur Erfüllung der Verwaltungs-, Begleitungs- und Bewertungsanforderungen dieser Verordnung notwendigen Daten vorgesehen ist. Das Verarbeiten personenbezogener Daten ist nach unserem Dafürhalten hier nicht notwendig. Art. 34 Abs. 1 Buchst. a) kann dabei nicht als Rechtsgrundlage für eine personenbezogene Datenerhebung herangezogen werden. Der Verordnungsgeber spricht hier von der Errichtung

eines Systems für die Erfassung zuverlässiger finanzieller und statistischer - also anonymisierter - Daten.

Die Fördermittelvergabe selbst ist dagegen stets auch eine Verarbeitung personenbezogener Daten, also ein Eingriff in das Recht auf informationelle Selbstbestimmung des Antragstellers, der einer gesetzlichen Grundlage bedarf. Die zitierte EU-Verordnung entspricht nicht den Erfordernissen einer normenklaren Regelung.

Soweit personenbezogene Daten in der zentralen Förderdatenbank verarbeitet werden sollen, bedarf dies einer gesetzlichen Grundlage. Eine solche ist im EU-Recht derzeit nicht vorhanden.

## 12.2 Umfang der Auskunftspflicht der Finanzbehörden nach § 21 Abs. 4 SGB X

*Es kommt immer wieder vor, dass Träger von Sozialhilfe zur Prüfung von Unterhaltsansprüchen die Finanzämter um Übersendung von Einkommenssteuererklärungen und -bescheiden von Unterhaltspflichtigen im Rahmen von § 116 Bundessozialhilfegesetz (BSHG) i. V. m. § 21 Abs. 4 Zehntes Buch Sozialgesetzbuch (SGB X) bitten.*

*In einem uns vorgelegten Fall kam das Finanzamt diesem Ersuchen insoweit nach, als dem Träger der Sozialhilfe die Höhe der gewerblichen sowie anderer Einkünfte und anerkannter Sonderausgaben mitgeteilt wurde. Die vollständige Übersendung der gewünschten Unterlagen lehnte es jedoch mit der Begründung ab, dass sich aus den Steuererklärungen und Steuerbescheiden Angaben unbeteiligter Dritter ergeben können. Das Finanzamt war der Ansicht, gem. § 30 Abgabenordnung (AO) zur Offenbarung der geschützten Verhältnisse befugt, jedoch nicht verpflichtet zu sein.*

Die Pflicht zur Auskunftserteilung ergibt sich aus § 116 BSHG i. V. m. § 21 Abs. 4 SGB X . Die Finanzbehörde ist nur dann zu einer Auskunft verpflichtet, soweit dies im Verfahren nach dem Sozialgesetzbuch erforderlich ist. Erforderlich ist die Einholung einer Auskunft der Finanzbehörde jedoch erst, wenn die erbetenen Angaben nicht mit Hilfe der nach dem Sozialgesetzbuch auskunftspflichtigen Personen festgestellt werden können (vgl. § 67 Abs.2 SGB X und §§ 60 ff. SGB I).

Nach § 116 BSHG sind die Unterhaltspflichtigen verpflichtet, dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben, soweit die Durchführung des Bundessozialhilfegesetzes es erfordert. Soweit der unterhaltsrechtliche Auskunftsanspruch nach bürgerlichem Recht

gem. § 91 Abs. 1 Satz 1 Bundessozialhilfegesetz (BSHG) auf den Träger der Sozialhilfe übergeht, richtet er sich nach §§ 1605 Bürgerliches Gesetzbuch (BGB) und 116 BSHG. Der Einkommenssteuerbescheid und der Vorauszahlungsbescheid weisen bei Einkünften aus Gewerbebetrieb und selbständiger Arbeit die Einnahmen für sich genommen noch nicht aus. Geschuldet wird eine systematische Aufstellung von Einkünften und Vermögen. Bei selbständigen Unternehmen müssen durch Aufschlüsselung von Einnahmen und Ausgaben die Einkommens- und Vermögensverhältnisse über einen längeren Zeitraum belegt werden, die mit einer Bilanz- bzw. Gewinn- und Verlustrechnung mit Erläuterung der einzelnen Titel vorzulegen sind.

Um eine weitgehende inhaltliche Übereinstimmung mit dem unterhaltsrechtlichen Auskunftsanspruch gem. § 1605 BGB herzustellen, ist in § 116 BSHG eine Verpflichtung zur Vorlage von Beweisurkunden eingefügt worden. Die Einkommenssteuererklärungen sowie -bescheide dürfen nur dann vollständig verlangt werden, wenn auch der gesamte Inhalt für die Unterhaltsberechnung erforderlich ist.

Eine Finanzbehörde ist verpflichtet, dem Träger der Sozialhilfe im Rahmen der Auskunftserteilung Steuererklärungen und Steuerbescheide eines Unterhaltspflichtigen vorzulegen. Soweit nicht alle in der Steuererklärung gemachten Angaben für die Unterhaltsberechnung erforderlich sind, sind diese in geeigneter Weise unkenntlich zu machen.

## 12.3 Elektronische Steuererklärung ELSTER

*Seit Mitte des Jahres 1999 ist es auch im Land Brandenburg möglich, die Steuererklärung elektronisch an das zuständige Finanzamt zu übermitteln. Mit der **EL**ektronischen **ST**eu**ER**erklärung (ELSTER)[66] sollen die Weichen für eine zukunftsorientierte, später papierlose Steuerverwaltung gestellt werden. Der Steuerpflichtige kann seine Daten direkt vom eigenen PC an die Großrechenzentren der Finanzämter senden.*

In den Steuersoftwarepaketen muss das so genannte Tele-Modul von ELSTER integriert sein. Nachdem der Bürger oder auch der Steuerberater die erhebungswichtigen Daten eingegeben hat, kann er sie elektronisch an das zuständige Finanzamt schicken. Die Steuererklärung wird dann zunächst an die Clearingstelle in München, die von der dortigen Finanzverwaltung betrieben wird, übermittelt. Das Rechenzentrum in der Oberfinanzdirektion (OFD) Cottbus fragt täglich über das "ELSTER-Control-Center (ECC)" den

[66] http://www.elster.de

Server in München nach neu eingegangenen Steuererklärungen ab.

Für den Versand über das Internet werden die Daten über das Tele-Modul mit dem öffentlichen Schlüssel des jeweiligen Bundeslandes verschlüsselt. ELSTER verwendet hierzu ein Hybridverfahren aus 3-DES-(112 Bit Schlüssellänge) und RSA-(1024 Bit Schlüssellänge) Schlüsseln. Nach der Übertragung der verschlüsselten Steuererklärungen an die OFD wird die externe Verbindung getrennt, die Daten über eine Firewall auf einen weiteren ECC-Rechner übertragen und dort mit dem privaten Schlüssel entschlüsselt, auf Viren geprüft und im Festsetzungsspeicher der OFD abgelegt.
Bis zur Einführung einer rechtsverbindlichen elektronischen Signatur muss der Steuerpflichtige jedoch wie bisher seine Unterlagen eigenhändig unterschrieben beim zuständigen Finanzamt einreichen. Es genügt allerdings eine komprimierte Steuererklärung, die von der Steuersoftware erzeugt wird. Dabei werden nur die tatsächlich belegten Datenfelder ausgedruckt.

Die elektronische Steuererklärung erleichtert nur den Finanzämtern die Arbeit, da die Mitarbeiterinnen und Mitarbeiter die Daten nicht mehr manuell eingeben müssen. Im Jahr 2000 sind allein in Brandenburg ca. 13.000 elektronische Steuererklärungen eingegangen.

Eine erste Überprüfung des Projekts im Rechenzentrum der OFD Cottbus hat ergeben, dass ELSTER gegenwärtig ein hinreichendes Maß an Vertraulichkeit gewährleistet.

Das Projekt ELSTER gewährleistet in der gegenwärtigen Entwicklungsphase ein hinreichendes Maß an Vertraulichkeit.

## Teil B

## Akteneinsicht und Informationszugang

Drei Jahre nach In-Kraft-Treten des Akteneinsichts- und Informationszugangsgesetzes in Brandenburg gibt es auf europäischer Ebene sowie in Bund und Ländern verstärkte Bestrebungen, den voraussetzungslosen Zugang zu amtlichen Unterlagen zu ermöglichen. Die praktischen Erfahrungen mit dem Akteneinsichts- und Informationszugangsgesetz und die in zunehmender Zahl eingehenden Bürgerbeschwerden sind die Grundlage für eine erste Evaluation des Gesetzes durch den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht.

### 1 Entwicklung des Informationszugangsrechts

### 1.1 Europa

Das Zugangsrecht aller natürlichen oder juristischen Person mit Wohnsitz oder Niederlassung in einem Mitgliedsstaat in der Union zu Dokumenten der Institutionen der Europäischen Union (Parlament, Rat und Kommission) ist verbindlich bereits in Artikel 255 des Vertrages von Amsterdam garantiert. Auch wenn die auf dem Gipfel in Nizza proklamierte Grundrechtecharta der Europäischen Union bisher nicht verbindlich ist, bleibt es doch bemerkenswert, dass das Recht auf Zugang zu Dokumenten der Europäischen Institutionen in dieser möglichen Basis einer späteren Europäischen Verfassung ausdrücklich verankert worden ist (Artikel 42).

Allerdings bedarf das Grundrecht auf Informationszugang noch einer Umsetzung durch eine Verordnung des Rates, die nach dem Vertrag von Amsterdam bis zum 1. Mai 2001 ergehen soll. In diesem Punkt haben sich die Mitgliedsstaaten der Europäischen Union allerdings bisher nicht auf eine entsprechende Verordnung einigen können. Im Gegenteil: Der Rat hat am 14. August 2000 entgegen früheren Entscheidungen den Zugang der Öffentlichkeit zu Ratsdokumenten deutlich eingeschränkt. Danach bleiben nicht nur als geheimhaltungsbedürftig klassifizierte Dokumente unter Verschluss, sondern auch solche Ratsdokumente aus dem Bereich des nicht-militärischen Krisenmanagements, die einen Rückschluss auf den Inhalt von geheimhaltungsbedürftigen Unterlagen zulassen. Derartige Dokumente dürfen nicht einmal in das öffentliche Register der Ratsdokumente aufgenommen werden. Damit wird die Geheimhaltung über den militärischen Bereich hinaus auch auf Angelegenheiten der gemeinsamen Außen- und Sicherheitspolitik erstreckt.

Insgesamt machen die langwierigen Verhandlungen über die Informationszugangsverordnung der Europäischen Union deutlich, dass die Entwicklung zu mehr Transparenz auch von Rückschlägen gekennzeichnet ist, zumal die Geheimhaltungsinteressen der Mitgliedstaaten nach wie vor dominant sind.

### 1.2 Bundesrepublik Deutschland

In der Bundesrepublik gewinnt die vom Brandenburgischen Akteneinsichts- und Informationszugangsgesetz ausgelöste Entwicklung zu mehr Verwaltungstransparenz zunehmend an Dynamik. Im Berichtszeitraum ist bereits in einem dritten Bundesland (nach Brandenburg und Berlin), nämlich in Schleswig-Holstein, ein Gesetz über die Freiheit des Zugangs zu Informationen in Kraft getreten. In drei weiteren Bundesländern, in Hessen, Nordrhein-Westfalen und Sachsen, sind entsprechende Gesetzentwürfe in die Landtage eingebracht worden. Daneben ist damit zu rechnen, dass die Bundesregierung im Frühjahr 2001 den Entwurf für ein Informationsfreiheitsgesetz des Bundes vorlegen wird. Ihr ursprüngliches Vorhaben, durch Bundesgesetz auch den Zugang zu amtlichen Unterlagen bei den Behörden der Länder, die zum großen Teil Bundesrecht auszuführen haben, zu regeln, hat sie angesichts des Widerstandes der Länder nicht weiter verfolgt. Dennoch würde ein Bundesgesetz, selbst wenn es ausschließlich für die Bundesverwaltung gelten würde, zweifellos eine zusätzliche Signalwirkung auch für die noch zögernden Länder entwickeln.

Insgesamt beginnt sich damit der Grundsatz des freien und nicht begründungsbedürftigen Zugangs zu amtlichen Unterlagen in Deutschland immer mehr durchzusetzen. Dazu hat Brandenburg den Anstoß gegeben.

## 2 Umsetzung des Akteneinsichts- und Informationszugangsrechts

### 2.1 Dienstanweisungen zur Akteneinsicht - Orientierung für Behörden

*Verwaltungsinterne Richtlinien zur Anwendung des Akteneinsichts- und Informationszugangsgesetzes (AIG) können die Bearbeitung der Anträge erleichtern, vereinheitlichen und dadurch für den Antragsteller beschleunigen. Einige der von uns geprüften Dienstanweisungen enthalten lediglich eine Zuständigkeitsregelung für die Bearbeitung von Anträgen auf Akteneinsicht; andere hingegen befassen sich ausführlicher mit inhaltlichen Fragen.*

Eine Verwaltung, die sich entscheidet, den Umgang mit der Akteneinsicht

intern zu regeln, sollte bei der Festlegung der Zuständigkeiten die behördliche Ansprechperson für Akteneinsicht bzw. die/den behördliche/n Datenschutzbeauftragten einbeziehen. Des Weiteren sollten möglichst kurze Bearbeitungsfristen festgelegt sowie auf die verschiedenen für eine Akteneinsicht in Frage kommenden Anspruchsgrundlagen (neben dem Akteneinsichts- und Informationszugangsgesetz beispielsweise das Brandenburgische Datenschutzgesetz, das Verwaltungsverfahrens- oder das Umweltinformationsgesetz) hingewiesen werden. Der Umgang mit personenbezogenen Daten in einer Akte kann durch entsprechende Erläuterungen[67] erleichtert werden. Neben den Bestimmungen zur Aussonderung schutzbedürftiger Daten sind auch die Gebührenregelungen von Bedeutung.

Um die Bemühungen einiger der von uns befragten Landkreise sowie anderer Behörden, die auf uns zugekommen sind, zu unterstützen, haben wir Hinweise zur Erstellung einer internen Dienstanweisung zur Anwendung des Akteneinsichts- und Informationszugangsgesetzes zusammengestellt, die wir in unserem Internetangebot ständig aktualisieren.

Insbesondere größeren Behörden sowie Stellen, bei denen häufig Akteneinsicht beantragt wird, ist zu empfehlen, interne Dienstanweisungen zum Umgang mit dem AIG zu erlassen. Hinweise zur Erstellung solcher Vorschriften sind der Anlage 3 oder unserer Website zu entnehmen. Der Landesbeauftragte steht für eine weitergehende Beratung gerne zur Verfügung.

## 2.2 Personenbezogene Daten bei Anträgen auf Akteneinsicht schützen - aber wie?

*Das Akteneinsichts- und Informationszugangsgesetz schützt personenbezogene Daten in der Regel vor der Einsicht durch Dritte. Es ist zu entscheiden, wie mit diesen Angaben umzugehen ist, unter welchen Umständen sie offen gelegt werden können und wie ein Antragsteller die begehrten Informationen erhält, ohne dass dadurch unzulässigerweise in die Schutzrechte Dritter eingegriffen wird.*

Man kann die personenbezogenen Daten in drei verschiedene Kategorien einteilen: Daten aus allgemein zugänglichen Quellen haben in der Regel den niedrigsten Schutzbedarf. Sie können nach Anhörung des Betroffenen offenbart werden. Handelt es sich um nicht allgemeine zugängliche Informationen, an deren Geheimhaltung der Betroffene aber möglicherweise ein geringeres Interesse hat als der ein politisches Mitgestaltungsinteresse geltend machende Antragsteller an der Offenbarung, so ist der Antragsteller

[67] s. auch B 2.2

aufzufordern, sein Offenbarungsinteresse darzulegen. Nach der Anhörung des Betroffenen und anschließenden Abwägung beider Interessen kann auch hier eine Akteneinsicht erfolgen, wenn das Offenbarungsinteresse überwiegt. Bei Daten, die die eben genannten Kriterien nicht erfüllen, kommt eine Gewährung der Akteneinsicht nur in Frage, wenn der Betroffene ihr zustimmt.

In der Praxis werden die beiden Verfahren "Anhörung des Betroffenen" und "Einholung seiner Zustimmung" häufig verwechselt. Der grundsätzliche Unterschied besteht darin, dass bei der Anhörung letztendlich die Entscheidung, ob Einsicht gewährt wird, von der Behörde zu treffen ist. Sie bittet den Betroffenen von sich aus um eine Stellungnahme und prüft die vorgebrachten Argumente. Im Ergebnis kann sie also auch bei einer Ablehnung durch den Betroffenen die Akte zur Einsicht freigeben.

Ist dagegen die Zustimmung erforderlich, kann die Behörde Informationen nicht offen legen, wenn der Betroffene sie verweigert bzw. innerhalb von zwei Monaten nicht reagiert. Auf Verlangen des Antragstellers ist sie jedoch von der Behörde einzuholen. Der Antragsteller sollte auf diese Möglichkeit hingewiesen werden.

Wird schließlich der Antrag auf Akteneinsicht beschieden, handelt es sich um einen Verwaltungsakt mit Doppelwirkung. Gewährt die Behörde Akteneinsicht, begünstigt sie den Antragsteller, belastet aber gleichzeitig den Betroffenen, dessen Daten offenbart werden. Der Verwaltungsakt ist deswegen dem Betroffenen zuzustellen, der ihn mit Widerspruch und Klage anfechten kann.

Kommt die Einsichtnahme in personenbezogene Daten nicht in Frage, sind diese Informationen so weit wie möglich, z. B. durch Schwärzung, auszusondern. Die Tatsache, dass ein Dokument geheimhaltungsbedürftige personenbezogene Daten enthält, rechtfertigt nicht die vollständige Verweigerung der Einsicht. Nur in Ausnahmefällen, in denen eine Aussonderung unverhältnismäßig aufwändig wäre, kann sich das Einsichtsrecht auf die Auskunfterteilung reduzieren. Bei der Gewährung der Einsicht in Teile der Akte bzw. bei einer Auskunfterteilung handelt es sich um die teilweise Ablehnung des Antrages auf Akteneinsicht, die in jedem Fall schriftlich zu begründen ist.

Das Vorliegen personenbezogener Daten in einer Akte rechtfertigt nicht von vornherein die Ablehnung eines Einsichtsantrags. Handelt es sich um nur in geringem Umfang schützenswerte Informationen, hat die Behörde nach einer Anhörung des Betroffenen zu entscheiden, ob eine Einsicht gewährt werden kann. Bei schutzbedürftigen Daten hat die Behörde den Betroffenen auf Verlangen des Antragstellers zu fragen, ob er der Einsichtnahme zustimmt. Erst wenn der Betroffene dies ablehnt, sind die personenbezogenen Daten der Akte auszusondern und der übrige Teil zugänglich zu machen. Nur ausnahmsweise reduziert sich hier das Einsichtsrecht auf die Auskunfterteilung. Die schematische Übersicht in Anlage 4 fasst dieses komplexe Verfahren in vereinfachter Form zusammen.

## 2.3 Wer Akteneinsicht nimmt, hat auch ein Recht auf Fotokopien

*Eine Behörde weigerte sich, Fotokopien eines bereits eingesehenen Dokumentes anfertigen zu lassen. Zuvor hatte sie der Akteneinsicht zugestimmt, da sich keine schutzbedürftigen Daten in den Unterlagen befanden. Die Behörde rechtfertigte dies mit der Erklärung, der Antragsteller hätte mit den Kopien schließlich "etwas anfangen können".*

Welche Absicht ein Antragsteller mit den von ihm zur Einsicht begehrten Informationen hat, spielt beim Akteneinsichts- und Informationszugangsgesetz keine Rolle. Das Recht auf Akteneinsicht gilt grundsätzlich ohne Voraussetzung. Spekulationen über den möglichen Verwendungszweck von Fotokopien können die Ablehnung ihrer Herausgabe nicht rechtfertigen.

Das Akteneinsichts- und Informationszugangsgesetz regelt zwar den Fall, dass der Antragsteller der Übermittlung von Vervielfältigungen an Stelle der Einsicht in die Originaldokumente zustimmt (§ 7), trifft aber keine Aussage zur Anfertigung von Fotokopien im Allgemeinen. Dennoch muss die Behörde ein entsprechendes Verlangen des Antragstellers nach pflichtgemäßem Ermessen überprüfen. Das Recht auf Informationszugang schließt das Recht ein, Informationen in verwendbarer Weise zu erhalten. In der Regel reduziert sich daher das behördliche Ermessen auf eine Pflicht, Kopien herauszugeben. Es besteht kein qualitativer Unterschied zwischen der Einsicht, der Fertigung von Notizen oder dem Fotokopieren der eingesehenen Dokumente. Die Verwaltung muss aber berücksichtigen, dass ihr in der Regel höhere Kosten entstehen, wenn sie den Antragsteller handschriftliche Notizen anfertigen lässt und ihm währenddessen einen kompetenten Ansprechpartner für Rückfragen zur Verfügung stellt, als wenn sie dem Antragsteller die nötigen Kopien gegen Auslagenersatz übergibt. Im Übrigen besteht der Anspruch, die Originaldokumente einzusehen, auch dann noch, wenn der Antragsteller der Übersendung von Kopien gem. § 7 AIG zugestimmt hat.

Jeder Antragsteller hat grundsätzlich das Recht, von der Verwaltung Fotokopien eingesehener Unterlagen gegen Ersatz der Auslagen zu erhalten. Das Recht auf Einsicht in die Originalunterlagen wird dadurch aber nicht ersetzt.

## 2.4 Ablehnungsbescheide müssen nachvollziehbar begründet sein

*Die Ablehnung eines Antrags auf Akteneinsicht ist von der Akten führenden Behörde schriftlich zu begründen. In der Praxis wird oft pauschal auf gewisse Bestimmungen des Akteneinsichts- und Informationszugangsgesetzes (AIG) verwiesen. Nur selten treffen diese aber auf sämtliche Unterlagen zu.*

Jeder kann von der Behörde eine nachvollziehbare und detaillierte Begründung verlangen. Der allgemeine Hinweis, das Gesetz lasse eine Einsicht nicht zu, reicht nicht aus. Auch genügt es insbesondere bei einem umfangreichen Aktenbestand nicht, pauschal auf einzelne Paragrafen des Akteneinsichts- und Informationszugangsgesetzes zu verweisen, die einer Einsicht entgegenstehen. Vielmehr hat die Behörde klar erkennbar darzustellen, welche Unterlagen im Einzelnen in der Akte vorhanden sind und aus welchen Gründen die Einsicht jeweils verweigert wird. Das ist möglich, ohne dass der Inhalt geheimhaltungsbedürftiger Unterlagen preisgegeben wird. Nur so kann der Antragsteller erkennen, ob sein Antrag vollständig bearbeitet wurde. Die Behauptung, dass eine Akte geheimhaltungsbedürftig ist, reicht als Begründung nicht aus. Es ist beispielsweise möglich, dass ein Dokument schutzbedürftige personenbezogene Daten oder geheimhaltungsbedürftige Angaben aus einem Bußgeldverfahren enthält, und ein weiteres aber problemlos offen gelegt werden kann. In solchen Fällen sind die unterschiedlichen Beurteilungen nicht pauschal auf die gesamte Akte zu beziehen, sondern den jeweiligen Unterlagen explizit zuzuordnen. Außerdem muss für den Antragsteller erkennbar sein, dass die Akten führende Stelle geprüft hat, ob eine Schwärzung bzw. Auskunftserteilung nach § 6 Abs. 2 AIG möglich ist. Nur wenn dies nicht der Fall ist, kann ein Dokument komplett zurückgehalten werden.

Die schriftliche Begründung der Ablehnung eines Einsichtsantrags muss für den Antragsteller nachvollziehbar sein. Die geprüften Akten sind aufzulisten und die Ablehnungsgründe den einzelnen Unterlagen zuzuordnen. Auch muss erkennbar sein, weshalb die Aussonderung schutzbedürftiger Daten bzw. eine Auskunfterteilung nicht in Frage kommt.

## 2.5 Gebührenordnung - Klarheit über die Kosten der Akteneinsicht

*Nahezu drei Jahre nach In-Kraft-Treten des Akteneinsichts- und Informationszugangsgesetzes hat die Landesregierung mit dem Innenausschuss*

*des Landtages das Benehmen über eine Gebührenordnung hergestellt.*

Die Bestimmung des Akteneinsichts- und Informationszugangsgesetzes, nach der die Gebühren so zu bemessen sind, dass "zwischen dem Verwaltungsaufwand einerseits und dem Recht auf Akteneinsicht andererseits ein angemessenes Verhältnis" bestehen soll, trägt der Tatsache Rechnung, dass es sich beim Akteneinsichtsrecht um ein in der Landesverfassung verankertes Grundrecht handelt. Gebühren dürfen deshalb nur in einer Höhe erhoben werden, die nicht von der Antragstellung und damit von der Nutzung des Grundrechts abschreckt.

In der Gebührenordnung ist für Amtshandlungen nach dem Gesetz - je nach Arbeitaufwand für die Behörde - eine Spanne von 0,- bis 2.000,- DM vorgesehen. Die Untergrenze bei umfangreichem Verwaltungsaufwand liegt bei 200,- DM und bei außergewöhnlichem Verwaltungsaufwand sogar bei 1.000,- DM. Weniger kann in solchen Fällen also nicht verlangt werden. Pro Kopie werden für die ersten 50 Seiten jeweils 1,- DM fällig werden. Eine Ermäßigung der Gebühren ist nur unter Berücksichtigung der wirtschaftlichen Verhältnisse des Antragstellers vorgesehen.

In unserer Stellungnahme gegenüber dem Ausschuss für Inneres haben wir die Möglichkeit begrüßt, in einfachen Fällen auf eine Gebührenerhebung zu verzichten. Auch bei aufwändigeren Amtshandlungen sollte jedoch nach unserer Auffassung keine Mindestgebühr vorgeschrieben werden. Zudem halten wir eine Obergrenze von 2.000,- DM für durchaus geeignet, Interessierte von der Antragstellung von vornherein abzuhalten. Dasselbe gilt auch für die Auslagen für Kopien, deren pauschale Höhe über die Erstattung tatsächlich entstandener Sachkosten weit hinausgeht. Zudem besteht auf der Grundlage der Gebührenordnung keine Möglichkeit, das von der Verfassung ausdrücklich vorgesehene und vom Gesetz explizit zu fördernde politische Mitgestaltungsinteresse auch bei Kostenerhebungen in besonderer Weise zu berücksichtigen. Nach unserer bisherigen Erfahrung machen aber gerade Bürgerinitiativen und politisch engagierte Einzelpersonen zunehmend von ihren Einsichtsrechten Gebrauch. Auch für solche Fälle sollte eine Gebührenreduzierung möglich sein.

In seiner Entscheidung zum Umweltinformationsgesetz stellte der Europäische Gerichtshof fest, dass eine Gebührenerhebung für die Ablehnung eines Informationszuganges nicht zulässig ist. Hintergrund ist die Überlegung, dass von dem Informationsinteressenten nur dann die Zahlung einer Gebühr erwartet werden kann, wenn er dafür auch eine Gegenleistung - den Informationszugang - erhält. Eine entsprechende Änderung des

Umweltinformationsgesetzes wurde von der Bundesregierung eingeleitet[68]. Die Möglichkeit, nach der Landesgebührenordnung auch für Ablehnungsbescheide auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes Gebühren zu erheben, ist vor diesem Hintergrund problematisch.

Allerdings lässt die Gebührenordnung indirekt bei der Ablehnung von Anträgen die Reduzierung oder den vollständigen Verzicht auf Gebühren zu. Dieser Ermessensspielraum sollte regelmäßig im Sinne eines Gebührenverzichts ausgeübt werden, um eine zusätzliche abschreckende Wirkung bei negativen Bescheiden zu vermeiden.

Da die Gebührenordnung auf drei Jahre befristet ist, werden wir ihre Anwendung in der Praxis beobachten und zu gegebener Zeit Vorschläge für Änderungen machen.

Werden Gebühren und Auslagen für die Akteneinsicht verlangt, so handelt es sich um eine Kostenerhebung für die Ausübung eines Grundrechts. Die Gebührenordnung zum Akteneinsichts- und Informationszugangsgesetz berücksichtigt dies bei der Höhe der Gebühren nicht ausreichend. Eine vollständige Kostendeckung darf nicht Ziel der Gebührenordnung sein. Auch sollten für abgelehnte Anträge in der Regel keine Gebühren erhoben werden.

## 2.6 Informationen als Bringschuld - Behörden und das Internet

*Bei der Suche nach Informationen jeglicher Art greifen immer mehr Menschen auf das Internet zu. Häufig finden sich auf den Informationsseiten der Landesregierung nur solche Daten, die ohnehin bereits veröffentlicht worden sind.*

Vom Ideal des unmittelbaren Zugangs der Bürgerinnen und Bürger über elektronische Medien zu öffentlichen Informationen ist man hier zu Lande noch weit entfernt. Häufig wird "öffentliche Information" als "veröffentlichte Information" missverstanden. So gehören Pressemitteilungen und Ministerreden zum selbstverständlichen Inhalt der Websites. Andere, als Papierversion bereits vorhandene, Publikationen können heruntergeladen oder online bestellt werden.

Bisher als "intern" geltende Informationen, die auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes jedoch ohne Weiteres offen gelegt werden könnten, finden sich auf den Websites der Landesregierung dagegen nicht. Dabei gibt es in jedem Ministerium genügend Dokumente, die

[68] s. Pkt. A 10.2

für die Öffentlichkeit interessant sind und deren Veröffentlichung keine schutzwürdigen Belange entgegenstehen: Gutachten als Grundlage für behördliche Entscheidungen, interne Verwaltungsanweisungen, Statistiken - die Auflistung könnte beliebig ergänzt werden. Aber selbst, wer sich aktiv um Informationen bemüht, findet in den Organigrammen nicht einmal einen Hinweis auf die Ansprechpersonen für Akteneinsicht und Datenschutz. Allerdings ist festzustellen, dass einige Häuser bemüht sind, ihr Angebot ständig zu erweitern und insbesondere beabsichtigen, den Zugang der Bürgerinnen und Bürger zu verschiedenen Daten und Statistiken zu erleichtern.

Während das Akteneinsichts- und Informationszugangsgesetz die brandenburgische Verwaltung lediglich verpflichtet, auf Antrag Informationen einmal offen zu legen, schreibt das Informationszugangsgesetz der USA seit seiner letzten Änderung durch den Electronic Freedom of Information Act eine aktive Informationspolitik vor. Dort hat jede Behörde ihre eigene Website zum Informationszugang, auf der sie sowohl das Gesetz und das Verfahren der Antragstellung erläutert, als auch eine Vielfalt behördlicher Informationen in aufbereiteter Weise zur Verfügung stellt. Damit lassen sich sowohl größere Bürgernähe herstellen als auch die Behörden von Einzelanträgen entlasten.

Die Veröffentlichung der Aktenpläne wird als unabdingbare Voraussetzung für die Wahrnehmung des Informationszugangs begriffen: Nur wer weiß, über welche Arten von Unterlagen die Behörde verfügt, kann seine Rechte überhaupt erst wahrnehmen.

Die Verwaltungen sollten ihre Internetseiten informativer gestalten. Ein erster Schritt wäre die Veröffentlichung ihrer Aktenpläne. Alle Dokumente, die nach dem Akteneinsichts- und Informationszugangsgesetz eingesehen werden können, eignen sich - jedenfalls soweit sie keine personenbezogenen Daten enthalten - auch zur Veröffentlichung im Internet.

# 3 Erfahrungen mit Anträgen und Akteneinsicht

## 3.1 Eingaben und Anfragen beim Landesbeauftragten

*Angenommen, eine Behörde verweigert mir die Akteneinsicht und ich beschwere mich darüber beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht: Wie wird dieser tätig, um mir zu meinem Recht zu verhelfen?*

Sobald wir von Ihnen eine Beschwerde erhalten, fordern wir die Behörde, die die Einsicht verweigert hat, zu einer Stellungnahme auf, um deren Sichtweise der Angelegenheit zu erfahren. Diese bewerten wir und teilen den Petenten

das Ergebnis umgehend mit. In Zweifelsfällen hat der Landesbeauftragte ein eigenes, uneingeschränktes Akteneinsichtsrecht, d. h. er kann die umstrittenen Akten selbst einsehen und prüfen, ob die Verweigerung der Einsicht durch den Antragsteller rechtmäßig war. Gelangen wir zu der Auffassung, dass die Behörde kein Recht hatte, die Einsicht zu verwehren, fordern wir diese auf, den Antrag erneut zu prüfen und die Akten offen zu legen. Für den Fall, dass eine Behörde entweder gar nicht tätig wird oder unsere Hinweise bzw. Aufforderungen nicht beachtet, stellt der Landesbeauftragte einen Verstoß gegen das Recht auf Akteneinsicht und Informationszugang fest, der beanstandet werden kann.

Die Zahl der an uns gerichteten Beschwerden von Bürgerinnen und Bürgern hat sich - verglichen mit dem Vorjahr - im Berichtszeitraum erneut deutlich erhöht. Der Anteil der Eingabe von Bürgerinitiativen nahm dabei überproportional zu. Dies lässt darauf schließen, dass das Gesetz als Instrument zur Stärkung der politischen Mitgestaltung deutlich an Bekanntheit gewonnen hat. Auffällig war auch eine Entwicklung, die dafür spricht, dass das Recht auf Informationszugang sich den Konturen Brandenburgs als Flächenstaat annähert: Während sich 1998 noch eine große Zahl der an uns gerichteten Beschwerden auf Einsichtsanträge bei den Ministerien des Landes bezog, wurden im zurückliegenden Berichtszeitraum etwa drei Viertel aller uns zur Kenntnis gelangten Anträge im kommunalen Bereich gestellt. Der Schwerpunkt lag mit etwa der Hälfte der Fälle auf Unterlagen aus dem Straßen-, Wohnungs- und Bauwesen.

Nur in wenigen Fällen stellten wir fest, dass eine Behörde die Akteneinsicht zu Recht verweigerte. Weit überwiegend hatten die Beschwerden hingegen Erfolg und die Antragsteller konnten nach unserer Vermittlung Akteneinsicht nehmen.

Zur Durchsetzung des Akteneinsichtsrechts kann der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht eingeschaltet werden. Er prüft selbständig, ob eine Verweigerung der Einsicht zu Recht erfolgte oder nicht und teilt dies den Beschwerde führenden Bürgerinnen und Bürgern mit.

## 3.2 Rechtsgrundlagen zur Akteneinsicht - mehr als nur das Akteneinsichts- und Informationszugangsgesetz

*Ein Landwirt beantragte beim Ministerium für Landwirtschaft, Umwelt und Raumordnung Einsicht in Dokumente, in denen auch Daten mit Bezug zu seiner Person verbunden waren. Obwohl das Brandenburgische Datenschutzgesetz ihm als Betroffenen ein ausdrückliches Auskunfts- bzw. Einsichtsrecht zubilligt, wurde der Antrag - gestützt auf das*

*Akteneinsichts- und Informationszugangsgesetz - abgelehnt. In einem anderen Fall begehrte eine Bürgerinitiative Einblick in Unterlagen zu einer landwirt-schaftlich-industriellen Anlage. Auch hier lehnte der zuständige Landkreis den Antrag auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes ab.*

Das Akteneinsichts- und Informationszugangsgesetz (§ 1) sieht den Vorrang bereichsspezifischer Regelungen für einen unbeschränkten Personenkreis vor. Auch gehen speziellere Landes- und alle Bundesgesetze dem allgemeinen brandenburgischen Akteneinsichtsrecht vor. Häufig beziehen sich Antragsteller nur auf das Akteneinsichts- und Informationszugangsgesetz, obwohl sie weitergehendere Ansprüche aufgrund anderer Gesetze hätten. Zunächst muss die Behörde in jedem Fall prüfen, auf welcher Grundlage ein Einsichtsanspruch besteht. Sie darf sich nicht darauf berufen, dass ein ihr vorliegender Antrag sich nur auf ein bestimmtes Gesetz bezieht. Schließlich ist die Rechtsmaterie so kompliziert, dass von einem Antragsteller nicht verlangt werden kann, sich ohne Unterstützung der Verwaltung zurechtzufinden.

In vielen Unterlagen, die zur Einsicht beantragt werden, finden sich Angaben zur Person des Antragstellers. Häufig geht es sogar ausschließlich um diese Person, sodass hier der Auskunfts- bzw. Einsichtsanspruch gem. § 18 Brandenburgisches Datenschutzgesetzes gilt. Personenbezogene Daten umfassen auch Angaben über sächliche, d. h. auch wirtschaftliche oder vermögensrelevante Informationen. Der datenschutzrechtliche Auskunfts- bzw. Einsichtsanspruch ist ein wesentlicher Bestandteil des Grundrechts auf informationelle Selbstbestimmung: Jeder Mensch hat das Recht, zu erfahren, was Behörden über ihn wissen (Art. 11 der Landesverfassung). Nachdem wir in einem Fall die Akten selbst eingesehen und uns vergewissert hatten, dass es um Daten mit Bezug zum Antragsteller geht, haben wir empfohlen, den Antrag erneut auf der Grundlage des vorrangigen Datenschutzgesetzes zu prüfen.

Auch das Umweltinformationsgesetz des Bundes geht dem brandenburgischen Akteneinsichtsrecht vor. Der Einsichtsanspruch nach diesem Gesetz gilt für einen unbeschränkten Personenkreis und kommt zum Tragen, sobald die zur Einsicht begehrten Akten Umweltinformationen enthalten. Der Begriff der Umweltinformation ist recht umfassend[69]. Die Unterlagen zu einer landwirtschaftlich-industriellen Anlage, die eine Bürgerinitiative interessierten, dürften in erster Linie Umweltinformationen erhalten.

[69] Zu den Einsichtsrechten nach dem Umweltinformationsgesetz s. auch Pkt. A 10.2

Neben dem Brandenburgischen Datenschutzgesetz und dem Umweltinformationsgesetz kann auch das Brandenburgische Verwaltungsverfahrensgesetz gegenüber dem Akteneinsichts- und Informationszugangsgesetz vorrangig sein. Es ist anzuwenden, wenn Personen Einsicht in die Akten zu einem laufenden Verwaltungsverfahren beantragen, an dem sie selbst beteiligt sind. Wer sich beispielsweise bei einer Behörde über die Bearbeitung seines Bauantrages informieren möchte, kann auf dieser Grundlage Einsicht in den Vorgang nehmen. § 13 Brandenburgisches Verwaltungsverfahrensgesetz regelt, wer an einem Verfahren beteiligt ist.

Speziellere und bundesgesetzliche Regelungen zum Informationszugang für einen unbeschränkten Personenkreis gehen dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz vor. Das Recht, "eigene" Daten einzusehen, ist im Brandenburgischen Datenschutzgesetz verankert. Das Umweltinformationsgesetz berechtigt zum Erhalt von Umweltinformationen und das Brandenburgische Verwaltungsverfahrensgesetz bietet Beteiligten die Möglichkeit zur Einsicht in Akten aus laufenden Verwaltungsverfahren. Die Behörden haben Anträge auf Akteneinsicht grundsätzlich von sich aus auf der Grundlage aller in Betracht kommenden Regelungen zu prüfen. Der Bescheid muss auf der Grundlage des im Antragsfall anwendbaren Gesetzes ergehen.

### 3.3 Ordner, Hefter, lose Blätter - Was ist eine "Akte"?

*Der hohe Geräuschpegel, der von einem Kinderspielplatz ausgeht, war für einen Bewohner aus der Nachbarschaft Anlass, bei der Stadtverwaltung Akteneinsicht zu beantragen. Sein Antrag wurde jedoch mit der Begründung abgelehnt, es seien keine Akten zum Spielplatz vorhanden.*

Die Stadtverwaltung argumentierte uns gegenüber, dass es sich bei Pflege- und Erhaltungsmaßnahmen öffentlicher Einrichtungen um Geschäfte der laufenden Verwaltung handele, zu denen keine weiteren Beschlüsse der Stadtverordneten gefasst würden und somit keine Akte angelegt worden sei. Gleichzeitig bestätigte die Stadt aber, im Haushaltsplan Mittel für die Instandsetzungsmaßnahmen bereit gestellt zu haben. Die Bestätigung des Haushaltsplanes habe als Grundlage für die Reparaturen genügt. Das Baubetriebsamt habe sämtliche Rechnungen, TÜV-Kontrollen und Ähnliches unter der entsprechenden Haushaltsstelle abgeheftet und keine eigene Akte angelegt.

Nach Auffassung der Stadtverwaltung könnte Akteneinsicht aber nur in separate Akten und Vorgänge gewährt werden. Dies ist jedoch unzutreffend, da sich der Begriff der "Akte" nach § 3 Akteneinsichts- und

Informationszugangsgesetz auf alle schriftlich, elektronisch, optisch, akustisch oder auf andere Weise aufgezeichneten Unterlagen bezieht und somit keineswegs einen "klassischen", separaten Aktenvorgang voraussetzt. Ein Antrag auf Akteneinsicht muss hinreichend bestimmt sein, d. h. es muss erkennbar sein, für welches Thema sich der Antragsteller interessiert. Dabei kommt es nicht darauf an, wie und in welche Vorgänge Informationen abgelegt worden sind.

Schließlich wurde die behördliche Datenschutzbeauftragte der Stadt mit einer Recherche zu den Unterlagen beauftragt, die sich in unterschiedlichen Vorgängen befanden. Dem Antragsteller wurde daraufhin Akteneinsicht angeboten.

Eine "Akte" ist mehr als der klassische, separat angelegte Verwaltungsvorgang mit Aktendeckel und Vorblatt. Als "Akten" sind auch einzelne Unterlagen, elektronisch oder anderweitig gespeicherte Informationen zu verstehen. Diese sind grundsätzlich bei der Akteneinsicht offen zu legen.

### 3.4 Informationszugang für alle - das Gesetz schließt Missbrauch aus

*"Scientology erhält freie Einsicht in Behörden-Akten", titelte im Juni eine große, regionale Tageszeitung. Im Vorfeld hatte ein Vertreter der Organisation bei der Landesregierung Akteneinsicht in Unterlagen zu Scientology beantragt. Kritiker wähnten darin einen Missbrauch des Akteneinsichts- und Informationszugangsgesetzes und schlugen vor, das gerade erst eingeführte Recht auf Informationszugang wieder einzuschränken.*

Das Grundrecht auf Informationszugang und das Akteneinsichts- und Informationszugangsgesetz gelten ohne Voraussetzung. Die Entscheidung, ob Akten eingesehen werden dürfen oder nicht, richtet sich ausschließlich danach, ob die begehrten Unterlagen schutzwürdige Daten enthalten. Die Person des Antragstellers spielt keine Rolle. Auch das dem Antrag zu Grunde liegende Interesse ist unerheblich und darf - bis auf bestimmte im Gesetz geregelte Ausnahmen - von der Akten führenden Stelle weder erfragt noch zur Grundlage der Prüfung des Antrags gemacht werden. Die Bedeutung des Gesetzes beruht schließlich gerade darauf, dass weder ein berechtigtes noch ein rechtliches Interesse geltend gemacht werden muss. Eine Einschränkung des Gesetzes in diesem Punkt würde zugleich an verfassungsrechtliche Grenzen (Art. 21 Abs. 4 Landesverfassung) stoßen.

Allerdings ist auch hier - wie in allen anderen Fällen der Akteneinsicht - zu beachten, dass schutzwürdige Informationen nicht offenbart werden dürfen.

Dies gilt insbesondere für personenbezogene Daten. Aufgrund einer Eingabe haben wir die Ministerien aufgefordert, darzustellen, wie sie den Schutz personenbezogener Daten bei der Durchführung der Akteneinsicht gewährleisten wollen. Im Ergebnis konnten wir feststellen, dass die Akten führenden Stellen den Schutz personenbezogener Daten sichergestellt haben. In vielen Fällen waren solche Informationen auch gar nicht in den Unterlagen vorhanden.

Bei der Entscheidung über einen Antrag auf Akteneinsicht kommt es nicht darauf an, wer diesen stellt oder zu welchem Zweck der Antragsteller die Informationen verwenden möchte. Das Einsichtsinteresse darf von Behörden nicht erfragt werden. Durch den im Gesetz vorgesehenen Schutz privater und öffentlicher Interessen ist ein Missbrauch der Informationen in ausreichender Weise ausgeschlossen.

### 3.5 Eine Bürgerinitiative beantragt Akteneinsicht

*Fünfzehn Mitglieder einer Bürgerinitiative beantragten Einsicht in die Unterlagen eines Trink- und Abwasserzweckverbandes. Ihnen ging es vor allem um Informationen zum Finanzierungsgebaren des Verbandes. Ihren Antrag stellten sie jedoch nicht als Bürgerinitiative, sondern jeweils als Einzelperson. Weil dem Verband der zeitliche Aufwand zu groß erschien, gewährte er zwar Akteneinsicht, gestand jedem einzelnen Antragsteller dafür aber nur zwanzig Minuten zu.*

Das Recht auf Informationszugang beinhaltet, dass die Informationen dem Antragsteller in verwertbarer Weise zugänglich zu machen sind. Dies bedeutet, dass ihm für das Erfassen der Informationen eine angemessene Zeit zur Verfügung zu stellen ist. Bei einem umfangreichen Aktenbestand wie im vorliegenden Fall sind 20 Minuten mit Sicherheit nicht ausreichend. Obwohl die Behörde eine Zeitbegrenzung nicht auf eine gesetzliche Grundlage stellen kann, sind ihre Bedenken hinsichtlich des Zeitaufwandes durchaus nachvollziehbar. Wir haben dem Antragsteller deshalb empfohlen, einige wenige Personen zur Einsichtnahme zu bevollmächtigen, um den Aufwand zu reduzieren.

Das Akteneinsichts- und Informationszugangsgesetz findet nach § 9 Anwendung auf Bürgerinitiativen und Verbände zur Beeinflussung öffentlicher Angelegenheiten. Damit trägt das Gesetz den Vorgaben des Artikels 21 Abs. 3 der Landesverfassung Rechnung, der das Informationsrecht von Bürgerinitiativen und Verbänden gesondert hervorhebt. Im oben geschilderten Fall stellte sich heraus, dass dies den Antragstellern nicht bekannt war und daher fünfzehn Personen gleichlautende Anträge einreichten. Grundsätzlich ist dies zulässig. Allerdings kann auf das

Auskunftsrecht verwiesen werden, wenn mehr als 50 gleichförmige Anträge vorliegen.

Der Zweck der politischen Mitgestaltung hat bei einem Einsichtsantrag auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes stets besonderes Gewicht. Einen solchen Mitgestaltungswillen kann man Bürgerinitiativen in der Regel von vornherein unterstellen. Geht es um personenbezogene Daten, die durch eine Akteneinsicht offen gelegt würden, hat die Behörde nämlich zwischen deren Schutzbedürftigkeit und dem politischen Mitgestaltungsinteresse des Antragstellers abzuwägen. Überwiegt das Einsichtsinteresse, sind die Daten nach der Anhörung der Betroffenen offen zu legen. Selbstverständlich ist das politische Mitgestaltungsinteresse auch bei Einzelpersonen zu berücksichtigen, es muss aber ausdrücklich dargelegt werden. Für eine Bürgerinitiative ist es in den meisten Fällen deshalb vorteilhaft, sich als solche erkennen zu geben und den Einsichtsantrag durch den Vorstand bzw. einen besonders hierzu Bevollmächtigten zu stellen.

Der Antragsteller muss ausreichend Zeit haben, um die bei der Akteneinsicht vorgelegten Informationen erfassen zu können. Eine Zeitbeschränkung ist nicht zulässig. Im Interesse der politischen Mitgestaltung haben Bürgerinitiativen ein hervorgehobenes Informationsrecht. Es kann deshalb vorteilhaft sein, wenn sie sich bei der Antragstellung als Bürgerinitiative zu erkennen geben.

### 3.6 Auftragsgutachten sind keine schützenswerten Akten

*Nach der Rückübertragung eines Grundstücks, beauftragte die Behörde einen externen Gutachter mit der Überprüfung des Vorgangs, der die Rechtswidrigkeit der Vermögensübertragung feststellte. Diese wurde daraufhin zurückgenommen. Zwar wurde der ursprüngliche, positive Bescheid im Widerspruchsverfahren bestätigt, doch machte der Betroffene einen Schaden durch Pachtausfälle geltend, die ihm aufgrund der zwischenzeitlich negativen Entscheidung entstanden seien. Die Verwaltung verweigerte ihm die Einsicht in das Gutachten mit dem Argument, es handele sich um eine rein arbeitsrechtliche Überprüfung des damals zuständigen Sachbearbeiters. Außerdem befänden sich schützenswerte Daten des Gutachters darin, die einer Einsichtnahme entgegenstünden.*

Der Vorgang beinhaltete vor allem Angaben zu dem Betroffenen und dessen Vermögensverhältnissen, sodass diesem schon aus datenschutzrechtlichen Gründen Einsichtsrechte zustanden. Im Übrigen hätten arbeitsrechtliche Informationen über Dritte ohne Weiteres geschwärzt werden können. Solche Daten fanden sich jedoch nicht. Zu dem war allen Beteiligten klar, wer das

Gutachten verfasst hat. Es vermochte auch nicht zu überzeugen, dass personenbezogene Daten eines externen Gutachters schutzbedürftiger sind als Daten von regulär in der Dienststelle Beschäftigten. Das Gutachten wurde von der Behörde in Auftrag gegeben. Es kann also davon ausgegangen werden, dass die Behörde das von ihr in Auftrag gegebene Gutachten im Rahmen ihrer öffentlich-rechtlichen Bindungen nutzen darf. Es fällt damit unter das Akteneinsichtsrecht. Schließlich diente das Ergebnis des Sachverständigen der Verwaltung auch als Grundlage ihrer Entscheidung zur Rückübertragung. Ein Gutachter ist grundsätzlich genauso zu behandeln wie ein Amtsträger, d. h. er hat die Offenlegung seiner Mitwirkung an dem Verwaltungsvorgang hinzunehmen. Schutzwürdige Belange, die dem entgegenstehen könnten, waren hier nicht zu erkennen. Die Behörde gewährte schließlich Akteneinsicht.

Gutachten, die eine Behörde in Auftrag gibt, können grundsätzlich eingesehen werden. Angaben zur Person des Gutachters sind dabei genauso zu behandeln wie Daten der Amtsträger. Sie haben eine Offenlegung hinzunehmen, sofern schutzwürdige Belange nicht entgegenstehen.

### 3.7 Eine Behörde spielt "Toter Mann"

*Die Auskunft, um die ein Bürger einen Landkreis zu einer Bürgschaft bzw. Kreditaufnahme bat, wurde ihm nicht gewährt. Daraufhin stellte er einen schriftlichen Antrag auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes, der monatelang nicht beschieden wurde.*

Auch wenn das Akteneinsichts- und Informationszugangsgesetz bisher keine Bearbeitungsfrist setzt, darf die Behörde nicht untätig bleiben. Anträge auf Informationszugang sind zügig zu bearbeiten, weil Informationen rasch veralten. Werden sie zu spät zur Verfügung gestellt und können nicht mehr verwendet werden, ist dies gleichbedeutend mit der Verweigerung der Einsicht. Für den Fall, dass eine Akteneinsicht aus rechtlichen Gründen nicht gewährt werden kann, muss die schriftliche Ablehnung einschließlich Begründung zeitnah erfolgen.
Anträge auf Akteneinsicht sind möglichst zeitnah zu bearbeiten. Werden Informationen zu spät offen gelegt, ist dies einer Verweigerung der Einsicht gleichzusetzen. Der Landesbeauftragte kann Verstöße gegen das Recht auf Akteneinsicht beanstanden. Dazu gehört neben einer verzögerten Bearbeitung auch die Weigerung der Behörde, auf einen Antrag überhaupt zu reagieren.

### 3.8 Welche Behörde ist die "Akten führende Stelle"?

*Ein Landratsamt verweigerte einem Antragsteller die Einsicht in Akten zu einer vermögensrechtlichen Angelegenheit. Im weiteren Verlauf beschul-*

*digte der Antragsteller die Behörde, Straftaten im Zusammenhang mit diesem vermögensrechtlichen Verfahren begangen zu haben. Um eine Klärung herbeizuführen, erstattete die Behörde daraufhin Strafanzeige gegen Unbekannt. Die Akten, in denen entsprechende Hinweise enthalten gewesen sein sollen, übersandte sie an die Staatsanwaltschaft. Danach kündigte sie dem Antragsteller die Ablehnung des Einsichtsantrags an, da der Behörde keine Unterlagen mehr vorlägen.*

Anträge auf Akteneinsicht werden von der Akten führenden Stelle bearbeitet. Gibt diese die Unterlagen jedoch an eine andere Behörde weiter, stellt sich die Frage, welche von beiden dann Akten führende Stelle ist und somit den Antrag zu bearbeiten hat.

Aus der in Rede stehenden Akte ergaben sich keine Gründe, die Einsicht auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes zu verweigern, da sie nicht zum Zweck des strafrechtlichen Ermittlungsverfahrens angelegt, sondern lediglich hinzugezogen worden war. Es handelte sich daher nicht um staatsanwaltschaftliche Ermittlungsakten, die nach den Vorschriften des Akteneinsichts- und Informationszugangsgesetzes von der Einsichtnahme ausgeschlossen sind.

Eine bloße Weitergabe der Akten bedeutet nicht, dass die Behörde, die gerade über die Akten verfügt, Akten führende Stelle im Sinne des Akteneinsichts- und Informationszugangsgesetzes ist. Dies ist vielmehr nur dann der Fall, wenn eine Behörde die Akten zum Zweck der Weiterbearbeitung abgibt und nicht mehr zurückerhält. In allen anderen Fällen bleibt die abgebende Stelle Akten führend und ist somit nach wie vor für die Durchführung der Akteneinsicht verantwortlich. Keinesfalls kann in einem solchen Fall ein Antrag mit der Begründung abgelehnt werden, die Akten seien im Hause nicht mehr vorhanden. Ansonsten könnte eine Behörde nach Belieben Akten abgeben und die Einsicht stets mit diesem Argument verwehren.

Die Behörde hat die Akten vielmehr zurückzufordern und für die Einsicht zur Verfügung zu stellen. Im geschilderten Fall ist der Landkreis nach unserer Aufforderung so verfahren und der Antragsteller konnte die Unterlagen einsehen.

Eine Behörde bleibt auch dann Akten führende Stelle im Sinne des Akteneinsichts- und Informationszugangsgesetzes, wenn sie Akten an andere Behörden weiterleitet. Zur Durchführung der Akteneinsicht hat sie Unterlagen gegebenenfalls zurückzufordern und dem Antragsteller zur Verfügung zu stellen.

## 4 Evaluation des Akteneinsichts- und Informationszugangsgesetzes

Seit März 1998 ist das Brandenburgische Akteneinsichts- und Informationszugangsgesetz in Kraft, mit dem das Grundrecht nach Artikel 21 Abs. 4 der Landesverfassung konkretisiert wird. Zum ersten Mal in der Bundesrepublik konnten in den zurückliegenden drei Jahren Erfahrungen mit einem allgemeinen verfahrensunabhängigen Informationszugangsrecht gesammelt werden.

Diese praktischen Erfahrungen, die der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht bei der Anwendung des Gesetzes von 1998 gesammelt hat, bieten im Zusammenhang mit der Entwicklung des Informationszugangsrechts in anderen Bundesländern und auf Bundesebene und vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs zum Umweltinformationsrecht die Grundlage für eine Evaluation dieses Gesetzes.

Zunächst ist festzuhalten, dass die im Gesetzgebungsverfahren vielfach befürchtete übermäßige Inanspruchnahme der Verwaltung durch Akteneinsichtsanträge in Brandenburg ausgeblieben ist. Die Behörden auf Landes- und Kommunalebene begreifen eine größere Transparenz gegenüber den Bürgerinnen und Bürgern nach unseren Erfahrungen ganz überwiegend nicht als Behinderung ihrer Aufgabenerfüllung. Hinzu kommt, dass das geltende Gesetz zahlreiche Ausnahmen und ausreichende Sicherungsvorschriften gegen möglichen Missbrauch enthält. Eine Beschränkung des Akteneinsichts- und Informationszugangsrechts z. B. durch die Einführung eines "berechtigten“ oder gar „rechtlichen“ Interesses als zusätzliche Bedingung ist daher nicht erforderlich und würde zudem die Frage nach der Vereinbarkeit mit dem voraussetzunglos garantierten Grundrecht auf Informationszugang (Art. 21 Abs. 4 Landesverfassung) aufwerfen[70].

In sechs zentralen Punkten hat die praktische Anwendung des Gesetzes allerdings Probleme aufgezeigt. Darüber hinaus haben sich im Detail einige weitere Defizite ergeben.

---

[70] s. Pkt. B 3.

1. In der Praxis gerät der Grundrechtscharakter des Akteneinsichtsrechts häufig aus dem Blick. Das Recht auf politische Mitgestaltung, das die Verfassung des Landes in Artikel 21 als Grundlage für das Akteneinsichtsrechts nennt, wird bisher im Akteneinsichtsgesetz nur an einer sehr versteckten Stelle ausdrücklich erwähnt. Damit wird zu wenig deutlich, dass das gesamte Gesetz dem Ziel dient, den Bürgerinnen und Bürgern des Landes die politische Mitgestaltung auf allen Ebenen des staatlichen und kommunalen Handelns zu ermöglichen. Die verfassungsrechtliche Verankerung des Akteneinsichts- und Informationszugangsgesetzes sollte deshalb auch auf einfach-gesetzlicher Ebene stärker hervorgehoben werden, z. B. indem wie im Datenschutzgesetz eine Aufgabenbestimmung an den Anfang des Gesetzes gestellt wird. Zugleich könnte damit verhindert werden, dass die Verwaltung - wie im Berichtszeitraum geschehen - dem Bürger das Recht abspricht, amtliche Unterlagen einzusehen, weil er nach ihrer Auffassung nur ein "privates" und kein "politisches" Anliegen verfolgt.

2. Der bisherige Ausschluss der Anwendbarkeit des Akteneinsichts- und Informationszugangsgesetzes in allen laufenden Verfahren hat sich nicht bewährt. So berief sich eine Stadt auf diese "Verfahrensausnahme" gegenüber Bürgern, die durch Akteneinsicht lediglich klären wollten, wann und wie das Gewerbeamt gegen eine Diskothek vorgegangen sei, die farbigen Besuchern den Zutritt verwehrt hatte. Der Ausschluss laufender Verfahren führt dazu, dass ein Großteil des Verwaltungshandelns Bestimmungen unterliegt, die den Informationszugang nur sehr restriktiv zulassen. Zugleich führt das geltende Recht zu dem merkwürdigen Ergebnis, dass vor Beginn bzw. nach Abschluss eines Verwaltungsverfahrens jede Person Akteneinsicht ohne Begründung verlangen kann, während des Verfahrens jedoch nur die daran Beteiligten und diese auch nur insoweit, als die Kenntnis der Akten zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 29 Abs. 1 Satz 1 Verwaltungsverfahrensgesetz). Beides ist mit dem Grundrecht auf voraussetzungslosen Informationszugang kaum zu vereinbaren.

3. Das geltende Akteneinsichts- und Informationszugangsgesetz regelt das Verhältnis zwischen dem Informationszugangsrecht und dem Recht auf informationelle Selbstbestimmung in der Weise, dass der Zugang zu personenbezogenen Daten ohne Zustimmung der (datenschutzrechtlich) Betroffenen grundsätzlich ausgeschlossen ist. Nur in zwei Fällen lässt das Gesetz Ausnahmen von diesem Verbot zu, wenn im Einzelfall im Hinblick auf den Zweck der politischen Mitgestaltung das Offenbarungsinteresse des Antragstellers das Geheimhaltungsinteresse

der betroffenen Person überwiegt oder wenn es sich um Daten von Amtsträgern handelt, die an Verwaltungsvorgängen beteiligt sind.

Diese Regelung erscheint vor dem Hintergrund der brandenburgischen Landesverfassung, in der sowohl das Akteneinsichtsrecht als auch das Recht auf Datenschutz Grundrechtsqualität haben, als zu restriktiv. In der Praxis führt diese Regelung sehr häufig dazu, dass die Verwaltung den Zugang zu Informationen verweigern kann, weil personenbezogene Daten betroffener Bürger in den Verwaltungsvorgängen enthalten sind.

Der Gesetzgeber sollte demgegenüber eine differenziertere Abwägung zwischen den Grundrechten auf Informationszugang und Datenschutz vornehmen, um einen Ausgleich (praktische Konkordanz) zwischen diesen prinzipiell gleichwertigen Verfassungsgewährleistungen zu erzielen.

Auch wenn es angesichts der modernen Datenverarbeitung keine belanglosen personenbezogenen Daten gibt, ist der Schutz des Grundrechts auf informationelle Selbstbestimmung innerhalb der Privatsphäre im engeren Sinne intensiver als im Bereich der Sozialsphäre. Personenbezogene Daten über Bürgerinnen und Bürger mit stärkerem Sozialbezug, insbesondere solche, die durch die Kontaktaufnahme mit der allgemeinen Verwaltung und die Beteiligung an Verwaltungsverfahren entstehen, sind regelmäßig nicht in vergleichbarer Weise schutzwürdig. Soweit im Einzelfall selbst in diesen Fällen schutzwürdige Belange der Betroffenen dem Informationszugang entgegenstehen, ist er zu verweigern. Insgesamt würde die Aufzählung bestimmter Arten personenbezogener Daten, deren Offenlegung bei einer Akteneinsicht schutzwürdige Belange der Betroffenen in der Regel nicht beeinträchtigen, den Verwaltungen die Rechtsanwendung, insbesondere die Abwägung zwischen den Datenschutz- und Akteneinsichts-Interessen praktisch erleichtern. Eine derartige Regelung würde es auch zuverlässiger ausschließen, dass - wie in der Praxis zum Teil üblich - der Datenschutz als Vorwand zur Informationsverweigerung benutzt wird.

4. Der Schutz von unternehmensbezogenen Angaben ist im geltenden Gesetz nicht angemessen geregelt. Es ist praktisch in das Belieben des betroffenen Unternehmens gestellt, ob eine Information geheim zu halten ist oder nicht. Richtigerweise müsste die Akten führende Stelle in jedem Fall, also gerade auch dann, wenn ein Unternehmen eine Information geheim halten will, selbständig überprüfen, ob an deren Geheimhaltung objektiv ein schutzwürdiges Interesse besteht. Diese Bewertung wäre ihrerseits justitiabel. Das geltende Gesetz lässt diese Handhabung aber nicht zu, sondern überlässt den Unternehmen das letzte Entscheidungsrecht darüber, ob Informationen in behördlichen Unterlagen geheim zu halten sind oder nicht.

   Hinzu kommt, dass das geltende Recht von einer verfassungsrechtlich problematischen Asymmetrie im Verhältnis zwischen dem Schutz personenbezogener Daten einerseits und dem Schutz von Unternehmensdaten andererseits gekennzeichnet ist. Während personenbezogene Daten im Einzelfall im Hinblick auf den Zweck der politischen Mitgestaltung offen gelegt werden dürfen, wenn das Offenbarungsinteresse das Geheimhaltungsinteresse überwiegt, ist eine solche Möglichkeit bei unternehmensbezogenen Daten nicht vorgesehen. Dies führt zu einem verfassungsrechtlich kaum vertretbaren erhöhten Schutz von unternehmensbezogenen Daten im Vergleich zu personenbezogenen Daten.

   Das geltende Gesetz sieht zudem eine fingierte Zustimmungsverweigerung in dem Fall vor, dass die Zustimmung zur Offenlegung von personen- oder unternehmensbezogenen Daten innerhalb der Frist nicht vorliegt. Dies entspricht dem datenschutzrechtlichen Grundsatz, dass Schweigen nicht als Zustimmung zur Verarbeitung personenbezogener Daten gewertet werden darf. Nicht gerechtfertigt ist diese gesetzliche Fiktion aber bei der Offenlegung von unternehmensbezogenen Informationen (Betriebs- und Geschäftsgeheimnissen) und bei der Beteiligung anderer Behörden. Hier ist vielmehr - wie auch sonst im kaufmännischen Rechtsverkehr - eine Zustimmungsfiktion angemessener. Vergleichbare Regelungen finden sich im Kartell- und Immissionsschutzrecht[71].

5. Wie die praktische Erfahrung in Brandenburg zeigt, liegt eine zentrale Schwäche des Akteneinsichts- und Informationszugangsgesetzes im Fehlen einer Frist zur Bearbeitung der Einsichtsanträge. Da

[71] § 111 Abs. 3 Satz 2 GWB (für Betriebs- und Geschäftsgeheimnisse) und § 11 Satz 3 der Neunten Verordnung zur Durchführung des Bundesimmissionsschutzgesetzes (zur Beteiligung anderer Behörden)

Informationen häufig nach kurzer Zeit an Wert einbüßen, kann die Verwaltung durch zögerliche Behandlung das Akteneinsichtsrecht bisher ohne Weiteres leer laufen lassen. Viele Akten führende Stellen berücksichtigen die Bedeutung der Aktualität von Informationen bei der Gesetzesanwendung nicht ausreichend. Von der Möglichkeit einer Untätigkeitsklage (zulässig frühestens drei Monate nach Antragstellung) wird praktisch kein Gebrauch gemacht. Auch die bisher vorgesehene 2-Monatsfrist, innerhalb derer die Zustimmung Dritter einzuholen ist, verzögert den Informationszugang unverhältnismäßig.

6. Die Verwaltung sollte dazu verpflichtet werden, Aktenpläne und -verzeichnisse zu führen und zu veröffentlichen. Dies würde den Antragstellern die Beurteilung ermöglichen, zu welchen Themen die Behörde überhaupt Akten führt. Auch Verwaltungsvorschriften sollten unaufgefordert veröffentlicht werden. Entsprechende Veröffentlichungen müssten in verständlicher und leicht zugänglicher Form erfolgen. Auch sollte die Verwaltung verpflichtet werden, vorhandene Möglichkeiten der Veröffentlichung in elektronischer Form zu nutzen. Das Akteneinsichts- und Informationszugangsgesetz würde auf diese Weise "internetfähig" gemacht. Dies hätte - wie die Erfahrungen in den USA zeigen - auch einen erheblichen Entlastungseffekt für die Verwaltung, weil die Zahl der Einzelanträge auf Informationszugang auf diese Weise deutlich gesenkt werden kann.

Auch in einer Reihe von weiteren Detailfragen legt die praktische Erfahrung mit dem ersten deutschen Informationszugangsgesetz gewisse Änderungen nahe:

- Das Brandenburgische Gesetz verpflichtet bisher Private nur dann, wenn eine öffentliche Stelle sich ihrer zur Erledigung hoheitlicher Aufgaben bedient. Die Einsehbarkeit von Unterlagen sollte aber nicht von der Rechtsform der Akten führenden Stelle, sondern von dem Charakter der zu erledigenden Aufgabe abhängen. Die Wahl, privatrechtliche Formen zur Aufgabenerfüllung zu nutzen, darf nicht zur Absenkung des verfassungsrechtlich vorgeschriebenen Transparenzniveaus führen.

- Gegenwärtig schreibt das Gesetz bei bestimmten öffentlichen oder privaten Geheimhaltungsinteressen, die dem Einsichtsinteresse entgegenstehen, zwingend die Ablehnung der Akteneinsicht vor. Grundrechtsfreundlicher wäre demgegenüber eine Regelung, die der Verwaltung einen Ermessensspielraum eröffnen würde. Sie hätte dann die Möglichkeit, in derartigen Fällen nach einer fehlerfreien Ausübung ihres Ermessens die Akteneinsicht zu verweigern, könnte aber in Einzelfällen dem verfassungsrechtlichen

Akteneinsichtsrecht den gebotenen Vorrang einräumen.

- Aufsichtsakten geben Aufschluss darüber, welche Beanstandungen eine Aufsicht führende Stelle gegenüber der beaufsichtigten Stelle trifft oder weshalb sie von Beanstandungen absieht, welche Fragen zur Ermittlung des Sachverhalts gestellt wurden und wie die beaufsichtigte Behörde reagiert hat. Dies pauschal geheimzuhalten, wie es das geltende Gesetz vorschreibt, ist nicht gerechtfertigt. Das Gesetz enthält eine Vielzahl anderer Ausnahmevorschriften, die den Schutz überwiegender öffentlicher Interessen ausreichend sicherstellen. Der Aufsichtsprozess an sich bedarf eines solchen Schutzes nicht. Das zeigen auch die praktischen Erfahrungen des Landesbeauftragten für das Recht auf Akteneinsicht mit Bürgereingaben. Es würde vielmehr das Vertrauen der Bürgerinnen und Bürger in eine effektiv arbeitende Aufsicht erhöhen, wenn die entsprechenden Akten prinzipiell zugänglich wären und nicht stärker geheimgehalten würden als andere Verwaltungsvorgänge.

- Der Schutz geistigen Eigentums, insbesondere von Urheberrechten, die nach geltendem Recht ebenfalls zur Ablehnung von Akteneinsichtsanträgen zwingen, stehen nach richtiger Auffassung nicht dem Informationszugang, sondern nur der unkontrollierten Vervielfältigung und Weitergabe von urheberrechtlich geschützten Informationen entgegen. Der ausdrückliche Verweis auf den Urheberrechtsschutz hat außerdem keine praktische Bedeutung in der Gesetzesanwendung erlangt. Falls es zu Konflikten in diesem Bereich kommen sollte, würde das Urheberrechtsgesetz des Bundes ohnehin Vorrang vor dem brandenburgischen Landesrecht haben.

- Die Behörde ist nur dann zur Einholung der Zustimmung Dritter (betroffener Personen, Behörden des Bundes bzw. anderer Bundesländer) verpflichtet, wenn der Antragsteller sie dazu auffordert. Allerdings ist diese Möglichkeit häufig nicht bekannt und die Erfahrungen des Landesbeauftragten zeigen, dass die Verwaltung auch kein Interesse daran hat, ohne eine rechtliche Verpflichtung die Antragsteller auf diese Möglichkeit hinzuweisen. Häufig werden Verweigerungen der Akteneinsicht durch die Akten führenden Stellen pauschal damit begründet, dass eine Zustimmung Dritter nicht vorliege, ohne dass der Versuch unternommen wurde, sie einzuholen. Diese Praxis sollte der Gesetzgeber beenden.

  Wird Akteneinsicht abgelehnt, so ist den Antrag stellenden Personen häufig nicht bekannt, dass sie - unabhängig von der Möglichkeit, förmliche Rechtsbehelfe einzulegen - das Recht haben, den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht anzurufen. Die Akten

führenden Stellen sollten dazu verpflichtet werden, auf diese Möglichkeit hinzuweisen.

- Die geltende Fassung des Gesetzes[72] wird in der Praxis von den Behörden häufig als Begründung dafür herangezogen, dass die Aushändigung von Fotokopien generell abgelehnt wird. Zum Teil wird sogar zu Unrecht die Auffassung vertreten, das Gesetz lasse die Aushändigung von Fotokopien nur zu, wenn die Behörde dies vorschlägt und die Antragsteller dem zustimmen. Tatsächlich regelt das Gesetz nur den Fall, dem ein Antragsteller an Stelle der Einsicht in die Originalakte der Zusendung von Kopien zustimmt, weil er beispielsweise eine weite Anreise vermeiden möchte.

  In allen anderen Fällen ist nach der Rechtsprechung des Bundesverwaltungsgerichts zum Umweltinformationsgesetz[73] das Auswahlermessen der Akten führenden Stelle jedoch stark eingeschränkt, sodass häufig nur eine Entscheidung, nämlich die Zurverfügungstellung von Fotokopien, ermessensfehlerfrei ist. Lediglich wenn gewichtige, von der Verwaltung darzulegende Gründe dagegen sprechen, dem Verlangen des Antragstellers nachzukommen, ist eine Ablehnung rechtmäßig. Dies sollte im Gesetz klargestellt werden.

- Die Möglichkeit, Gebühren für die Bearbeitung von Anträgen auf Akteneinsicht zu erheben, sollte auf positive Bescheide beschränkt werden. Damit würde eine abschreckende Wirkung der Gebührenregelung auf künftige Einsichtsanträge vermieden und ein Gleichklang mit dem Umweltinformationsrecht erreicht. Bürgerinnen und Bürger sollten nur für Informationen zahlen müssen, die sie auch tatsächlich erhalten.

Insgesamt zeigen die Erfahrungen der vergangenen drei Jahre mit dem Akteneinsichts- und Informationszugangsgesetz, dass sich keine der anfangs geäußerten Befürchtungen um die Effizienz der Verwaltung bestätigt hat. Vielmehr ist jetzt der Zeitpunkt gekommen, um eine verfassungskonforme Weiterentwicklung des Gesetzes in Angriff zu nehmen, damit Brandenburg seine bisher führende Stellung in diesem Bereich in der Bundesrepublik behauptet.

---

[72] Insbesondere § 7 Satz 1 AIG

[73] Urteil vom 06.12.1996 - 7C64/95 -

## Teil C

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

### 1 Die Dienststelle

Im Berichtszeitraum schlug der Versuch, die Voraussetzungen für eine Verlagerung der Dienststelle des Landesbeauftragten in die Landeshauptstadt zu schaffen, wiederum fehl. Die erforderlichen Haushaltsmittel für die Herrichtung eines vorhandenen geeigneten Gebäudes wurden nicht bewilligt. Der Landesbeauftragte ist jedoch weiter bestrebt, seine Dienststelle mittelfristig nach Potsdam zu verlegen, weil auch in allen anderen Bundesländern eine Einrichtung von so zentraler Bedeutung für die Bürgerinnen und Bürger in der jeweiligen Landeshauptstadt angesiedelt ist. Zudem lassen die notwendige Präsenz in den Ausschüssen und im Plenum des Landtages sowie die gebotene Beratung der Ministerien eine größere räumliche Nähe zum Parlament und zur Landesregierung angezeigt erscheinen. Es bleibt zu hoffen, dass eine entsprechende Lösung spätestens im Zusammenhang mit der Entscheidung über einen Neu- oder Umbau des Landtages gefunden wird.

Die bisher bestehende Raumnot im gegenwärtigen Dienstgebäude in Kleinmachnow konnte zwischenzeitlich dadurch behoben werden, dass zusätzliche Räume im benachbarten Haus 3 am Stahnsdorfer Damm 77 zur Nutzung durch den Bereich Recht hergerichtet wurden. Die Aufteilung der Dienststelle auf zwei benachbarte Gebäude wurde übergangsweise hingenommen, um die dringend erforderliche Verbesserung der räumlichen Arbeitsbedingungen zu erreichen.

Der Landtag hat zudem im vergangenen Jahr die Voraussetzung für die Verbesserung der personellen Situation durch die Bewilligung einer zusätzlichen Stelle im höheren Dienst für den Bereich Technik und Organisation geschaffen. Damit soll dem drastisch gestiegenen Beratungsbedarf im Bereich der datenschutzgerechten Nutzung von Informations- und Kommunikationstechniken, insbesondere des Internets wie auch der elektronischen Akteneinsicht, Rechnung getragen werden.

## 2 Zusammenarbeit mit dem Landtag

Auf die Bitte des Präsidenten des Landtages hin hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht im Präsidium des Landtages zum Entwurf der Landesregierung für Grundsätze der Entscheidung über Ansprüche von Angeordneten des Landtages gemäß Artikel 56 Abs. 3 der Landesverfassung Stellung genommen. Über einen früheren Entwurf hatten wir bereits 1998 berichtet[74]. In seiner Stellungnahme hat der Landesbeauftragte einzelne von der Landesregierung vorgesehene Regelungen vor dem Hintergrund des verfassungsrechtlichen Informationsanspruchs der Parlamentsmitglieder als zu restriktiv bewertet. Außerdem hat er seine dringende Empfehlung bekräftigt, dass der Landtag sich eine Datenschutzordnung geben sollte. Mit diesem Schritt würde die Position des Landtages wie auch der einzelnen Abgeordneten erheblich gestärkt, weil die Landesregierung dann die Weitergabe personenbezogener Daten an das Parlament nicht mehr auf Grund dort fehlender Datenschutzvorkehrungen ablehnen könne.

Die Verfahrensregelungen der Landesregierung zu Artikel 56 Abs. 3 der Landesverfassung sind inzwischen im Zuge der Änderung der Gemeinsamen Geschäftsordnung für die Ministerien des Landes Brandenburg in Kraft getreten[75].

Die Tätigkeitsberichte 1998 und 1999 wurden im Berichtszeitraum im Innenausschuss eingehend erörtert und führten zu Beschlussempfehlungen, die vom Plenum des Landtages gebilligt wurden. Zudem hat der Landesbeauftragte im Rahmen einer öffentlichen Anhörung zum zwischenzeitlich verabschiedeten Entwurf der Landesregierung für ein Zweites Gesetz zur Änderung des Polizeigesetzes, insbesondere zur Frage der Videoüberwachung von öffentlichen Straßen und Plätzen[76], Stellung genommen. Im Zusammenhang mit dem Tätigkeitsbericht 1999 hat der Landtag die Landesregierung aufgefordert sicherzustellen, dass rechtswidrig erhobene Verbindungsdaten in Telekommunikationsanlagen grundsätzlich nicht für Personalentscheidungen verwertet werden dürfen[77].

Schließlich hat der Landesbeauftragte mit der Vorsitzenden des Petitionsausschusses des Landtages Fragen der praktischen Zusammenarbeit zwischen diesen beiden vor allem Bürgerfragen bearbeitenden Einrichtungen erörtert.

---

[74] Tätigkeitsbericht 1998 Pkt. B 5

[75] ABl. 2000, S. 550, 559 f,

[76] s. Pkt. A 4.1.1

[77] vgl. Drs. 3/2237

In diesem Zusammenhang hat der Landesbeauftragte empfohlen, in das Petitionsgesetz bei nächster Gelegenheit eine Regelung zum Umgang mit personenbezogenen Daten aufzunehmen, um auch in diesem Zusammenhang größere Rechtssicherheit zu erreichen.

# 3 Kooperation mit anderen Datenschutzbehörden

## 3.1 Allgemeine Kontakte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Berichtszeitraum unter dem Vorsitz des niedersächsischen Datenschutzbeauftragten, Burckhard Nedden, in Hannover und Braunschweig getagt und mehrere Entschließungen zu aktuellen Themen des Datenschutzes gefasst, die in dem Band "Dokumente zu Datenschutz und Informationsfreiheit 2000" veröffentlicht sind. Dieser Band kann bei uns gesondert angefordert werden. Den Vorsitz für das Jahr 2001 hat turnusmäßig die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Bettina Sokol, übernommen.

Unter dem Vorsitz des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht hat der Arbeitskreis "Medien" der Datenschutzkonferenz im vergangenen Jahr wieder zweimal in Potsdam getagt und Entschließungsentwürfe zu diesem Themenkreis für die Konferenz erarbeitet.

Der Landesbeauftragte hat außerdem in der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation mitgearbeitet. Diese Arbeitsgruppe hat auf seinen Vorschlag hin unter anderem Gemeinsame Standpunkte zu "Datenschutz und Urheberrechts-Management" und "Infomediaries (Informationsmakler) - eine datenschutzfreundliche Geschäftsidee?"[78] beschlossen.

Der internationalen Kooperation der Datenschutzbehörden diente auch die XXII. Internationale Datenschutzkonferenz in Venedig, an der der Landesbeauftragte für Datenschutz und Akteneinsicht zugleich als Referent teilgenommen hat.

Im vergangenen Jahr fanden erneut mehrere Koordinationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich statt, um bei vergleichbaren Problemstellungen (z. B. Videoüberwachung im öffentlichen Personennahverkehr) möglichst zu einheitlichen Standpunkten zu

[78] s. Dokumente zu Datenschutz und Informationsfreiheit 2000, Teil C

gelangen. Außerdem wurden gemeinsame Prüfungen, z. B. bei einer gesetzlichen Krankenkasse, durchgeführt.
Auch die Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht wurde fortgesetzt und intensiviert. Im kommenden Jahr ist daran gedacht, gemeinsam mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht und der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich in Brandenburg gemeinsame Prüfungen bei Anbietern von Tele- und Mediendiensten durchzuführen. Außerdem haben wir - wie in den beiden Vorjahren - erneut gemeinsam die "Dokumente zu Datenschutz und Informationsfreiheit" (bisher: "Dokumente zum Datenschutz") als Anlagenband zu diesem Tätigkeitsbericht herausgegeben.

Im vergangenen Jahr hat der Landesbeauftragte zudem seine Gespräche mit allen Landräten, den Oberbürgermeistern der kreisfreien Städte und den dort tätigen behördlichen Datenschutzbeauftragten abgeschlossen. Dabei wurden zahlreiche Fragen des Datenschutzes und des Informationszugangs erörtert, die sich in der Praxis ergeben.

## 3.2 Nicht nur für Profis und Freaks - Datenschutz im Internet

*"Wie steht's eigentlich mit Datenschutz und Datensicherheit?" Das fragen sich auch immer mehr Nutzerinnen und Nutzer, die sich gerade im Internet, z. B. bei ihrer persönlichen Kommunikation und beim Online-Shopping, unsicher fühlen. Jetzt gibt es eine Anlaufstelle im Internet, bei der alle möglichen Informationen rund um den Datenschutz abrufbar sein werden: Das virtuelle Datenschutzbüro.*

Das virtuelle Datenschutzbüro wird als gemeinsames Projekt von den meisten deutschen und mehreren internationalen Datenschutzbeauftragten angeboten. Neben Informationen finden sich im virtuellen Datenschutzbüro auch Diskussionsforen zu aktuellen Datenschutzthemen. Außerdem wird ein Bereich mit Empfehlungen für Werkzeuge (zumeist freie Software) eingerichtet, mit Hilfe derer Anwender ihre Privatsphäre im Internet sichern können. Die technische Plattform für das Datenschutzbüro wird gegenwärtig vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein bereitgestellt.

Transparenz ist das zentrale Motto im Datenschutzbüro. Das bedeutet: Offenheit für Konzepte, offene Diskussionen und der Einsatz von so genannter Open-Source-Software, die ihre Vertrauenswürdigkeit überprüfbar macht, indem ihr Quellcode offen gelegt und damit für alle einsehbar wird[79]. Im virtuellen Datenschutzbüro sollen datenschutzfördernde Techniken entwickelt

[79] s. Pkt. A 2.3

werden. Jede(r) ist eingeladen, dabei mitzuwirken. Nicht nur professionelle Datenschützer, sondern auch alle Experten, interessierte Freaks und Privacy-Aktivisten können das Projekt mit ihren Kenntnissen mitgestalten.

Die beteiligten Projektpartner betrachten das virtuelle Datenschutzbüro auch als eine Antwort auf die Herausforderungen für die Privatsphäre, die das grenzüberschreitende Internet mit sich bringt. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird unter anderem seine Erfahrungen mit der mitunter schwierigen Gratwanderung zwischen Datenschutz und Informationsfreiheit einbringen, die er seit Bestehen des brandenburgischen Akteneinsichts- und Informationszugangsgesetzes sammeln konnte.

Das virtuelle Datenschutzbüro im Internet - reinklicken!
**http://www.datenschutz.de**

## 4 Kooperation mit anderen Informationszugangsbeaufragten

Nachdem die Länder Berlin und Schleswig-Holstein dem brandenburgischen Beispiel gefolgt sind und eigene Informationsfreiheitsgesetze beschlossen haben, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht gemeinsam mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht und dem Landesbeauftragten für den Datenschutz Schleswig-Holstein die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland gebildet, in der praktische Fragen der Gewährleistung des freien Informationszugangs - auch soweit sie über den Bereich des Datenschutzes hinausgehen - regelmäßig erörtert werden sollen. Diese Arbeitsgemeinschaft hat sich zu ihrer ersten Arbeitssitzung auf Einladung des Landesbeauftragten für das Recht auf Akteneinsicht in Potsdam getroffen. Im kommenden Jahr wird der Berliner Beauftragte für Datenschutz und Akteneinsicht den Vorsitz in dieser Arbeitsgemeinschaft führen. Die Arbeitsgemeinschaft steht allen Beauftragten für den Informationszugang offen, die in Zukunft im Bund oder in anderen Bundesländern gewählt werden.

# 5 Öffentlichkeitsarbeit

## 5.1 Internationales Symposium "Informationsfreiheit und Datenschutz"

Noch im Herbst des vorangegangenen Jahres veranstaltete der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht das Internationale Symposium "Informationsfreiheit und Datenschutz". Die Erfahrungen mit den unterschiedlichen Regelungen zum Informationszugang sowie zum Spannungsfeld zwischen Informationsfreiheit und Datenschutz wurden hier ausgetauscht. Die Beiträge zu dieser Veranstaltung haben wir nun in Form eines Tagungsbandes ("Potsdamer Materialien zu Akteneinsicht und Informationszugang" Band 1) veröffentlicht. Nach einer durchweg positiven Resonanz im Nachgang zu dieser Veranstaltung haben wir uns entschlossen, im Herbst 2001 erneut ein Symposium zu diesem Thema anzubieten. Interessierte Bürger und Bürgerinnen sowie Beschäftigte aus allen Bereichen der Verwaltung und Wirtschaft sind dann wieder herzlich willkommen. Über den genauen Termin und das Tagungsprogramm werden wir rechtzeitig in unserem Internetangebot informieren. Unter http://www.lda.brandenburg.de können auch die Vorträge des letzten Symposiums sowie unsere übrigen Veröffentlichungen abgerufen werden.

## 5.2 Der Landesbeauftragte auf dem Brandenburg-Tag

Wie bereits im Vorjahr war der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht auch im Jahr 2000 wieder mit einem eigenen Informationsstand auf dem Brandenburg-Tag - diesmal in Frankfurt (Oder) - vertreten. Einen Tag lang standen wir für Informationen rund um die Themen "Datenschutz" und "Akteneinsicht" zur Verfügung. Viele Brandenburgerinnen und Brandenburger sowie weitere Gäste des Brandenburg-Tages nutzten die Gelegenheit, sich nach ihren Rechten zu erkundigen.

Zu zahlreichen Themen konnten wir Informationsmaterial anbieten. Mit zwei neuen Faltblättern informierten wir über die Grundrechte auf Datenschutz und Informationszugang und stellten die verschiedenen rechtlichen Möglichkeiten vor, Einsicht in Behördenakten zu nehmen. Einige Besucherinnen und Besucher kamen bereits mit konkreten Fragen an unseren Stand oder trugen uns Beschwerden über Datenschutzprobleme im persönlichen Gespräch vor. Auch dazu konnten wir vor Ort eine Beratung anbieten.

Wer sich für die Themen "Datenschutz" und "Akteneinsicht" interessiert, Fragen an uns hat oder einfach mit uns ins Gespräch kommen möchte, wird den Landesbeauftragten auch im Jahr 2001 wieder auf dem Brandenburg-Tag

antreffen und ist an unserem Stand in Luckau herzlich willkommen.

Kleinmachnow, den 5. März 2001

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg

# Anlagen

**Anlage 1**

# Rede des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, vor dem Landtag Brandenburg am 12. April 2000 zum Tätigkeitsbericht 1998

Herr Präsident,

sehr geehrte Damen und Herren,

wenn Ihnen erst heute der Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht für das Jahr 1998 zur abschließenden Beratung vorgelegt wird, könnte man erwarten, dass inzwischen alle von uns festgestellten Defizite behoben sein müssten. Dies ist jedoch nicht der Fall, wie die Beschlussempfehlung und der Bericht des Ausschusses für Inneres zeigen. Dieser Ausschuss hat nach eingehender Beratung dankenswerterweise unsere Anregung aufgegriffen und empfohlen, die Landesregierung in zwei Bereichen zum Tätigwerden aufzufordern, in denen nach wie vor Handlungsbedarf besteht.

Zum einen war bisher das Sicherheitskonzept des Landesverwaltungsnetzes unvollständig, weil für das Fachnetz der Finanzverwaltung ein derartiges Konzept seit 1997 fehlte. Inzwischen hat uns das Ministerium der Finanzen ein entsprechendes Konzept zugeleitet, das wir gegenwärtig überprüfen. Das Ergebnis dieser Überprüfung werden wir dem Ministerium mitteilen, damit die Landesregierung ihrem vom Innenausschuss empfohlenen Berichtsauftrag nachkommen kann.

Ein erhebliches Defizit besteht weiterhin bei den Rechtsgrundlagen für den sensiblen Bereich der Sicherheitsüberprüfung im öffentlichen Dienst. Während der Bund und mehrere Bundesländer hierfür bereits Regelungen getroffen haben, fehlen im Land Brandenburg nach wie vor die erforderlichen Vorgaben des Gesetzgebers. Sensible Daten der öffentlichen Bediensteten und ihrer Angehörigen dürfen nicht länger nur auf der Grundlage von Verwaltungsvorschriften verarbeitet werden.

Besondere Bedeutung messen wir auch der parlamentarischen Kontrolle von Maßnahmen der akustischen Wohnraumüberwachung oder Lauschangriffen zu Zwecken der Strafverfolgung bei. Hierzu hat der Minister der Justiz und für

Europaangelegenheiten die Zusage seines Amtsvorgängers bekräftigt, den Landtag jährlich über derartige Maßnahmen in Anlehnung an das Polizeirecht zu unterrichten. Ich begrüße dies ausdrücklich. Ich würde es darüber hinaus aber auch begrüßen, wenn die Landesregierung dem Beispiel der Bayerischen Staatsregierung folgen würde und einen Gesetzentwurf zur parlamentarischen Kontrolle derartiger Maßnahmen auf Landesebene vorlegen würde. Eine effektive Kontrolle hängt in jedem Fall davon ab, dass dem Landtag ein aussagekräftiger Bericht vorgelegt wird.Er sollte auch Angaben darüber enthalten, inwieweit völlig unbeteiligte Personen von derart einschneidenden Grundrechtseingriffen betroffen sind.

Außerdem sollte der Umgang mit personenbezogenen Daten in diesem Landtag jetzt möglichst zeitnah in einer Datenschutzordnung, wie sie das Brandenburgische Datenschutzgesetz vorsieht, geregelt werden. Das Grundrecht der Menschen auf Datenschutz muss auch im parlamentarischen Raum angemessen geschützt werden. Ich habe hierzu dem Vorsitzenden des Hauptausschusses und der Landtagsverwaltung meine Unterstützung bei der Erarbeitung einer Datenschutzordnung angeboten.

Wir werden gegenwärtig Zeugen einer Entwicklung, deren Bedeutung für das Menschenrecht auf informationelle Selbstbestimmung alles bisher Dagewesene übertrifft. Weltweit wird an der Entschlüsselung des menschlichen Genoms gearbeitet. Auch wenn manche Erfolgsmeldung der vergangenen Woche verfrüht gewesen sein mag, so steht doch fest, dass in nächster Zukunft die Möglichkeiten der medizinischen Diagnostik auf der Grundlage des menschlichen Bauplanes drastisch erweitert werden. Selbst Humangenetiker fordern bereits seit einiger Zeit den Gesetzgeber auf, den Umgang mit den genomanalytisch erhobenen Daten strikt zu begrenzen. Denn nur auf diese Weise kann verhindert werden, dass Menschen mit bestimmten genetischen Anlagen von vornherein auf dem Arbeitsmarkt chancenlos bleiben, die Bestimmungen des Arbeitsschutzrechts ausgehöhlt werden und Versicherungen durch entsprechende Untersuchungen ihre Risiken auf Kosten der Betroffenen weitgehend ausschließen.

Entsprechende gesetzliche Regelungen sind zwar nur auf Bundesebene sinnvoll; aber die Landesregierung sollte hier die Möglichkeit einer Bundesratsinitiative ernsthaft prüfen. Längeres Zuwarten in diesem Bereich könnte sich in naher Zukunft bitter rächen. Auch hier sind wir gern bereit, das zuständige Ministerium bei der Vorbereitung einer solchen Initiative zu beraten und zu unterstützen.

Schließlich noch ein Wort zur Akteneinsicht: Das allgemeine Informationszugangsrecht, für das im Land Brandenburg Pionierarbeit geleistet worden ist,

macht inzwischen Schule und ist von zwei weiteren Bundesländern - Berlin und Schleswig-Holstein - übernommen worden. Mit gewissen Einschränkungen ist das Akteneinsichtsgesetz fast zu einem "Exportschlager" Brandenburgs geworden. Den Kritikern dieses Gesetzes sei gesagt, dass gerade auch die Wirtschaft ein Interesse an transparenten Abläufen in der öffentlichen Verwaltung hat und ein allgemeines Akteneinsichtsrecht kein stichhaltiges Argument gegen den Wirtschaftsstandort Brandenburg ist. [Wer nach Nordamerika sieht, wird feststellen, dass Informationsfreiheit und wirtschaftliche Prosperität sich nicht ausschließen.] Unser Akteneinsichtsrecht enthält zudem ausreichende Sicherungen gegen Missbrauch.

Wir werden uns auch weiterhin dafür einsetzen, dass in Brandenburg die Entwicklung einer Kultur des Datenschutzes und der Verwaltungstransparenz vorankommt. Ich hoffe dabei auf Ihre Unterstützung.

Herzlichen Dank für Ihre Aufmerksamkeit.

**Anlage 2**

Schwerin/Kleinmachnow im Februar 2000

**Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern**
**Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg**

# Data-Warehouse und Datenschutz

## 1. Einleitung

### 1.1 Ausgangslage

Mit der ständig zunehmenden Leistungsfähigkeit der in Wirtschaft und Verwaltung eingesetzten Informations- und Telekommunikationstechnik wächst die Menge der automatisiert gespeicherten *personenbezogenen Daten* unaufhaltsam. Aus allen Lebensbereichen werden Daten beispielsweise durch Nutzung von Chipkartensystemen und neuen Kommunikationsmedien preisgegeben und sowohl in Privatunternehmen als auch im Bereich der öffentlichen Verwaltung gespeichert. Datensparsamkeit und Datenvermeidung spielen noch immer und z. T. ganz bewusst eine untergeordnete Rolle.

In Unternehmen und Behörden wächst das Interesse, das gesammelte Datenmaterial effektiver als bisher zu nutzen. Dabei wird davon ausgegangen, dass zu einem Betroffenen (Kunden) nicht durch Bewertung einzelner Daten ein aussagefähiges Gesamtbild entsteht, sondern erst durch die Analyse der Gesamtheit aller verfügbaren Daten einer Person und ihrer Beziehungen zueinander.

Das *Data-Warehouse* (DWH) ermöglicht diese neue Betrachtungsweise der Daten, indem in ihm alle im Unternehmen bzw. in der Behörde verfügbaren Daten nach bestimmten Kriterien sortiert gespeichert und zur Analyse und Auswertung bereitgehalten werden. Bisher unbekannte Zusammenhänge zwischen Einzeldaten sollen mit Hilfe des so genannten *Data Mining* (DM) aus der Gesamtheit des Datenbestandes erkannt werden, um aus diesen - die Aussagekraft der einzelnen Angaben meist deutlich übersteigenden - Informationen vor allem wirtschaftliche Vorteile für die speichernde Stelle erzielen zu können. Dabei ist beabsichtigt, dem Manager und künftig wohl

bald auch dem Behördenleiter aus der Fülle des Datenmaterials nur die strategisch wichtigen Informationen - möglichst in ansprechender und visuell einprägsamer Form - darzustellen, ohne dass er den Ballast der täglich anfallenden operativen Daten wahrnimmt und dabei auf die ständige Mitwirkung von Informatikern und Statistikern angewiesen ist. Die sich rasant entwickelnde Leistungsfähigkeit von Hardware und Datenbanktechnologien bietet dabei immer bessere Möglichkeiten zur Analyse und zur verständlichen, graphischen Präsentation von Datenbeständen.

## 1.2 Ziel der Abhandlung

Auch wenn DWH-Konzepte bisher meist nur im Bereich der Privatwirtschaft anzutreffen sind, erscheint die Untersuchung dieser neuen Technologie aus datenschutzrechtlicher und -technischer Sicht auch durch die für den öffentlichen Bereich zuständigen Datenschutzbeauftragten geboten, um für die Diskussion über Anwendung dieser Konzepte in der Verwaltung gewappnet zu sein. Künftige Anwender sollen den möglichen Nutzen für Wirtschaft und Verwaltung sorgfältig gegenüber den Gefahren für die Privatsphäre des Einzelnen abwägen können und im Ergebnis dieses Prozesses die jeweils erforderlichen und angemessenen datenschutzfreundlichen Technologien einsetzen.

Den Schwerpunkt der rechtlichen Bewertung bilden die für den öffentlichen Bereich geltenden Datenschutznormen, wobei aber versucht wird, allgemeingültige Aussagen herauszuarbeiten, welche auch auf den privatwirtschaftlichen Bereich übertragbar sind.

## 1.3 Gang der Darstellung

Zunächst werden die wichtigsten mit dem Konzept des DWH zusammenhängenden Begriffe definiert und erläutert (2. Kapitel) sowie die erforderlichen Softwaregrundlagen im Überblick vorgestellt (3. Kapitel). Anschließend werden verschiedene Überlegungen dargestellt, die den Einsatz des DWH in der Verwaltung interessant erscheinen lassen (4. Kapitel) und konkrete Realisierungsbeispiele aufgeführt (5. Kapitel). Den Hauptteil der Arbeit bilden die datenschutzrechtliche Bewertung des DWH-Konzeptes (6. Kapitel) und die damit einhergehenden Empfehlungen für seine datenschutzgerechte Umsetzung (7. Kapitel). Am Ende werden die Ergebnisse zusammengefasst und die Konsequenzen für das weitere Vorgehen gezogen (8. Kapitel).

## 2. Begriffe

*Operative Datenbasis*

Den Bestand an Daten einer *Daten verarbeitenden Stelle*, der ständig zur unmittelbaren Aufgabenerfüllung benötigt wird, bezeichnet man als operative Datenbasis. Diese Daten resultieren aus den Einzeloperationen des Tagesgeschäfts und kennzeichnen den Ablauf oder Status einzelner Geschäfts- bzw. Verwaltungsvorgänge. Aus datenschutzrechtlicher Sicht korrespondiert die operative Verarbeitung eng mit der Aufgabe der Daten verarbeitenden Stelle und hat nicht die Gewinnung strategischer Aussagen zum Ziel.

*Data Warehouse*

Im DWH werden alle von einer Daten verarbeitenden Stelle jemals erhobenen und gespeicherten Daten nach einem einheitlichen System geordnet und jederzeit verfügbar zum Abruf für unterschiedliche Zwecke bereitgehalten. Die Daten kommen aus allen Bereichen der Daten verarbeitenden Stelle. So können im nicht-öffentlichen Bereich beispielsweise neben Vertriebsinformationen und Kommunikationsdaten auch die Transaktionsdaten der Zahlungsvorgänge sowie weitere Informationen über die Kauf- und Zahlgewohnheiten des einzelnen Kunden einfließen. In der öffentlichen Verwaltung wäre denkbar, dass sämtliche Vorgänge aller Organisationseinheiten einer Stelle (z. B. Ämter einer Kommune oder Abteilungen eines Ministeriums usw.) betroffenen- oder bearbeiterbezogen recherchierbar gespeichert werden.

Im Gegensatz zur operativen Datenbasis, bei der Daten i. d. R. nach Abschluss des Vorgangs schwer zugreifbar archiviert oder gelöscht werden, hält das DWH Daten über einen langen Zeitraum umfassend für Recherchezwecke vor.

*Management-Informations-System*

Die Idee des DWH ist nicht neu. Bereits in den 70er Jahren wurde der Versuch unternommen, Managemententscheidungen auf der Basis der gespeicherten Daten einer Daten verarbeitenden Stelle zu treffen. Die damals propagierten Management-Informations-Systeme konnten die an sie gestellten Erwartungen jedoch nie erfüllen, weil im Gegensatz zum DWH-Konzept strategische Daten direkt aus der operativen Datenbasis gewonnen werden sollten.

*Extraktionswerkzeuge*

Das Zusammenführen aller operativen Daten einer Daten verarbeitende Stelle in das DWH ist keinesfalls eine triviale Aufgabe. Hierfür sind spezielle Softwarekomponenten erforderlich, die als Extraktionswerkzeuge bezeichnet werden. Sie haben u. a. die Aufgabe, Rohdatenstrukturen zu analysieren, Daten zu selektieren und für die Zusammenführung in das DWH vorzubereiten. Nach erfolgter Zusammenführung werden diese Werkzeuge für umfangreiche Prüfungen und ggf. Korrekturen genutzt. Erschwert wird das Zusammenführen der Daten insbesondere dadurch, dass in einer Daten verarbeitenden Stelle verschiedene Computersysteme und -programme eingesetzt werden, die ganz unterschiedliche Datenstrukturen erzeugen. Aus diesem Grund enthalten auf dem Markt angebotene DWH-Systeme bis zu 170 verschiedene Importschnittstellen.

*Data Mart*

Aus den o. g. Gründen ist das allumfassende, unternehmens- bzw. behörden-weite DWH z. Z. kaum realisierbar. In der Praxis erfolgt die Zusammenführung von Datenbeständen aber schon erfolgreich auf der Ebene von Abteilungen oder Geschäftsbereichen einer Daten verarbeitenden Stelle. Ein derart verkleinertes, themenspezifisches DWH wird als Data Mart (Marktplatz) bezeichnet.

*Data Mining*

Die Zusammenführung aller Daten im DWH bzw. im Data Mart und die danach erfolgte Trennung von der operativen Datenbasis ist Voraussetzung für die weitere Informationsgewinnung. Unter dem Begriff des DM werden alle Verfahren subsumiert, mit denen die scheinbar zusammenhanglosen Daten des DWH nach bisher unbekannten, wissenswerten Zusammenhängen durchsucht werden. Dabei kommt es nicht mehr darauf an, dass der Verdacht eines Zusammenhangs durch kluge Fragestellungen an das System bestätigt werden soll. Vielmehr soll der Computer selbständig nach unbekannten, bisher verborgenen Mustern oder Trends suchen.

## 3. Softwaregrundlagen

Softwarebasis des DWH ist i. d. R. ein auch als Standardsoftware verfügbares *Datenbank-Management-System* (DBMS). Die Menge der unterschiedlichen Daten, die im DWH vorgehalten werden (bei Warenwirtschaftssystemen können Größenordnungen von mehr als 20 Terabyte erreicht werden), hat auch zur Folge, dass die Zahl der Nutzer eines solchen Systems groß ist. Diese Nutzer sind in der Mehrheit jedoch keine

IT-Fachleute, die detaillierte Kenntnisse über DBMS und Abfragesprachen haben. Deshalb ist der erste Schritt zur effektiveren Gestaltung der Informationsgewinnung die Bereitstellung von *graphischen Benutzeroberflächen* und leicht bedienbaren *Visualisierungswerkzeugen*. Auch Nicht-Experten werden damit in die Lage versetzt, u. a. durch intelligente Menüführung Abfragen zu formulieren und die Ergebnisse mit Hilfe graphischer Darstellungen auszuwerten.

Ein DWH soll jedoch mehr leisten als ein konventionelles DBMS. Deshalb werden *Data-Mining-Tools* angeboten, die in den Daten verborgene Regeln entdecken, bisher nicht erkannte Zusammenhänge aufdecken oder bestimmte Sachverhalte voraussagen. Es können Unregelmäßigkeiten aufgespürt und "Ausreißer" sichtbar gemacht werden. Zur Datenanalyse werden neue Softwaretechnologien wie *neuronale Netze*, *Case Based Reasoning*, *Regelinduktion* oder *Clustering* genutzt.

Der Grund für den Einsatz solcher Technologien für das DWH ist die Lernfähigkeit der darauf basierenden Softwareprodukte. Die Software trainiert sich mit einem teilweise selbstorganisierenden Lernprozess anhand vorhandener Daten selbst. Es werden weiche Fragestellungen beispielsweise zur Generierung von Hypothesen sowie deren Validierung eingesetzt.

## 4. DWH in der Verwaltung

Obwohl DWH-Konzepte z. Z. fast nur mit privaten Unternehmen in Zusammenhang gebracht werden, stammt die Idee aus der Verwaltung. Bereits Anfang der 60er Jahre wurden Vorstellungen entwickelt, dass der Daseinsvorsorgestaat die allgemeine Bedürfnisbefriedigung durch seine Verwaltungstätigkeit sicherstellen solle. Die einsetzende Nutzung von Computern in der Verwaltung führte zu den ersten großen Datensammlungen. Man hoffte, dass mit diesen Daten auch die Verhaltensweisen in der Gesellschaft erforscht werden können. Die zur Verfügung stehende Rechentechnik war zu der Zeit jedoch nicht annähernd in der Lage, dieses hoch gesteckte Ziel zu erreichen.

Durch die rasante Entwicklung der Informations- und Kommunikationstechnik und die zunehmende Nutzung von DWH-Technologien durch die Privatwirtschaft kommt die Nutzung des DWH-Konzeptes auch für den öffentlichen Bereich ins Gespräch.

So gibt es inzwischen in nahezu allen Verwaltungen auf der Ebene von Bund, Ländern und Gemeinden umfangreiche Bestrebungen zur Verwaltungsmodernisierung. Um Verwaltungsabläufe effektiver und damit

letztlich kostensparender zu gestalten, ist in aller Regel eine fundierte Datenbasis erforderlich, aus der die möglichen Instrumente für eine Änderung der Abläufe entwickelt werden können. Dabei liegt es nahe, Daten, die von verschiedenen Organisationseinheiten einer Behörde zu ganz unterschiedlichen Zwecken erhoben, gespeichert und verarbeitet werden, in einem DWH zusammenzuführen. Die so zusammengeführten und im DWH gespeicherten Daten könnten dann mit Werkzeugen des DM nach allen möglichen Richtungen mit dem Ziel ausgewertet werden, Effektivierungspotentiale zu entdecken, auf die bisher niemand gekommen ist. Mit der Verwaltungsmodernisierung in engem Zusammenhang steht die Einführung von Kosten-Leistungs-Rechnung in die öffentliche Verwaltung, bei der ebenfalls DWH-Technologien genutzt werden könnten.

Unabhängig von Projekten der Verwaltungsmodernisierung ist es möglich, dass Behörden für die Erstellung von behördeninternen Statistiken auf DWH-Systeme und -technologien zurückgreifen.

Schließlich ist auch nicht auszuschließen, dass im Sozialversicherungsbereich DWH-Systeme eingesetzt werden, um auch hier mit Hilfe von DM bisher nicht bekannte Zusammenhänge zu erkennen und zu nutzen.

In allen Fällen stellt sich aus datenschutzrechtlicher Sicht die Frage, ob ein DWH in der öffentlichen Verwaltung mit den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahre 1983 vereinbar ist. Es wird vor allem darauf ankommen, ob die von den Datenschutzgesetzen von Bund und Ländern geforderte Zweckbindung bei der Verarbeitung - insbesondere der Nutzung - personenbezogener Daten gewährleistet werden kann. Zusätzliche Einschränkungen sind dabei bei besonders sensiblen Daten, wie beispielsweise Sozial- oder Personaldaten, gegeben.

## 5. Realisierungsbeispiele

DWH-Konzepte sind keineswegs nur Zukunftsmusik. Hinter Begriffen wie *"Semantic Computing"*, *"Knowledge Processing"* oder *"Computer Animation and Simulation"* verbergen sich ganz konkrete Verfahren und am Markt bereits angebotene Produkte, die als Bausteine für ein DWH dienen. Große Softwarefirmen bieten neben kompletten DWH-Produkten und Einzelbausteinen mit wohlklingenden Namen wie *"Business Information Warehouse"* oder *"sphinxVision"* auch bereits Schulungen zu solchen Produkten an.

Was demnächst auch in Deutschland erwartet werden kann, zeigt ein Blick in

die USA. Der "gläserne Kunde“ ist beispielsweise in einer amerikanischen Warenhauskette , die bereits Supermärkte in Deutschland eröffnet hat, längst Wirklichkeit. Der Konzern weiß genau, welche Produkte in welchen Filialen zu welchem Preis angeboten werden können, weil er detailliert registriert, welcher Kunde welche Waren in seinem Einkaufswagen hat.

Inzwischen werden allerdings in vielen Ländern bei Anbietern und Nutzern von DWH auch die Gefahren dieser Technologien erkannt. Das ist vor allem darauf zurückzuführen, dass zumindest in den Industriestaaten eine zunehmende Sensibilität für den Schutz der Privatsphäre zu beobachten ist und in vielen Ländern - insbesondere in Europa, aber auch in Kanada - DWH-Systeme an rechtliche Grenzen stoßen. Deshalb unternehmen auch bedeutende Anbieter von DWH zunehmend den Versuch, datenschutzfreundliche Technologien (*privacy enhancing technologies - PET*) in ihre Systeme zu implementieren.

Die Funktionsweise eines DWH unter Nutzung von PET könnte dabei in etwa wie folgt aussehen:

Zunächst werden eine Vielzahl von sehr detaillierten personenbezogenen Kundendaten erhoben und im DWH gespeichert. Innerhalb des DWH werden dann die identifizierenden Daten von den übrigen Daten getrennt. Somit werden die Daten innerhalb des DWH pseudonymisiert. Das DWH bietet nun die Möglichkeit, die Fülle der Daten mit Hilfe von DM auszuwerten und auf unterschiedlichen Ebenen (sog. *views*) zusammenzuführen. Wichtig ist, dass bei dieser Art der Nutzung der Daten keine Zugriffe auf die identifizierenden Daten möglich sind. Die Wiederherstellung eines Personenbezuges soll also weitgehend ausgeschlossen werden.

Die eingesetzten PET konzentrieren sich dabei auf die Beschränkung des Zugangs zu den Daten, vermeiden aber nicht die Erhebung und Speicherung personenbezogener Daten. Das Unternehmen stellt für sein DWH darüber hinaus verschiedene *tools* zur Verfügung, die es ermöglichen, dass z. B. auf Wunsch des Kunden einzelne Datensätze physisch gelöscht werden können oder die betroffenen Personen einen lesenden Zugriff auf alle ihre eigenen Daten erhalten können. Ob solche *tools* in Anspruch genommen werden, hängt aber vom Käufer des DWH ab.

Obwohl die bisher genannten Beispiele aus der privaten Wirtschaft stammen, ist auch zu beobachten, dass staatliche Stellen den Nutzen dieser neuen Technologie mehr und mehr erkennen. So ist beispielsweise das Bundesaufsichtsamt für den Wertpapierhandel dabei, für die Börsenaufsicht Softwareagenten einzuführen, die aus täglich etwa einer halben Million Meldungen

über Käufe und Verkäufe von Aktien und Optionsscheinen verdächtige Transaktionen herausfiltern sollen, um verbotene Insidergeschäfte aufzudecken.

Ein weiteres konkretes Beispiel ist das von den Betriebskrankenkassen (BKK) in Deutschland angedachte Projekt BKK-InfoNet. Dabei ist beabsichtigt, eine gemeinsame Datenbank für alle BKK zu schaffen. Diese Datenbank soll nicht nur dazu dienen, die üblichen Datenverarbeitungsvorgänge der Krankenkassen, insbesondere zur Abrechnung mit den Leistungserbringern und zur Verwaltung der Mitglieder, an einer Stelle zu konzentrieren und damit zu effektivieren. Vielmehr ist auch geplant, die zu ganz unterschiedlichen Zwecken gespeicherten Daten von Versicherten, Leistungserbringern und anderen Leistungsträgern zusammenzuführen und Auswertungen nach verschiedenen Richtungen - etwa zum Zwecke der Qualitätssicherung - vorzunehmen. Dafür sollen auch hier pseudonymisierte Daten verwendet werden.

Gerade im Bereich der öffentlichen Verwaltung ist zu klären, ob das Konzept des DWH in Verbindung mit dem Einsatz datenschutzfreundlicher Technologien Grundlage für datenschutzrechtlich zulässige Verfahren zur Datenverarbeitung sein kann.

## 6. Datenschutzrechtliche Bewertung

### 6.1 Einführung

Aufgabe des Datenschutzes ist es, das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Dieses Grundrecht auf informationelle Selbstbestimmung wurde vom Bundesverfassungsgericht (BVerfG) im sog. *Volkszählungsurteil* (BVerfGE 65, 1 ff.) aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) hergeleitet. Der Umsetzung dieses - mittlerweile in einigen Landesverfassungen ausdrücklich genannten - Grundrechts dienen die Datenschutzgesetze des Bundes und der Länder sowie die datenschutzrechtlichen Bestimmungen bereichsspezifischer Rechtsvorschriften.

Das *Bundesdatenschutzgesetz* (BDSG) gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die öffentlichen Stellen des Bundes und durch die Privatwirtschaft. Anwendungsbereich der Landesdatenschutzgesetze ist der Umgang mit personenbezogenen Daten durch die öffentlichen Stellen der Länder. Grundlage der folgenden Ausführungen ist das BDSG; die Landesdatenschutzgesetze werden nur dann erwähnt, wenn sie Regelungen enthalten, die im öffentlichen Bereich zu

einer abweichenden Bewertung führen. Berücksichtigt wird auch der auf Grund der EG-Datenschutzrichtlinie erstellte Entwurf für ein neues BDSG mit Stand Oktober 1999, sofern er für die Untersuchung maßgebliche Änderungen gegenüber dem geltenden BDSG enthält.

Die bereichsspezifischen Datenschutznormen basieren auf den Vorschriften und vor allem auf den Begriffen der allgemeinen Datenschutzgesetze. Als leges speciales gehen sie diesen grundsätzlich vor (§ 1 Abs. 4 S. 1 BDSG). Diese Abhandlung beschränkt sich allerdings auf die Darstellung der Zulässigkeit nach den allgemeinen Datenschutzgesetzen. Im Anwendungsbereich der bereichsspezifischen Gesetze wäre eine Reihe zusätzlicher Fragen zu beantworten. Dies würde den Rahmen dieses Papiers sprengen.

Dem Datenschutzrecht unterliegen nur *personenbezogene Daten*, also "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)" (§ 3 Abs. 1 BDSG). Daten einer juristischen Person, z. B. einer Anstalt oder einer Aktiengesellschaft, fallen genauso wenig unter das Datenschutzrecht wie Daten, die keiner konkreten natürlichen Person zugeordnet werden können, also anonym sind.

Eine Voraussetzung für den erfolgreichen Einsatz des DWH ist, dass alle verfügbaren Daten der Geschäfts- und Verwaltungsvorgänge und damit auch der Kunden bzw. Betroffenen erfasst werden. Um von anonymen Datenbeständen sprechen zu können, würde es nicht ausreichen, beispielsweise auf die Speicherung der Namen von Kunden oder anderer ihrer Identifikation dienenden Schlüssel (z. B. die Kundennummer) zu verzichten. Die Menge der darüber hinaus gespeicherten Daten (Anschrift, Kommunikationsdaten, Transaktionsdaten von Bezahlvorgängen, Bankverbindungen usw.) gestattet es i. d. R. ohne weiteres, den Personenbezug mit vertretbarem Aufwand an Zeit, Kosten und Arbeitskraft herzustellen. Um die Personenbeziehbarkeit sicher auszuschließen, wäre es also erforderlich, auch auf wenigstens einen Teil solcher Daten zu verzichten.

In der Wirtschaft wurde bisher in vielen Fällen der Personenbezug aber geradezu gefordert. Strategisches Ziel der Nutzung des DWH ist oft eine zielgerichtete kundenorientierte und damit personenbezogene Werbung. Die Analyse der Daten soll mitunter auch zeigen, welcher Kunde "wechselgefährdet" ist oder frühzeitig als potentieller "säumiger Schuldner" erkannt wird. Mittlerweile gibt es aber auch Ansätze, wonach die vorhandenen personenbezogenen Daten frühzeitig pseudo- oder gar anonymisiert und dennoch interessante Informationen für die Unternehmen

gewonnen werden (siehe 5. Kapitel).

Insgesamt ist festzuhalten: Aus der Zielsetzung des DWH-Konzeptes folgt, dass wenigstens in einzelnen Phasen des Umgangs mit den Daten diese zumindest personenbeziehbar und damit personenbezogene Daten sind.

Gemäß § 4 Abs. 1 BDSG sind die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit

- das BDSG es erlaubt,
- eine andere Rechtsvorschrift es zulässt oder
- der Betroffene eingewilligt hat.

Die Zulässigkeit des Umgangs mit personenbezogenen Daten nach dem BDSG und den Landesdatenschutzgesetzen wird unter 6.2, die aufgrund einer Einwilligung unter 6.3 untersucht.

## 6.2 Zulässigkeit nach den Datenschutzgesetzen

### 6.2.1 Nicht-öffentlicher Bereich

Im Folgenden sollen die wesentlichen Probleme, die sich aus datenschutzrechtlicher Sicht bei einem DWH ergeben können, aufgezeigt werden. Dabei werden zunächst die nicht-öffentlichen Stellen betrachtet, bevor unten (6.2.2) speziell und ausführlicher auf die Besonderheiten von DWH in der öffentlichen Verwaltung eingegangen wird.

Die Ermächtigung der datenverarbeitenden Stelle, personenbezogene Daten in einem DWH zu verarbeiten, kann sich - wie oben (6.1) gezeigt - unter anderem aus dem BDSG ergeben. Als Rechtsvorschrift i. S. v. § 4 Abs. 1 BDSG kommt zunächst die allgemeine Datenverarbeitungsvorschrift für den nicht-öffentlichen Bereich, § 28 BDSG, in Betracht. § 28 BDSG gestattet das Speichern, Verändern, Übermitteln oder Nutzen personenbezogener Daten für die Erfüllung eigener Geschäftszwecke unter bestimmten Voraussetzungen.

So könnte möglicherweise der *Vertragszweck* (§ 28 Abs. 1 S. 1 Nr. 1 BDSG) den Betrieb eines DWH decken. Da die Daten jedoch langfristig gespeichert werden und gerade nicht nur als operative Datenbasis zur Durchführung einzelner Geschäftsvorgänge dienen, weicht die vom Vertrag gedeckte von der im DWH vorgesehenen Nutzung der Daten ab und entfällt somit als Rechtsgrundlage.

So schließt beispielsweise der Kunde einer Bank den Vertrag zur Abwicklung von Zahlungstransaktionen. Die Ausführung der entsprechenden Anweisung durch die Bank erfordert die Verarbeitung zahlreicher Datensätze (u. a. die Übermittlung des Zahlungsgrundes). Die Bank übermittelt diese Informationen lediglich im Auftrag ihres Kunden während der Ausführung der Transaktion (Vertragszweck). Der Zahlungsgrund ist kein Vertragsdatum der Bank und darf deshalb nach Abschluss der Transaktion von ihr für eigene Zwecke nicht länger gespeichert und ausgewertet werden.

Folglich entfällt mit Erfüllung des jeweiligen Vertragszwecks die Erlaubnis zur Datenverarbeitung nach § 28 Abs. 1 S. 1 Nr. 1 BDSG. Das gleiche gilt für vertragsähnliche Vertrauensverhältnisse im Sinne dieser Vorschrift. § 28 Abs. 1 S. 1 Nr. 1 BDSG würde die Speicherung und weitere Verarbeitung in einem DWH nur dann erlauben, wenn gerade dies Vertragszweck wäre. Davon ist in der Regel nicht auszugehen.

Die Datenverarbeitung im DWH könnte weiterhin aufgrund einer *Interessenabwägung* gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG zulässig sein. Dabei ist zu beachten, dass die Vorschrift kein Auffangtatbestand zu § 28 Abs. 1 S. 1 Nr. 1 BDSG ist, so dass nach Nr. 1 erforderliche Daten nicht nach Nr. 2 zu anderen Zwecken verarbeitet oder genutzt werden können.

Nach § 28 Abs. 1 S. 1 Nr. 2 BDSG müsste einerseits das Speichern bestimmter Daten im DWH der Wahrung berechtigter Interessen des Betreibers dienen. Dass mit dem Betrieb eines DWH tatsächlich berechtigte Interessen eines Unternehmens gewahrt werden können (welche auch immer das sein mögen), kann nie mit Sicherheit gesagt werden, da der Erfolg der Auswertungen sich vorher überhaupt nicht einschätzen lässt. Darüber hinaus dürfen andererseits schutzwürdige Interessen des Betroffenen der Verarbeitung der Daten im DWH nicht entgegenstehen. Ob die Auswertung der Daten und die Verknüpfung mit anderen Daten sowie die Interpretation des Ergebnisses schutzwürdige Interessen tatsächlich unberührt lässt, darf wohl zu Recht bezweifelt werden. Es ist beispielsweise nicht auszuschließen, dass im Ergebnis der Auswertungen der Betroffene zu Unrecht als potentieller "säumiger Schuldner“ oder aus anderen Gründen als "unzuverlässiger Kunde“ klassifiziert wird. Bereits die Tatsache, dass er als "gläserner Kunde“ geführt wird, dürfte nicht im Interesse des Betroffenen sein.

Es bleibt festzuhalten, dass auch die Interessenabwägung gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG als Rechtsgrundlage für den Betrieb eines DWH mit personenbezogenen Daten ausscheiden dürfte.

Im DWH werden u. U. auch personenbezogene *Daten aus öffentlichen*

*Quellen* verarbeitet. Sofern nicht das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung überwiegt, könnte der Betrieb des DWH dann auf § 28 Abs. 1 S. 1 Nr. 3 BDSG gestützt werden. Diese Vorschrift kann jedoch nicht für das gesamte DWH als Rechtsgrundlage dienen. Selbst für den aus öffentlichen Quellen stammenden Teil der Daten ist zu bezweifeln, ob die Verarbeitung im DWH zulässig ist, da durchaus schutzwürdige Interessen Betroffener überwiegen können, wenn diese Daten mit anderen verknüpft und ausgewertet werden.

§ 28 Abs. 1 S. 1 Nr. 4 BDSG eröffnet Unternehmen eine weitere Möglichkeit, personenbezogene Daten zur Erfüllung eigener Geschäftszwecke zu verarbeiten, wenn nämlich die speichernde Stelle diese Daten *für Zwecke der wissenschaftlichen Forschung* verwendet. Dass ein DWH Forschungszwecken dient, darf jedoch bezweifelt werden, denn die vom Unternehmen beabsichtigte Marktforschung ist vom Gesetzgeber hier nicht gemeint.

Eine weitere Legitimation für die Verarbeitung personenbezogener Daten in einem DWH könnte die *Einwilligung* des Betroffenen sein, vgl. § 4 Abs. 2 BDSG. Hierbei ergeben sich insbesondere Probleme hinsichtlich der Informiertheit des Betroffenen (*informed consent*), da beim DWH vorher die einzelnen Datenverarbeitungsvorgänge noch nicht feststehen. Zur ganzen Thematik wird unten (6.3) ausführlicher Stellung genommen.

### 6.2.2 Öffentlicher Bereich

#### 6.2.2.1 Erheben

Nach § 13 BDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der Daten verarbeitenden Stelle erforderlich ist.

Zu untersuchen ist, ob die Erhebung personenbezogener Daten direkt für die Verwendung im DWH zulässig ist. Dazu müsste das Betreiben eines DWH selbst eine Aufgabe der Daten verarbeitenden Stelle oder für eine andere Aufgabe erforderlich sein. Bestimmungen, die einer Daten verarbeitenden Stelle den Betrieb eines DWH vorschreiben, existieren bislang weder im allgemeinen, noch im bereichspezifischen Datenschutzrecht.

Ein DWH könnte aber für eine andere Aufgabe der Daten verarbeitenden Stelle erforderlich sein. Bei Daten, die in einem DWH verarbeitet werden, steht zum Zeitpunkt ihrer Erhebung/Speicherung nicht fest, auf welche Weise sie ausgewertet, mit welchen anderen Daten sie verknüpft , welche neuen

Informationen durch ihr Hinzukommen zu den anderen Daten gewonnen und wie diese Informationen - und damit auch die erhobenen Daten - genutzt werden. Zumindest für die typischen öffentlichen, dem allgemeinen (Datenschutz-)Recht unterliegenden Stellen, die Aufgaben der Eingriffs- und Leistungsverwaltung erfüllen, ist eine solche Datenerhebung nicht zulässig. Denn Daten, von denen man bei der Erhebung noch nicht weiß, wofür sie "gut" sind, können zur Erfüllung einer konkreten Aufgabe eines staatlichen Eingriffs oder einer Leistungsgewährung nicht erforderlich sein. Dass sie dafür u. U. nützlich sein können, reicht nicht aus. Es bleibt eine unzulässige Datenerhebung auf Vorrat. Denkbar wäre eine Erhebung für bereichsspezifisch geregelte spezielle, vor allem statistische Zwecke, oder mit Einwilligung des Betroffenen (Abschnitt 6.3).

Etwas anderes könnte für Datenerhebungen zu wissenschaftlichen Zwecken gelten, da Datenumgang im Forschungsbereich durch das Datenschutzrecht privilegiert wird. Auch könnte die Sammlung und Auswertung verschiedenartiger personenbezogener Daten durch DM-Technologien für die Forschung vielversprechend sein. So schreibt § 40 Abs. 1 BDSG lediglich vor, dass für wissenschaftliche Zwecke erhobene Daten nur für solche Zwecke verarbeitet werden dürfen. Dem Wortlaut nach verlangt sie keine vorhergehende Festlegung des genauen Forschungszweckes. Die originäre Datenerhebung zu Forschungszwecken wäre aber wiederum nur aufgrund einer speziellen Rechtsvorschrift oder einer Einwilligung zulässig. Da Rechtsvorschriften, die eine Erhebung zu Forschungszwecken vorsehen, nicht ersichtlich sind, bleibt als Legitimation nur die Einwilligung der Betroffenen. Für diese gilt das unten im Punkt 6.3 Ausgeführte. Damit ist auch hier zweifelhaft, ob die Datenerhebung zum Zwecke der Auswertung in einem DWH zulässig ist.

Insgesamt ist festzuhalten, dass die Erhebung personenbezogener Daten für den Zweck der Verwendung in einem DWH i. d. R. nicht durch Vorschriften des allgemeinen Datenschutzrechts gerechtfertigt werden kann.

#### 6.2.2.2 Verarbeiten

Gemäß § 3 Abs. 5 S. 1 BDSG ist Verarbeiten das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

Eine wichtige Form der Verarbeitung ist das *Speichern*. Das Speichern personenbezogener Daten ist nach § 14 Abs. 1 BDSG zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben bzw., wenn keine Erhebung vorausgegangen ist, gespeichert worden sind.

In 6.2.2.1 wurde dargelegt, dass die Erhebung von personenbezogenen Daten für die Verwendung in einem DWH unzulässig ist. Die dort angestellten Überlegungen gelten auch für eine unmittelbare Speicherung ohne vorangehende Erhebung. Somit kommt eine Speicherung nach § 14 Abs. 1 BDSG grundsätzlich nicht in Betracht.

Die Speicherung personenbezogener Daten, die für andere Zwecke erhoben oder erstmals gespeichert worden sind, (Zweckänderung) richtet sich nach § 14 Abs. 2 BDSG(-E) und wird ausführlich in 6.2.2.3 behandelt.

Für das *Verändern, Übermitteln, Sperren* und *Löschen* personenbezogener Daten, welche in einem DWH gespeichert sind, ergeben sich bei der Anwendung der einschlägigen Vorschriften keine rechtlichen Besonderheiten. In technischer Hinsicht kann es insoweit Probleme geben, als das Berichtigen, Sperren oder Löschen als Rechtsfolge sich nicht nur auf sämtliche Kopien eines Datums sondern vor allem auch auf solche Daten und Informationen auswirkt, die durch Verarbeitung und Nutzung des in Rede stehenden Datums entstanden sind. Ähnliche Schwierigkeiten können bei den Verarbeitungsformen *Anonymisieren* und *Pseudonymisieren* entstehen.

### 6.2.2.3 Zweckbindung

Wie in 6.2.2.1 gezeigt, werden personenbezogene Daten von öffentlichen Stellen zulässigerweise dann erhoben, wenn dieses zu deren Aufgabenerfüllung erforderlich ist, vgl. § 13 BDSG. Alle weiteren Datenverarbeitungsvorgänge, wie z. B. Speichern (siehe 6.2.2.2) und Nutzen, setzen voraus, dass die Daten für den Zweck verarbeitet werden, für den sie erhoben worden sind.

Bei einem DWH einer öffentlichen Stelle sind die Daten in aller Regel nicht zum Zwecke der weiteren Auswertung in einem DWH erhoben worden. Sinn des DWH ist es ja gerade, dass die Daten für Zwecke verarbeitet und vor allem genutzt werden, die mit dem ursprünglichen Erhebungszweck nichts zu tun haben. Die Daten werden für die operative Aufgabenerfüllung nicht mehr benötigt. Sieht man von dem Fall ab, dass die Daten eigens zum Zwecke der Auswertung in einem DWH erhoben worden sind, so ist in den übrigen Fällen für das Nutzen der Daten in einem DWH eine Änderung des Erhebungszwecks - also eine Durchbrechung der Zweckbindung - erforderlich.

Alle Datenschutzgesetze enthalten Ausnahmetatbestände, nach denen Daten auch zu einem anderen als dem Erhebungszweck genutzt werden dürfen. Die einzelnen Vorschriften in den Bundesländern und im BDSG ähneln sich dabei

mehr oder weniger stark. Hier wird wie oben auf § 14 BDSG und zwar dessen Abs. 2, abgestellt. Mit jeder Zweckänderung ist ein neuer Eingriff in das Recht auf informationelle Selbstbestimmung verbunden. Die Ermächtigung zur Zweckänderung in § 14 Abs. 2 BDSG ist wegen der Bedeutung des Grundrechts eng auszulegen.

Die Zweckänderung könnte zulässig sein, weil eine *Rechtsvorschrift* dies vorsieht oder zwingend voraussetzt, § 14 Abs. 2 Nr. 1 BDSG. Eine Rechtsvorschrift, die das zweckverändernde Nutzen von Daten in einem DWH ausdrücklich zulässt, ist nicht ohne Weiteres erkennbar. Dasselbe gilt für eine Rechtsvorschrift, die eine solche Zweckänderung *zwingend voraussetzt*. Abgesehen von den verfassungsrechtlichen Zweifeln an dieser Formulierung, müsste es sich zumindest um eine Rechtsvorschrift handeln, die nicht ausgeführt werden kann, ohne dass die Daten zweckändernd in einem DWH ausgewertet werden. Eine solche Rechtsvorschrift ist nicht denkbar und würde auf jeden Fall gegen das vom BVerfG in seinem Volkszählungsurteil geforderte Gebot der Normenklarheit verstoßen.

Eine weitere Möglichkeit der zulässigen Zweckänderung mit dem Ziel der Auswertung in einem DWH wäre die *Einwilligung* des Betroffenen, § 14 Abs. 2 Nr. 2 BDSG. Dies soll hier nicht weiter besprochen werden, sondern wird unter 6.3 gesondert behandelt.

Weiterhin kommt gemäß § 14 Abs. 2 Nr. 3 BDSG in Betracht, dass die Zweckänderung *offensichtlich im Interesse des Betroffenen* liegt und nicht davon auszugehen ist, dass er in Kenntnis der Zweckänderung seine Einwilligung verweigern würde. Diese Lösung dürfte ebenfalls ausscheiden. Die Vorschrift verlangt, dass der Betroffene klar überwiegende unmittelbare Vorteile davon hat, dass seine ursprünglich zu einem anderen Zweck erhobenen Daten in einem DWH ausgewertet werden. Das kann in der Regel nicht angenommen werden. Zwar mag es zumindest mittelbare Vorteile für die Bürger geben, wenn Daten in einem DWH ausgewertet werden, da sich möglicherweise viele Verwaltungsabläufe auch zum Nutzen der Bürger verbessern lassen könnten. Konkrete Vorteile, die aus der Nutzung gerade seiner Daten entstehen, kann der Betroffene jedoch nicht erlangen. Angesichts der Gefahren, die ein DWH unter Verwendung personenbezogener Daten für das Persönlichkeitsrecht der Betroffenen darstellt, ist vielmehr davon auszugehen, dass ein DWH deutlich mehr Nachteile als Vorteile für den Betroffenen hat. Darüber hinaus kann aus eben diesen Gründen auch nicht angenommen werden, dass ein Betroffener seine Einwilligung erteilen würde, weshalb die Voraussetzungen des § 14 Abs. 2 Nr. 3 BDSG schon deshalb nicht gegeben sind.

§ 14 Abs. 2 Nr. 4 BDSG scheidet als Legitimation für die Zweckbindung von vornherein aus, da die Nutzung in einem DWH in keinem Zusammenhang mit der Unrichtigkeit von Daten steht und der Sinn des DWH nicht in der *Korrektur unrichtiger Daten* liegt.

Stammen die Daten aus *allgemein zugänglichen Quellen,* ist unter den weiteren Voraussetzungen von § 14 Abs. 2 Nr. 5 BDSG ebenfalls eine Zweckänderung möglich. Sollen solche Daten in einem DWH genutzt werden, entstehen allerdings die gleichen Probleme, die oben unter 6.2.1 hinsichtlich § 28 Abs. 1 S. 1 Nr. 3 BDSG beschrieben wurden. Die Nutzung wird in der Regel also spätestens an den überwiegenden schutzwürdigen Interessen der Betroffenen, die Zweckbindung einzuhalten, scheitern.

Die Zusammenhänge, die mit einem DWH untersucht und festgestellt werden sollen, dienen - abgesehen von dem Fall, dass die Daten eigens zu diesen Zwecken erhoben worden sind - weder der *Strafverfolgung* oder *-vollstreckung* noch der *Abwehr von Gefahren für die öffentliche Sicherheit*. Insofern kommen nach § 14 Abs. 2 Nr. 6 und 7 BDSG keine Zweckänderungen zugunsten der Nutzung in einem DWH in Betracht.
Ebensowenig sind Fälle denkbar, bei denen die zweckändernde Nutzung von Daten in einem DWH zur *Abwehr schwerwiegender Beeinträchtigungen der Rechte einer anderen Person* erforderlich ist, so dass auch § 14 Abs. 2 Nr. 8 BDSG als Rechtsgrundlage ausscheidet.

Die Zweckänderung nach § 14 Abs. 2 Nr. 9 BDSG (die Daten sind für die Durchführung *wissenschaftlicher Forschung* erforderlich) ist schon deshalb zweifelhaft, weil es sich um ein bestimmtes Forschungsvorhaben handeln muss. Dies ist aufgrund der Charakteristik des DWH aber vorher gerade nicht abzusehen. Darüber hinaus wird die Zulässigkeit i. d. R. an den überwiegenden schutzwürdigen Interessen der Betroffenen scheitern, die nicht wissen können, in welcher Art und Weise ihre Daten im DWH verarbeitet werden.

Zusammenfassend lässt sich feststellen, dass die mit einer Änderung des Erhebungszwecks einher gehende Nutzung personenbezogener Daten durch öffentliche Stellen in einem DWH nach § 14 Abs. 2 BDSG im Allgemeinen nicht zulässig ist.

Darüber hinaus könnte die Nutzung personenbezogener Daten in einem DWH nach § 14 Abs. 3 BDSG bzw. den entsprechenden landesrechtlichen Vorschriften zulässig sein. Die Norm stellt klar, dass die Nutzung personenbezogener Daten zu den dort genannten Zwecken (Aufsicht, Rechnungsprüfung) keine Änderung des Erhebungszwecks darstellt, sondern

von diesem Primärzweck mit umfasst ist. Zu beachten ist, dass § 14 Abs. 3 BDSG keine eigenständige Befugnis ist, personenbezogene Daten zu den dort genannten Zwecken zu verarbeiten oder zu nutzen. Die Verarbeitung bzw. Nutzung muss selbstverständlich trotzdem zur Aufgabenerfüllung i. S. v. § 14 Abs. 1 BDSG erforderlich sein.

In Betracht kommt hier eine Nutzung der Daten für Organisationsuntersuchungen gemäß § 14 Abs. 3 S. 1 BDSG. Bei solchen Untersuchungen sind vor allem Personaldaten der Beschäftigten betroffen, deren zulässige Verarbeitung nach bereichsspezifischem Recht (z. B. § 29 BbgDSG) zu beurteilen wäre. Auf diese Thematik wird nicht weiter eingegangen.

Nach dem *BDSG-E* ergeben sich hinsichtlich der obigen Ausführungen keine Änderungen, da die Vorschrift des § 14 Abs. 2 und 3 BDSG weitgehend unverändert fortgelten soll. Neu ist gemäß § 14 Abs. 5 BDSG-E allerdings, dass im Vergleich zu § 14 Abs. 2 und 3 BDSG(-E) bei den besonders sensiblen Daten i. S. v. Art. 8 der EG-Datenschutzrichtlinie (§ 3 Abs. 9 BDSG-E) eine wesentlich strengere Zweckbindung gilt. Die Befugnisse zur zweckändernden Verarbeitung sind bei diesen Daten folglich noch stärker beschränkt worden. Bei diesen Daten gilt deshalb erst recht, dass eine personenbezogene Speicherung in einem DWH nicht nach § 14 BDSG(-E) zulässig wäre.

## 6.3 Einwilligung

### 6.3.1 Allgemeine Voraussetzungen nach den Datenschutzgesetzen

Eine mögliche Legitimation zur Verarbeitung personenbezogener Daten durch öffentliche Stellen stellt die *Einwilligung* des Betroffenen dar. Grundsätzlich ist jeder Datenverarbeitungsvorgang erlaubt, soweit der Betroffene darin eingewilligt hat, vgl. nur § 4 Abs. 1 BDSG. Im öffentlichen Bereich gilt dies aber nur sehr eingeschränkt. Wenn auch scheinbar ein gleichberechtigtes Verhältnis zwischen Einwilligung und der Erlaubnis zur Datenverarbeitung aufgrund einer Rechtsvorschrift besteht, so kann nicht außer Acht gelassen werden, dass öffentliche Stellen nur ausnahmsweise auf die Einwilligung zurückgreifen können, solange es an einer ausdrücklichen bereichsspezifischen Regelung fehlt. Dies liegt vor allem daran, dass öffentliche Stellen ohnehin darauf beschränkt sind, ihren gesetzlich und verfassungsrechtlich zugewiesenen Aufgaben nachzugehen. Eine Datenverarbeitung, die außerhalb der Aufgabenerfüllung der öffentlichen Stelle stattfindet, kann deshalb grundsätzlich auch nicht durch die Einwilligung des Betroffenen legitimiert werden.

Dies vorausgesetzt sind eine Reihe von besonderen Anforderungen an die Form und den Inhalt von Einwilligungen zu stellen. Formal bedarf die Einwilligung grundsätzlich der Schriftform und muss in bestimmter Art und Weise erkennbar gemacht werden.

Inhaltlich ist vor allem wichtig, dass die Einwilligung so bestimmt ist, dass der Betroffene weiß, worin er einwilligt und deren Tragweite erkennt. Dies hat bestimmte Informationspflichten der datenverarbeitenden Stelle zur Folge. Nur eine informierte Einwilligung (*informed consent*) ist wirksam. Der Betroffene muss wissen, zu welchem Zweck welche Daten gespeichert, übermittelt oder sonst verarbeitet werden. Bei Übermittlungen muss ihm auch der Adressatenkreis bekannt sein.

### 6.3.2 Einwilligung und DWH

Legt man die oben beschriebenen Anforderungen an Wirksamkeit und Zulässigkeit einer Einwilligung zugrunde, so ist fraglich, ob ein Betroffener der Verarbeitung seiner personenbezogenen Daten in einem DWH einschließlich notwendiger Zweckänderungen in diesem Sinne zustimmen kann.

Wie schon mehrfach ausgeführt, gehört das Betreiben eines DWH nicht zu den Aufgaben einer öffentlichen Stelle und ist zu deren Erfüllung nicht erforderlich. Deshalb ist es zweifelhaft, ob dies durch eine Einwilligung umgangen werden kann. Wäre dies zulässig, würde die öffentliche Stelle außerhalb der ihr zustehenden Aufgaben personenbezogene Daten verarbeiten. Die Datenverarbeitung würde auf der Basis einer Einwilligung durchgeführt, die zu erteilen der Betroffene sich angesichts des hoheitlichen Charakters staatlicher Tätigkeit möglicherweise gar gezwungen sieht.

Selbst wenn man die oben genannten Bedenken ausräumen könnte, so wäre die Einwilligung auch aus anderen Gründen in jedem Fall unwirksam. Bei einem DWH ist es weder möglich vorherzusagen, welche Datenverarbeitungsvorgänge stattfinden, was deren Ergebnis ist, noch für welchen Zweck die im DWH ablaufenden Verarbeitungsvorgänge im Einzelnen jeweils erfolgen. Der Verarbeitungszweck ergibt sich gerade erst aus den Ergebnissen nicht im Einzelnen vorhersehbarer Verarbeitungsvorgänge. Eine informierte Einwilligung wie sie § 4 Abs. 2 BDSG und die entsprechenden Vorschriften der LDSG verlangen, kann daher nicht erteilt werden.

Das Betreiben eines DWH durch öffentliche Stellen aufgrund einer Einwilligung nach § 4 Abs. 1, 2 BDSG ist deshalb nicht möglich. Da die Anforderungen an die Einwilligung bei den bereichsspezifischen

Datenschutzvorschriften entweder in etwa denen des BDSG entsprechen oder noch höher sind, gilt dies auch dort. Diese Problematik wird daher nicht gesondert ausgeführt.

# 7. Datenschutzfreundliche Technologien und DWH

## 7.1 Einführung

Die Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten, wie in einem DWH, und damit auch ihre Akzeptanz beim Betroffenen/Kunden hängt in hohem Maße davon ab, inwieweit sie nach dem Prinzip der *Datensparsamkeit* erfolgt. Es verlangt, so wenig personenbezogene Daten wie möglich zu erheben, verarbeiten und zu nutzen. *Datenvermeidung* ist die stets anzustrebende Form der Datensparsamkeit. In diesem Fall werden bei der Nutzung von Informations- und Kommunikationssystemen keine personenbezogenen Daten erhoben, verarbeitet und genutzt.

Bereits heute ist eine Reihe von Techniken und Hilfsmittel zur Umsetzung der Philosophie der Datenvermeidung und der Datensparsamkeit verfügbar. Die Technologie, die dafür gesorgt hat, dass personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, ist auch zur Wahrung der Privatheit des Einzelnen nutzbar. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff *"Privacy enhancing technology"* (PET) bezeichnet wird, umfasst ein ganzes System technischer Maßnahmen.
Im Abschnitt 7.2 werden die Methoden Anonymisierung, Pseudonymisierung und der *Identity Protector* ( I. P.) vorgestellt, die wichtigsten Realisierungshilfen dazu genannt und schließlich allgemeine Empfehlungen zur Implementierung eines datenschutzfreundlichen DV-Systems gegeben. Unter 7.3 wird dann - was schon in Kapitel 5 angesprochen wurde - ausführlich untersucht, wie mit Hilfe von PET datenschutzrechtliche Probleme bei der Datenverarbeitung im DWH gelöst werden können.

## 7.2 Methoden und Werkzeuge

### 7.2.1 Anonymisierung

Anonymisierung ist eine Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

In den Datenschutzgesetzen von Bund und Ländern ist Anonymisierung unterschiedlich definiert. So ist in einigen Datenschutzgesetzen (z. B. § 3

Abs. 7 BDSG, Art. 4 Abs. 8 BayDSG, § 3 Abs. 7 LDSG RP, § 2 Abs. 7 DSG-LSA) für eine Anonymisierung bereits "das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" ausreichend. Andere Datenschutzgesetze (z. B. § 3 Abs. 7 Nr. 5 DSG MV, § 3 Abs. 2 Nr. 4 SächsDSG, § 2 Abs. 2 Nr. 7 LDSG SH) stellen höhere Anforderungen. Hier wird unter Anonymisieren "das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse *nicht mehr* einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können", verstanden.

Die Qualität der Anonymisierungsprozedur hängt von verschiedenen Einflussfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen.

Auch konkrete Einzelangaben in einem Datensatz/einer Transaktion (z. B. Beruf/Amt = Bundeskanzler, konkrete Einkommensangaben) sind für die Qualität der Anonymisierungsprozedur von Bedeutung und können die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, verringern. Sind im Wertebereich Werte vorhanden, die die Anonymität gefährden, müssen sie mit anderen zusammengefasst werden. Ist eine solche Veränderung aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.

Das Ziel datenschutzfreundlicher Technologien ist es unter anderem, Daten schon ohne Personenbezug zu erheben oder bereits personenbezogen erhobene Daten so bald wie möglich zu anonymisieren. Ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen. Gelungene Beispiele hierfür sind anonyme Telefonkarten und anonyme Zahlkarten im öffentlichen Personennahverkehr. Beispiele für die Anwendung der Anonymisierung sind im Bereich der Statistik und in der Forschung zu finden.

### 7.2.2 Pseudonymisierung

Pseudonymisierung ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.

Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können. Die Reidentifizierung kann mitunter auch ausschließlich dem Betroffenen vorbehalten bleiben.

Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo Anonymisierung nicht möglich ist.

Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflussfaktoren ab, wie die Stärke der Anonymisierungsprozedur, nämlich vom Zeitpunkt der Pseudonymisierung, von der Rücknahmefestigkeit der Pseudonymisierungsprozedur, von der Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und von der Verkettungsmöglichkeit von einzelnen Transaktionen/Datensätzen desselben Betroffenen. Insbesondere können Transaktionen/Datensätze, die unter demselben Pseudonym getätigt/gespeichert wurden, miteinander verkettet werden.

Unter gleichen Bedingungen ist die Anonymisierung datenschutzfreundlicher als die Pseudonymisierung. Das Pseudonym kann dazu benutzt werden, den Personenbezug wiederherzustellen. Ansonsten kann ohne Berücksichtigung der genannten Faktoren nicht pauschal beurteilt werden, ob die Anonymisierung oder die Pseudonymisierung datensparsamer ist.

Je nach Verknüpfbarkeit und dem Geheimnisträger des Pseudonyms kann der Personenbezug

- nur vom Betroffenen (selbstgenerierte Pseudonyme),
- nur über eine Referenzliste (Referenz-Pseudonyme) oder
- nur unter Verwendung einer sog. Einweg-Funktion mit geheimen Parametern (Einweg-Pseudonyme)

wiederhergestellt werden.

Pseudonyme ermöglichen es, den Personenbezug herzustellen, so dass die Identität der Person nur in den vorab bestimmten Einzelfällen erkennbar wird.

Pseudonyme sollen zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme soll so mächtig sein, dass bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym generiert wird. Ist eine hohe Sicherheit erforderlich, muss die Menge der Pseudonymkandidaten mindestens so mächtig sein, wie der Wertebereich sicherer kryptographischer

Hashfunktionen.

Pseudonyme sollten insbesondere nicht anwendungsübergreifend, sondern nur für jeweils ein Verfahren eingesetzt werden. Jede anwendungsübergreifende Benutzung eines einzigen Pseudonyms würde die Gefahr erhöhen, dass aus sämtlichen, mit dem Pseudonym verbundenen Daten ein detailliertes Personenprofil erstellt werden kann, das wiederum den Rückschluss auf eine bestimmte Person erleichtert. Aber auch innerhalb einer Anwendung ist die Verwendung nur eines einzigen Pseudonyms nicht unproblematisch.

### 7.2.3 Der Identity Protector

DV-Systeme, für die eine anonyme Nutzungsform nicht vollständig möglich ist, sollten derart in unterschiedliche Einzelprozesse zerlegt werden, dass unmittelbar personenbezogene Daten (Identitätsdaten) nur erhoben, gespeichert und verarbeitet werden, wo dies unabdingbar nötig ist.

Durch geeignete technische Maßnahmen muss dafür Sorge getragen werden, dass die Bereiche des DV-Systems, die den vollen Personenbezug mit den Identitätsdaten benötigen, strikt von jenen getrennt werden, die nur mit einem Pseudonym auskommen. D. h. nur die tatsächlich und unmittelbar benötigten Daten stehen dem jeweiligen Prozess zur Verfügung. Eine Zusammenführung von Identitätsdaten und Pseudonymdaten ist nur unter vorab und genau definierten Umständen möglich.

Diese Aufgaben kann ein I. P. leisten. Er kann als Systemelement (Prozess) betrachtet werden, das den Austausch von Identitätsdaten und Pseudonymdaten zwischen den übrigen Systemelementen steuert.

Für einen I. P. sind verschiedene Ausprägungsformen möglich:

a) eigenständiges Element in einem DV-System,
b) eigenständiges DV-System, das unter der Kontrolle des Benutzers steht,
c) eigenständiges DV-System, das unter der Kontrolle einer Vertrauensstelle steht.

Im Falle a) sollte der I. P. ein - auch für den Betreiber des DV-Systems - unveränderbarer Baustein sein. Die Realisierung ließe sich als Softwarebaustein im DV-System selbst, im zugrundeliegenden Betriebssystem oder auch als Hardwarekomponente mit zugehöriger Software (z. B. als "Black-Box-Lösung") bewerkstelligen.

Im Falle b) wäre eine Abbildung des I. P. z. B. in Form einer Smart-Card möglich.

Der I. P. kann folgende Funktionalitäten leisten:

- kontrollierte Offenlegung und Freigabe der Identität,
- Generierung von Pseudonymen,
- Umsetzung von Pseudonymen in weitere Pseudonyme,
- Umsetzung von Identitäten in Pseudonyme (Pseudonymisierung),
- Umsetzung von Pseudonymen in Identitäten (Depseudonymisierung),
- vorbeugende Missbrauchsbekämpfung (u. a. durch die erstgenannte Funktionalität).

### 7.2.4 Realisierungshilfen

Als Hilfsmittel zur Umsetzung der in 7.2.1 bis 7.2.3 dargestellten Methoden kommen vor allem folgende Werkzeuge in Betracht:

- Hashfunktionen
- (blinde) digitale Signaturen
- (Signaturschlüssel-)Zertifikate
- biometrische Verfahren
- Vertrauensstellen (Trust Center)

### 7.2.5 Empfehlungen zur Vorgehensweise

Um die o. g. Grundsätze bei der Entwicklung oder Modifizierung von DV-Systemen in ausreichendem Maße berücksichtigen zu können, ist folgende Vorgehensweise empfehlenswert:

Zunächst müssen Daten verarbeitende Systeme und Teilsysteme einschließlich ihrer Schnittstellen definiert werden. Bei dieser Definition muss auch eine Unterscheidung derjenigen Systeme und Teilsysteme erfolgen, in denen

- ohne personenbezogene Daten gearbeitet werden kann,
- personenbezogene Daten anonymisiert werden können,
- personenbezogene Daten pseudonymisiert werden können bzw.
- der direkt herstellbare Personenbezug unvermeidlich ist.

Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System/Teilsystem eine entsprechende Prozedur zu finden,

- die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert,
- die nicht unzulässig beeinflusst (Integrität) werden kann,
- die aus dem System/Teilsystem nicht mit geringem Aufwand wieder entfernt werden kann (Rücknahmefestigkeit),
- die den Betroffenen in einer hinreichend großen Menge möglicher Betroffener verbirgt und
- die die Verkettbarkeit von Einzeldaten oder Transaktionen zu Datenspuren unterdrückt.

Stellt sich heraus, dass die vorhandenen Risiken mit dem so konstruierten System nicht hinreichend reduziert werden können, so müssen ggf. Teile des Definitionsprozesses und Teile des Gestaltungsprozesses wiederholt werden.

## 7.3 Anwendung datenschutzfreundlicher Technologien auf DWH

### 7.3.1 Grundsatz

Aus Kapitel 6 folgt, dass in einem DWH grundsätzlich keine personenbezogenen Daten gespeichert, auf sonstige Weise verarbeitet oder genutzt werden können. Damit ist ein wichtiger Teil der o. g. Zielsetzung des DWH-Konzeptes im öffentlichen Bereich nicht umsetzbar. Das Betreiben eines DWH kann aber auch ohne die Verwendung personenbezogener Daten sinnvoll sein, beispielsweise dann, wenn es um statistische Aussagen und Gruppenverhalten geht.

Auch für ein "anonymes" DWH bildet die vorhandene operative Datenbasis, welche u. a. alle im Tagesgeschäft anfallenden personenbezogenen Daten enthält, die Grundlage für die zu verarbeitenden Daten. Dazu müssen die Daten der operativen Datenbasis unter Einsatz der PET und der dargelegten Vorgehensweise anonymisiert im DWH gespeichert werden.

### 7.3.2 Form der Speicherung der operativen Datenbasis

#### 7.3.2.1 Speicherung in einem Datensatz

Zunächst soll der einfache Fall betrachtet werden, dass die in der operativen Datenbasis gespeicherten personenbezogenen Daten von jeder Person (rechtmäßig - davon wird im Folgenden ausgegangen) in einem einzigen Datensatz gespeichert sind. Dann dürfen die Datensätze nur mit einer reduzierten Anzahl von Datenfeldern in das DWH übertragen werden. Gemäß dem Abschnitt 7.2.1 müssen alle Felder entfernt werden, die einen unmittelbaren (Name) oder einen mittelbaren Personenbezug ermöglichen.

Letzteres kann sich wie oben ausgeführt aus einzelnen Werten oder aus der Kombination der in verschiedenen Datenfeldern des selben Datensatzes enthaltenen Werten ergeben.

Ist der Personenbezug nur für wenige Personen über den Wert eines bestimmten Datenfeldes möglich, so könnte auch daran gedacht werden, auf die Übertragung aller Werte für diese Personen zu verzichten, dafür aber das besagte Datenfeld mit seinen Werten für die anderen Personen in das DWH zu übernehmen. Eine andere Möglichkeit wäre, die Wertemenge so zu vergröbern, dass ein Personenbezug nicht mehr hergestellt werden kann.

7.3.2.2 Speicherung in einer Datenbank

Komplizierter wird es, wenn die personenbezogenen Daten der einzelnen Personen in verschiedenen Datensätzen in einer Datenbank gespeichert sind. Im Allgemeinen gibt es sog. Schlüssel(-Felder), über die die Datensätze, welche die Daten zur selben Person enthalten, miteinander verknüpft werden können. Bei dieser Verbindung der Datenfelder zu einer Person sind dann die im vorstehenden Absatz ausgeführten Überlegungen anzustellen. Die technische Umsetzung für die überwiegend anzutreffenden relationalen Datenbanken erfolgt in der Weise, dass über eine Datenbankabfragesprache, beispielsweise SQL, ein mehrstufiger Programmbefehl abgesetzt wird, der mit Hilfe der Schlüsselfelder das Kreuzprodukt der betreffenden Datensätze bildet (Join), davon die interessierenden Datenfelder auswählt (Select) und diese schließlich in das DWH überträgt (Export). Gegen die kurzfristige Speicherung aller Datenfelder zu einer Person im Kreuzprodukt der Datensätze während der Befehlsausführung bestehen keine datenschutzrechtlichen Bedenken.

7.3.2.3 Speicherung in verschiedenen Datenbank(system)en

Sind die Daten zu einer Person in logisch und physisch verschiedenen Datenbank(system)en gespeichert, so kann i. d. R. nicht einfach wie im o. g. Fall ein mehrstufiger Programmbefehl formuliert werden, der dann das gewünschte Ergebnis liefert. Vielmehr müssen erst die technischen Grundlagen für eine Verknüpfung der Datensätze geschaffen werden. Hierbei müssen voraussichtlich folgende Schritte durchgeführt werden:

- Zurverfügungstellung entsprechenden Speicherplatzes
- Transport der von verschiedenen Systemen und Speicherorten kommenden Datensatzkopien wohl mit Betriebssystembefehlen zum neuen Speicherplatz
- Anpassung der unterschiedlichen Formate
- Übertragung der zuvor mittels der Dateibeschreibungen ausgewählten

Felder, die weder allein noch kombiniert einen Personenbezug ermöglichen, in das DWH
- Löschung der zwischengespeicherten Daten

Probleme bereitet hier die zeitlich nicht unerhebliche Zwischenspeicherung der personenbezogen zusammengeführten Datensätze, die - wie in 6.2.2.3 dargelegt - grundsätzlich als Verstoß gegen § 14 BDSG(-E) unzulässig sein dürfte. Eine Lösung könnte sein, dass die einzelnen Schritte vom Transport der Daten auf den neu geschaffenen Speicherplatz bis hin zur Löschung aller zwischengespeicherten Daten in einer Art "black box" so miteinander verkettet ablaufen, dass ein Zugriff auf die Daten weder während des normal ablaufenden Prozesses noch bei dessen (von außen erzwungener) Unterbrechung möglich ist.

7.3.2.4 "Anonymisierungs-Black-box"

Zur Anonymisierung bietet sich eine Variante des in 7.2.3 beschriebenen I. P. an. Kontrolliert von einer Vertrauensstelle sollte ein von ihr signierter *String* eingegeben werden können. Dieser enthält die Bezeichnung der keinen Personenbezug ermöglichenden Datenfelder, die in das DWH übertragen werden können. Der *String* ist der Daten verarbeitenden Stelle zwar bekannt - sinnvoller Weise sogar von ihr vorgeschlagen -, kann aber nicht mehr von ihr geändert, insbesondere nicht erweitert werden. Statt der Pseudonymisierungsfunktion hätte der I. P. eine Anonymisierungsfunktion, die zwei Operationen durchführt: kontrollierte Ausgabe nur der im String vorgegebenen Datenfelder, anschließend Löschung sämtlicher Daten. Diese beiden Operationen dürfen dabei nicht von der kritischen Prozedur der personenbezogenen Verknüpfung der verschiedenen Datensätze getrennt werden können. Die für den I. P. vorgesehene Funktionskombination "vorbeugende Missbrauchsbekämpfung durch kontrollierte Offenlegung und Freigabe der Identität" muss dabei - kontrolliert, versiegelt und möglichst zertifiziert - so eingestellt sein, dass die Preisgabe der Identität überhaupt nicht möglich ist.

Von den in 7.2.3 genannten drei Ausprägungsformen des I. P. sollte "c) eigenständiges DV-System, das unter der Kontrolle einer Vertrauensstelle steht" gewählt werden. "Kontrolle" bedeutet hier nicht notwendig, dass die Vertrauensstelle den I. P. ständig beaufsichtigt oder gar den alleinigen Zugriff auf ihn hat. Es genügt, wenn der I. P. von der Vertrauensstelle so (kryptographisch) sicher "abgeschlossen" und gegebenenfalls physisch versiegelt worden ist, dass der Daten verarbeitenden Stelle ein Zugriff auf personenbezogene Daten ohne Kenntnis des Schlüsselwortes auch durch Manipulation oder Zerstörung des I. P. nicht möglich ist.

## 8. Schlussfolgerungen

Die o. g. Betrachtungen machen deutlich, dass für das Betreiben eines DWH mit personenbezogenen Daten derzeit keine Rechtsgrundlage existiert. Im Grunde genommen ist das aber keine neue Erkenntnis.

Das BVerfG hat bereits 1969 festgestellt, dass es mit der Menschenwürde unvereinbar sei, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und katalogisieren. Spätestens nach dem Volkszählungsurteil ist auch klar, dass die Sammlung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zulässig ist. Solche Datensammlungen könnten beispielsweise Basis für die Erstellung detaillierter Persönlichkeitsprofile sein. 1988 stellte deshalb auch der Bundesgerichtshof fest, dass im staatlichen und im privaten Bereich die zwangsweise und heimliche Erstellung solcher Persönlichkeitsprofile verboten ist.

Diese höchstrichterlichen Entscheidungen beschreiben im Grunde genommen genau das DWH-Konzept, ohne diesen Begriff selbst zu nennen. Die Entscheidungen verdeutlichen, dass solche Konzepte mit personenbezogenen Daten grundsätzlich nicht realisiert werden dürfen.

Die EU-Datenschutzrichtlinie kommt zum gleichen Ergebnis. Auch dort wird die Forderung aufgestellt, personenbezogene Daten nur mit einer festgelegten Zweckbestimmung zu verarbeiten (Art. 7), wobei nicht zwischen öffentlichen und nichtöffentlichen Stellen unterschieden wird. Darüber hinaus wird klargestellt, dass besonders sensible Daten, die z. B. politische Meinungen, die Gesundheit oder das Sexualleben betreffen, grundsätzlich nicht verarbeitet werden dürfen (Art. 8). Weiterhin stellt das durch Art. 15 der Richtlinie aufgestellte Verbot automatisierter Entscheidungen, die beispielsweise die Kreditfähigkeit eines Betroffenen bewerten, eine weitere erhebliche Einschränkung für den Betrieb von DWH dar.

Jetzt die Schlussfolgerung zu ziehen, ein DWH dürfte aus datenschutzrechtlicher Sicht grundsätzlich nicht betrieben werden, wäre aber sicher voreilig. Wie insbesondere die Ausführungen im Kapitel 7 gezeigt haben, könnten DWH-Systeme unter Nutzung datenschutzfreundlicher Technologien so konzipiert werden, dass sie den datenschutzrechtlichen Anforderungen genügen. Natürlich sind dann technische und organisatorische Maßnahmen erforderlich, die eine Deanonymisierung verhindern.

Das Ziel, strategisch wichtige Informationen aus einem solchen Datenbestand abzuleiten, kann trotzdem erreicht werden. Durch sinnvolle Aggregierung und Partitionierung von Einzelangaben kann die Herstellung des Personenbezugs verhindert oder wenigstens erheblich erschwert werden. Für bestimmte Kundengruppen beispielsweise könnten trotzdem wertvolle Verkaufsinformationen abgeleitet werden, wobei aus datenschutzrechtlicher Sicht bereits die Zuordnung Einzelner zu solchen Kundengruppen problematisch ist. Das gleiche gilt für die Gewinnung strategischer Erkenntnisse im Bereich der Verwaltung.

Für alle technischen und organisatorischen Maßnahmen, die den Personenbezug der gespeicherten Daten verhindern oder einschränken, gilt jedoch immer, dass sie die Funktionalität des DWH beeinträchtigen. Dennoch muss an die Anwender dieser Technologien appelliert werden, sich im Interesse des Rechts auf informationelle Selbstbestimmung zu beschränken und DWH-Systeme nicht unter Verwendung personenbezogener Daten zu betreiben.

## Literatur


Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: "Datenschutzfreundliche Technologien", Schwerin, 1998

Bizer, J.: "TK-Daten im Data Warehouse", DuD 10/1998

Büllesbach, A.: "Datenschutz bei Data Warehouses und Data Mining", CR 1/2000, S. 11 ff.

Knoll, U.: "Echtes Wissen kommt aus Daten", UNIXopen 11/1998

Management Circle GmbH: Seminarangebot SAP Business Information Warehouse, 1999

Management Circle GmbH: Seminarangebot Praxisleitfaden für erfolgreiche Data-Warehouse-Konzepte, 1999

Möller, F.: "Ungeschliffene Diamanten", Datenschutz Nachrichten 3/1998

Möller, F.: "Data Warehouse als Warnsignal an die Datenschutzbeauftragten", DuD 10/1998

Möncke, U.: "Data Warehouses - eine Herausforderung für den Datenschutz?", DuD 10/1998

Schweizer, A.: "Data Mining Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen", Zürich, 1999

**Anlage 3**

## Hinweise zur Erstellung einer internen Dienstanweisung für brandenburgische Verwaltungen

Stand: September 2000

In seinem Tätigkeitsbericht für 1999 stellt der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht fest: "Verwaltungsinterne Richtlinien zur Anwendung des AIG können die Bearbeitung der Anträge auf Akteneinsicht erleichtern und dadurch beschleunigen." Mit den folgenden Hinweisen möchten wir öffentliche Stellen in Brandenburg bei der Erstellung einer solchen Dienstanweisung unterstützen. Rückfragen zu diesem Thema beantworten wir selbstverständlich gerne.

### 1. Ziel einer Dienstanweisung

- Ziel einer Dienstanweisung zur Anwendung des AIG ist es, dass Anträge auf Akteneinsicht möglichst schnell bearbeitet werden können, damit die zur Einsicht beantragten Informationen nicht unnötig an Aktualität verlieren.

- Gleichzeitig wird eine einheitliche Bearbeitungspraxis in den verschiedenen Organisationseinheiten einer Verwaltung sichergestellt.

### 2. Umfang und Form der Dienstanweisung

- Die Dienstanweisung kann entweder lediglich den Geschäftsgang von Anträgen nach dem AIG bzw. die Zuständigkeiten hierfür regeln oder darüber hinaus inhaltliche Aussagen zur Anwendung und Auslegung des Gesetzes sowie beispielsweise zur Gebührenerhebung nach AIG treffen.

- Für inhaltliche Hinweise zur Antragsbearbeitung können die Ersten Hinweise des Ministeriums des Innern zur Anwendung des AIG (veröffentlicht am 28. September 1998 im Amtsblatt für Brandenburg) herangezogen werden.

### 3. Zuständigkeiten und Geschäftsgang für die Bearbeitung von AIG-Anträgen

- Die/der behördliche Beauftragte für das Recht auf Akteneinsicht sollte an der Bearbeitung der Anträge auf Akteneinsicht beteiligt werden. Hier kommt beispielsweise eine (u.a. im Sinne einer möglichst kurzen Bearbeitungszeit) terminlich und hinsichtlich der Festlegung von Zuständigkeiten für die Bearbeitung koordinierende Funktion in Betracht. Beispielsweise ist es

möglich, grundsätzlich sämtliche eingehenden Anträge auf Akteneinsicht über die/den Beauftragte/n an die Akten führende Stelle weiterzuleiten oder dieser/diesem, um einen Zeitverlust zu vermeiden, von jedem Antrag eine Kopie zukommen zu lassen.

- Die Einbeziehung der/des behördlichen Datenschutzbeauftragten ist zudem erforderlich, wenn in den zur Einsicht beantragten Unterlagen personenbezogene Daten Dritter vorhanden sind. Schon aus diesem Grund erscheint es zweckmäßig, der/dem behördlichen Datenschutzbeauftragten zugleich die Funktion der/des behördlichen Beauftragten für Akteneinsicht zu übertragen.

- Anträge auf Informationszugang sind besonders zeitkritisch, da Informationen schnell veralten und die Offenlegung veralteter Informationen faktisch der Ablehnung eines Antrags entspricht. In die Anweisung sollte deshalb eine maximale Bearbeitungsfrist von vier Wochen ab Eingang des Antrags festgeschrieben werden.

4. Anwendung und Auslegung des AIG

- Einer Dienstanweisung vorangestellte Erläuterungen zur Bedeutung des Informationszugangsrechts sowie zu den Zielen des AIG können hilfreich sein.

- Es sollte darauf hingewiesen werden, dass für einen Einsichtsanspruch möglicherweise auch andere *Anspruchsgrundlagen* als das AIG zum Tragen kommen können, so zum Beispiel § 18 Brandenburgisches Datenschutzgesetz (BbgDSG), wenn es um Daten zur eigenen Person geht, § 29 BbgVwVfG bei Verfahrensbeteiligten oder das Umweltinformationsgesetz (UIG), wenn Informationen über die Umwelt betroffen sind. Bei der Prüfung, ob ein Anspruch auf Akteneinsicht besteht, sind neben dem AIG auch diese Rechtsgrundlagen zu berücksichtigen. Dies gilt auch, wenn der Antrag explizit auf das AIG gestützt wird. Von den Antrag stellenden Personen kann nicht verlangt werden, die Anspruchsgrundlage im Antrag korrekt zu benennen.

- Herauszustellen sind die *Durchführungsbestimmungen* des § 6 AIG (hier besonders die Unterstützung durch die Behörde bei der Bestimmung des Antrags, die Pflicht zur Weiterleitung an die zuständige Stelle, die Notwendigkeit der schriftlichen Begründung einer Ablehnung und die Einholung der Zustimmung betroffener Dritter).

- In Fällen, in denen Personen, deren Daten in den Akten vorhanden sind, gemäß § 5 Abs. 2 Nr. 1 i.V.m. § 6 Abs. 1 Satz 5 nach ihrer *Zustimmung zur Offenlegung* dieser Daten zu fragen sind, hat die Behörde dies "auf Verlangen des Antragstellers" zu tun. Von dieser Möglichkeit sollte die Antrag stellende Person jedoch informiert werden.

- Im Rahmen der Anfrage an die Betroffenen, ob sie mit der Offenlegung ihrer Daten einverstanden sind, dürfen *Daten mit Bezug zur Antrag stellenden Person* nicht ohne deren Zustimmung weitergegeben werden, d.h. den Betroffenen darf von vornherein nicht mitgeteilt werden, wer Einsicht in die Akte beantragt hat. Wenn allerdings die Betroffenen ihr Einverständnis an die Kenntnis des Namens der Antrag stellenden Person knüpfen, so ist diese darüber zu informieren. Lehnt sie die Bekanntgabe ihres Namens ab, so gilt die Zustimmung des Betroffenen als verweigert. Der Antrag ist dann von der Akten führenden Behörde abzulehnen.

- Hinsichtlich der Gründe aus den §§ 4 und 5 AIG, die einer Offenlegung entgegenstehen können, ist auf § 6 Abs. 2 AIG zu verweisen. So sind Akten nicht alleine deshalb insgesamt nicht einsichtsfähig, weil sie schutzwürdige Informationen beinhalten. Vielmehr muss die Behörde diese Informationen aussondern (z.B. durch *Schwärzung*) und die restlichen, nicht schutzbedürftigen Informationen offen legen. Dies gilt auch, wenn betroffene Personen ihre Zustimmung zur Offenlegung der zu ihnen in den Akten vorhandenen Daten verweigern.

- Das Recht auf Akteneinsicht gilt ohne Voraussetzung, d.h. auf das Interesse der Antrag stellenden Person kommt es nicht an; es darf von der Behörde nicht erfragt werden. Eine Ausnahme hiervon bilden § 4 Abs. 2 sowie § 5 Abs. 2 AIG. In diesen Fällen hat die Behörde vor der Entscheidung über die Akteneinsicht der Antrag stellenden Person die Gelegenheit zu geben, ihr *Offenbarungsinteresses* darzulegen. Eine Verpflichtung der Antrag stellenden Person, dies schon bei der Antragstellung zu tun, besteht jedoch nicht.

## 5. Kosten und Gebühren

- Bei der Erhebung von Kosten ist zwischen den Gebühren und den Auslagen zu entscheiden. Letztere können kostendeckend erhoben werden (z.B. für Fotokopien), während die Gebühr für die Akteneinsicht so zu bemessen ist, dass sie nicht von vornherein vom Stellen eines Antrags auf Akteneinsicht abschreckt (zur Angemessenheit der Gebührenhöhe siehe § 10 Abs. 1 AIG). Eine ausschließliche Orientierung der Gebühren an der Arbeitszeit, die für die Antragsbearbeitung aufgewandt wird, ist daher zu

vermeiden.

- Die Gebührenerhebung erfolgt nach zwei unterschiedlichen Rechtsgrundlagen: Geht es um die Einsicht in Unterlagen, die im Zusammenhang mit der kommunalen Selbstverwaltung stehen, gilt das Kommunalabgabengesetz bzw. eine darauf gestützte kommunale Gebührensatzung. Bei allen anderen, von den Kommunen wahrgenommenen Aufgaben (Auftragsangelegenheiten, Pflichtaufgaben zur Erfüllung nach Weisung) wird bei der Gebührenberechnung die *Landesgebührenordnung* zum AIG (ein von der Landesregierung beschlossener Entwurf wird in Kürze dem Innenausschuss des Landtages vorgelegt) zu Grunde gelegt.

- Für die Ablehnung eines Antrags auf Akteneinsicht sollte keine Gebühr erhoben werden. Geht der Antrag auf andere Rechtsgrundlagen zurück (z.B. Umweltinformationsgesetz), so ist unter Umständen sogar ein Verbot der Gebührenerhebung in diesen Fällen zu beachten.

## 6. Sonstiges

- Es ist möglich, für die Antragstellung nach AIG ein *Antragsformular* bereitzuhalten. Dabei ist zu beachten, dass Daten mit Bezug zur Antrag stellenden Person sparsam erfragt werden. Insbesondere ist zu beachten, dass das Einsichtsinteresse lediglich in den Fällen des § 4 Abs. 2 sowie § 5 Abs. 2 AIG anzugeben ist.

- Um einen Überblick über die Zahl der gestellten Anträge sowie die Fachbereiche, auf die sich diese beziehen, zu erhalten, kann es sinnvoll sein, eine entsprechende *Statistik* zu führen. Dies ist möglicherweise auch für die kommunalen Vertretungen von Interesse. Dabei ist aber zu beachten, dass eine solche Übersicht keine personenbezogenen Daten enthalten sollte. Sie könnte folgende Angaben beinhalten: Gegenstand des Antrags (z.B. "Einsicht in Bauakten"), Bearbeitungsdauer, Entscheidung (Einsicht gewährt / teilweise gewährt / nicht gewährt), festgesetzte Gebühren sowie etwaige Widerspruchs- oder Gerichtsverfahren.

- Der Informationszugang nach AIG ist gemäß § 7 AIG nicht ausschließlich durch die Einsicht in Originaldokumente zu gewähren. Vielmehr können - mit Zustimmung des Antragstellers - auch *Fotokopien* der Unterlagen gefertigt werden. Der Antragsteller stimmt in einem solchen Fall zu, dass die Einsicht durch die Übermittlung der Vervielfältigungen an Stelle der Einsicht in die Originaldokumente stattfindet. Die Verwaltung kann ein solches Vorgehen beispielsweise vorschlagen, wenn keine Räumlichkeiten

für die Einsicht zur Verfügung stehen oder wenn sich die Fertigung von Kopien aus anderen organisatorischen Gründen anbietet. Das Recht auf Einsicht in die Originaldokumente wird durch das Aushändigen von Fotokopien aber nicht eingeschränkt.

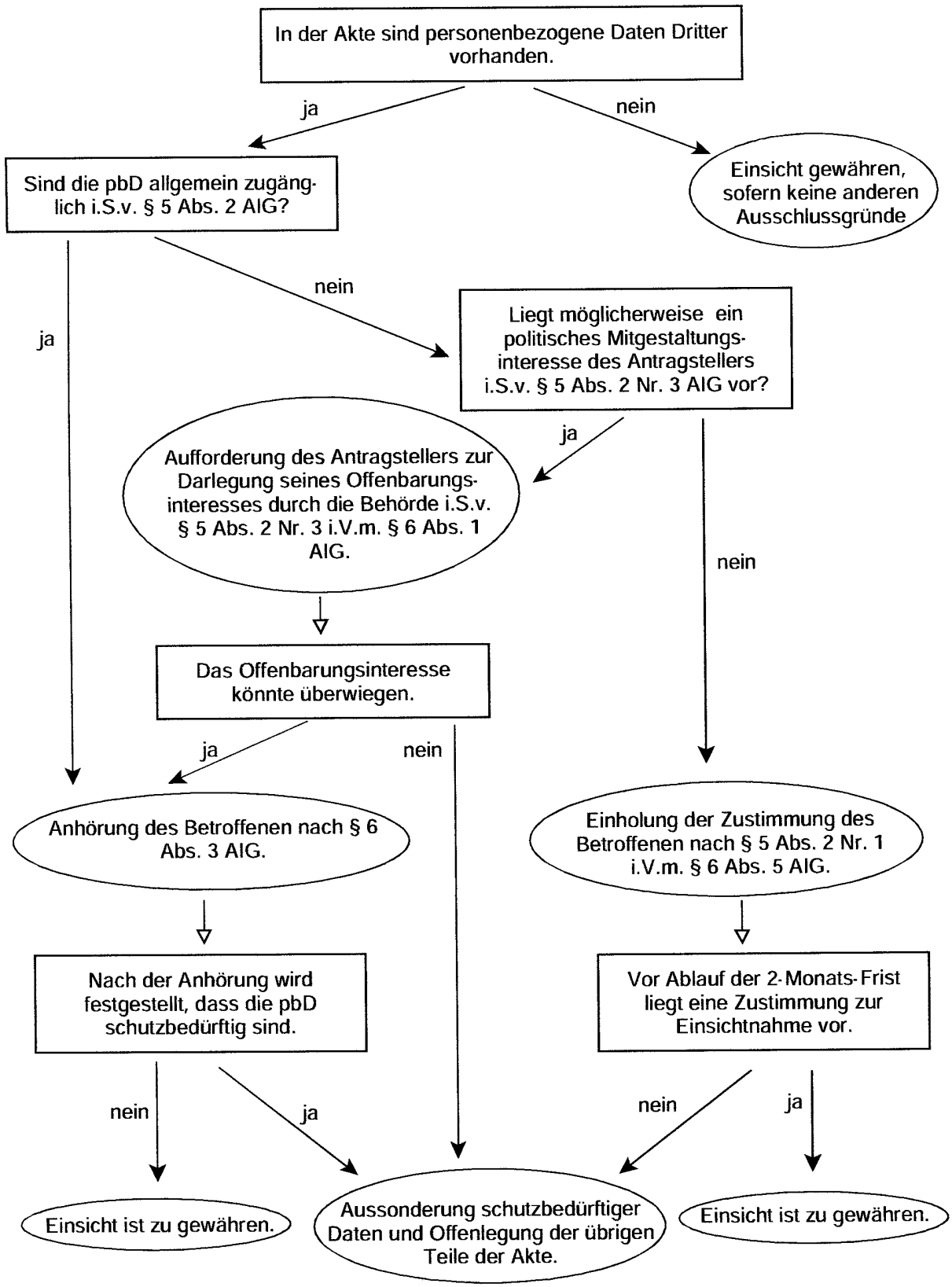
- Grundsätzlich besteht - auch, wenn die Originale eingesehen werden - eine *Pflicht der Verwaltung*, Kopien auf Verlangen der Antrag stellenden Person zur Verfügung zu stellen.

- Werden Fotokopien ausgehändigt, so kann die Behörde dies in der Verfahrens- oder Sachakte (gemeint ist hier das Verfahren nach AIG, nicht die auf den Sachverhalt in den einzusehenden Unterlagen bezogene Akte) dokumentieren, um im Bedarfsfall nachweisen zu können, welche Unterlagen mit welchem Bearbeitungsstand etc. als Kopie herausgegeben wurden. Ebenfalls zu *Dokumentationszwecken* in der Verfahrensakte kann die Behörde von der Antrag stellenden Person verlangen, per Unterschrift zu bestätigen, dass bzw. wann und in welche Unterlagen eine Einsicht stattgefunden hat.

- In Bescheiden, mit denen Anträge auf Akteneinsicht abgelehnt werden, sollte darauf hingewiesen werden, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht sowohl für Fragen als auch für Beschwerden zur Verfügung steht.

# Anlage 4

**Umgang mit personenbezogenen Daten (pbD) bei der Akteneinsicht auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes**



**Anlage 5**

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

Stand: 4. Januar 2001

| | |
|---|---|
| Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht | Dr. Alexander Dix |
| Stellvertreter | Kurt Urban |
| Mitarbeit bei:<br>- Akteneinsicht und Informationszugang<br>- Verwaltungsmodernisierung<br>- Redaktion von Veröffentlichungen | App. 20 |
| Sekretariat | App. 10 |

### Bereich Recht

| | |
|---|---|
| Bereichsleiter | Dr. Frank Jendro<br>App. 34 |
| Arbeitsgebiete:<br>- Rechtliche Grundsatzfragen<br>- Landtag, Staatskanzlei<br>- Landesrechnungshof<br>- Wissenschaft, Forschung und Kultur<br>- Beauftragter des Haushalts | |
| Arbeitsgebiete:<br>- Inneres (insbes. Polizei, Verfassungsschutz, Verkehrsordnungswidrigkeiten, Ausländer, Asylverfahren)<br>- Staatsanwaltschaften<br>- Presse- und Öffentlichkeitsarbeit | Lena Schraut<br>App. 41 |
| Arbeitsgebiete:<br>- Arbeit, Soziales, Gesundheit, Frauen<br>- Sozial- und Gesundheitsdaten allgemein | App. 44 |

Arbeitsgebiete: App. 40
- Bildung, Jugend, Sport
- Finanzen
- Kommunalrecht (außer Abwasserzweckverbände)
- Telekommunikation und Medien

Arbeitsgebiete: App. 22
- Justiz (außer Staatsanwaltschaften)
- Stadtentwicklung, Wohnen, Verkehr
- Wirtschaft

Arbeitsgebiete: App. 45
- Landwirtschaft, Umweltschutz, Raumordnung (einschließlich Abwasserzweckverbände)
- Personaldaten allgemein
- Inneres (Außer Sicherheitsbehörden und Kommunalrecht)

Arbeitsgebiete: App. 42
- Personal- und Verwaltungsangelegenheiten des LDA
- Büroleitungsaufgaben
- Haushaltsangelegenheiten- Beschaffungen allgemein

Arbeitsgebiete: App. 43
- Bibliothek
- Literaturbeschaffung
- Schreibdienst
- Informationsmaterialien

## Bereich Technik

Bereichsleiter Kurt Urban
App. 30

Arbeitsgebiete:
- Technisch/organisatorische Grundsatzfragen
- Landesverwaltungsnetz
- komplexe IT-Verfahren

Arbeitsgebiete: App. 31
- Großrechner
- Datenbanksysteme
- kryptographische Verfahren
- Organisations-/ Dienstanweisungen
- Statistik
- Beratung der behördlichen Datenschutz-beauftragten und Personalräte

Arbeitsgebiete: App. 32
- UNIX-Systeme
- Sicherheitsprodukte
- Kartentechnologien
- Kommunikationsnetze
- Telekommunikation und Medien

Arbeitsgebiete: App. 33
- Systemverwalter
- Gebäudesicherung
- Datenträgerentsorgung
- Isolierte und vernetzte PC

Arbeitsgebiete: App. 12
- Teilaufgaben der autom. Vorgangsverwaltung
- Mailboxkommunikation mit BfD, LfDen
- Schreibdienst
- Informationsmaterialien

**Gleichstellungsbeauftragte** App. 43

**Personalrat** App. 31

**Behördlicher Datenschutzbeauftragter** App. 40

**Anlage 6**

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

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

## Abkürzungsverzeichnis

| | |
|---|---|
| ABl. | =Amtsblatt |
| Abs. | =Absatz |
| AIG | =Akteneinsichts- und Informationszugangsgesetz |
| AmtsO | =Amtsordnung |
| Anl. | =Anlage |
| AO | =Abgabenordnung |
| Art. | =Artikel |
| Bbg. | =Brandenburgisch(es) |
| BbgDSG | =Brandenburgisches Datenschutzgesetz |
| BbgHSG | =Brandenburgisches Hochschulgesetz |
| BbgMeldeG | =Brandenburgisches Meldegesetz |
| BbgSchulG | =Brandenburgisches Schulgesetz |
| BbgStatG | =Brandenburgisches Statistikgesetz |
| BbgSÜG | =Brandenburgisches Sicherheitsüberprüfungsgesetz |
| BDSG | =Bundesdatenschutzgesetz |
| BDSG-E | =Entwurf für eine neues Bundesdatenschutzgesetz vom Oktober 1999 |
| BGB | =Bürgerliches Gesetzbuch |
| BGS | =Bundesgrenzschutz |
| BIS | =Brandenburgische InformationsStrategie |
| BKA | =Bundeskriminalamt |
| BR-Drs. | =Bundesrats-Drucksache |
| BSHG | =Bundessozialhilfegesetz |
| BSI | =Bundesamt für die Sicherheit in der Informationstechnik |
| BStBl. | =Bundessteuerblatt |
| Buchst. | =Buchstabe |
| BVerfG | =Bundesverfassungsgericht |
| BVerfGE | =Bundesverfassungsgerichtsentscheidung |
| BVerwG | =Bundsverwaltungsgericht |
| bzw. | =beziehungsweise |
| c‘t | =ct magazin für computertechnik |
| ca. | =circa |
| d. h. | =das heißt |
| DBMS | =Datenbank-Management-System |
| DES | =Data Encryption Standard (112 Bit oder 168 Bit Schlüssellänge) |
| 3DES | =Data Encryption Standard (56 Bit Schlüssellänge) |
| DM | =Data Mining |
| DSG | =Datenschutzgesetz |
| DSV | =Datenschutzverordnung Schulwesen |
| DV | =Datenverarbeitung |

| | |
|---|---|
| DWH | =Data Warehouse |
| e. V. | =eingetragener Verein |
| ebda. | =ebenda |
| ECC | =ELSTER-Control-Center |
| EG | =Europäische Gemeinschaft |
| ELSTER | =Elektronische Steuererklärung |
| EStG | =Einkommenssteuergesetz |
| EU | =Europäische Union |
| evtl. | =eventuell |
| ff. | =folgende |
| GByte | =GigaByte |
| geänd. | =geändert |
| gem. | =gemäß |
| GereB/Wikri | =Gesellschaftsrechtliche Beziehungen/Wirtschafts-kriminalität |
| GG | =Grundgesetz |
| ggf. | =gegebenenfalls |
| GmbH | =Gesellschaft mit beschränkter Haftung |
| GO | =Gemeindeordnung |
| GVBl. | =Gesetz- und Verordnungsblatt |
| GWS | =Gewalttäter Sport |
| HTTP | =HyperText Transport Protocol |
| HundehHV | =Hundehalterverordnung |
| i. d. Fass. | =in der Fassung |
| i. d. R. | =In der Regel |
| I. P. | =Identity Protector |
| i. S. v. | =im Sinne von |
| i. V. m. | =in Verbindung mit |
| IDEA | =International Data Encryption Algorithm |
| INPOL | =Informationssystem der Polizei |
| insbes. | =insbesondere |
| InVeKoS | =Integriertes Verwaltungs- und Kontrollsystem |
| IP | =Internet-Protokoll |
| ISDN | =Integrated Services Digital Network |
| ISO | =International Organization for Standardization |
| Kap. | =Kapitel |
| Kfz | =Kraftfahrzeug |
| KitaG | =Kindertagesstättengesetz |
| LBG | =Landesbeamtengesetz |
| LBVS | =Landesamt für Bauen, Wohnen und Straßenverkehr |
| LDA | =Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht |
| LDS | =Landesbetrieb für Datenverarbeitung und Statistik |

| | |
|---|---|
| LDSG | =Landesdatenschutzgesetz |
| LT-Drs. | =Landtags-Drucksache |
| LVN | =Landesverwaltungsnetz |
| m.a.u.s | =Medien an unsere Schulen |
| MDStV | =Mediendienste-Staatsvertrag |
| MeldDÜV | =Meldedatenübermittlungsverordnung |
| MEGA | =Mobile Einsatzgruppe gegen Ausländerfeindlichkeit |
| MiStra | =Anordnung über Mitteilungen in Strafsachen |
| MRRG | =Melderechtsrahmengesetz |
| Nr. | =Nummer |
| o. g. | =oben genannte |
| o. Ä. | =oder Ähnliches |
| OFD | =Oberfinanzdirektion Cottbus |
| OSS | =Open-Source Software |
| PC | =Personalcomputer |
| PET | =Privacy Enhancing Technologies; datenschutzfreundliche Technologien |
| Pkt. | =Punkt |
| Pkw | =Personenkraftwagen |
| PLIB | =Pädagogisches Landesinstitut Brandenburg |
| POGBbg | =Polizeiorganisationsgesetz |
| RSA | =Verschlüsselungsalgorithmus nach den Rivest, Shamir und Adleman |
| s. | =siehe |
| S. | =Seite; Satz |
| s. o. | =siehe oben |
| SDÜ | =Schengener Durchführungsabkommen |
| SGB | =Sozialgesetzbuch |
| SGB I | =Erstes Buch Sozialgesetzbuch |
| SGB VIII | =Achtes Buch Sozialgesetzbuch |
| SGB X | =Zehntes Buch Sozialgesetzbuch |
| SIS | =Schengener Informationssystem |
| SOAP | =Simple Object Access Protocol |
| sog. | =so genannt |
| StPO | =Strafprozessordnung |
| TDDSG | =Teledienstedatenschutzgesetz |
| TDG | =Teledienstegesetz |
| TDSV | =Telekommunikations-Datenschutzverordnung |
| TK | =Telekommunikation |
| TKG | =Telekommunikationsgesetz |
| TÜ-Maßnahmen | =Telefonüberwachungsmaßnahmen |
| TÜ-Unterlagen | =Telefonüberwachungsunterlagen |
| u. a. | =unter anderem |

| | |
|---|---|
| u. Ä. | =und Ähnliches |
| u. U. | =unter Umständen |
| UIG | =Umweltinformationsgesetz |
| UMTS | =Universal Mobile Telecommunications System |
| Urt. | =Urteil |
| US | =United States |
| USA | =United States of America |
| usw. | =und so weiter |
| v. | =von, vom |
| VDE | =Verband Deutscher Elektroingenieure |
| VDV | =Verband Deutscher Verkehrsunternehmen |
| VfGBbg | =Verfassungsgericht des Landes Brandenburg |
| vgl. | =vergleiche |
| VO | =Verordnung |
| VOwiZustV | =Verkehrsordnungswidrigkeitenzuständigkeitsverordnung |
| WWW | =World Wide Web |
| XML | =Extensible Markup Language |
| z. B. | =zum Beispiel |
| z. T. | =zum Teil |
| z. Z. | =zur Zeit |
| ZIS | =Zentralstelle Information Sport |

## Stichwortverzeichnis