Landtag Brandenburg **Drucksache 2/697**
2. Wahlperiode

Dritter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. April 1994 bis 31. März 1995

Inhaltsverzeichnis Seite

Datum des Eingangs: 29.05.1995 / Ausgegeben: 29.05.1995

1 Datenschutzrechtliche Entwicklung in Brandenburg

1.1 Einleitung

Im Berichtszeitraum hat meine Behörde die Datenverarbeitung bei zahlreichen Behörden (wie z. B. Polizei, Verfassungsschutz, Statistikstellen, Justizvollzugsanstalten, Jugendämter und Wohnungsstellen) kontrolliert. Entscheidend für die Auswahl der kontrollierten öffentlichen Stellen waren zum einen die Fortsetzung von Prüfungen aus dem Vorjahr, zum anderen bevorstehende landesweite Erhebungen und nicht zuletzt schwerwiegende Hinweise durch Eingaben von Bürgern.

Im Ergebnis waren Beanstandungen auszusprechen, die überwiegend technisch-organisatorische Probleme der Datenverarbeitung und Datensicherung betrafen. Dies überrascht nicht, wenn man allein die Unterbringung der öffentlichen Stellen in Betracht zieht. Die beanstandeten Behörden begründeten die Unzulänglichkeiten mit fehlenden Haushaltsmitteln. Dies kann ich jedoch nicht hinnehmen. Kostengründe können - vor allem auf Dauer - nicht dem verfassungsmäßig geschützten Recht auf informationelle Selbstbestimmung entgegengehalten werden.

Wie in den vorhergehenden Tätigkeitsberichten habe ich die ausführliche Darlegung eines juristischen sowie technischen Schwerpunktthemas an den Anfang gestellt. Entsprechend den bei den Prüfungen der kontrollierten Behörden vorgefundenen Mängeln lag es nahe, hierfür die Umsetzung von technisch-organisatorischen Maßnahmen gem. § 10 Brandenburgisches Datenschutzgesetz in den öffentlichen Stellen auszuwählen und darüber hinaus sind Mindestanforderungen an Dienstanweisungen zusammengestellt. Im weiteren folgt der Aufbau des Tätigkeitsbericht nach dem Ressortprinzip. Im Anhang finden sich u. a. die im Wortlaut abgedruckten Entschließungen der 48. und 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie ein Stichwort- und Abkürzungsverzeichnis.

Grundsätzliche Entscheidungen - auf die hier nur kurz hingewiesen werden soll - standen auf der Bundes- und auch auf der Europaebene im Berichtszeitraum an. Beim Gesetz zur Änderung des Grundgesetzes[1] wurde u. a. darüber beraten, das Recht auf informationelle Selbstbestimmung in den Grundrechtskatalog aufzunehmen. Diese vor allem von den Datenschutzbeauftragten und von Bürgerrechtsorganisationen vorgetragene Forderung wurde von der Gemeinsamen Verfassungskommission abgelehnt. Zur Begründung hieß es, der Datenschutz sei nur ein Ausschnitt aus dem Persönlichkeitsrecht und solle deshalb nicht durch einen eigenständigen Grundgesetzartikel verselbständigt werden. Angesichts der nicht absehbaren Folgen und der damit verbundenen Gefahren, die eine künftige "Informationsgesellschaft" in bezug auf massenhafte Datenverarbeitung und systemische Verknüpfungen für den Einzelnen bringt, bedaure ich dies sehr.

Die Bemühungen um einheitliche europäische Mindeststandards im Datenschutzrecht haben demgegenüber eine entscheidende Hürde genommen; der Rat der Europäischen Union hat am 22. Dezember 1994 den Entwurf der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verabschiedet. Nunmehr muß nur noch das Europäische Parlament selbst diesem zustimmen, damit vor allem die Datenverarbeitung im privaten Bereich vergleichbaren Datenschutzregelungen wie im öffentlichen Bereich unterworfen ist.

Meinen Kollegen vom Bund und den Kollegen in den anderen Bundesländern habe ich wiederum zu danken für die gewährte Unterstützung sowie gelungene zweckdienliche

---

[1] vom 27. Oktober 1994, BGBl. I S. 3146

Kooperation. Hervorzuheben ist an dieser Stelle die Zusammenarbeit mit der für den privaten Bereich zuständigen Aufsichtsbehörde für den Datenschutz beim Ministerium des Innern. Der kontinuierliche Informationsaustausch über gemeinsam berührende datenschutzrechtliche Fragestellungen förderte die Durchsetzung datenschutzrechtlicher Belange im Land Brandenburg. Hier möchte ich auch meinen Mitarbeitern für ihr beharrliches Engagement, mit denen sie sich für die Belange des Datenschutzes und damit für die Persönlichkeitsrechte der Bürgerinnen und Bürger des Landes Brandenburg erfolgreich eingesetzt haben, danken.

Für den Jahresbericht wurde als Stichtag der 31. März 1995 gewählt.

1.2 Ein allgemeines Akteneinsichtsrecht für alle Brandenburger

Die Brandenburgische Verfassung[2] garantiert den Bürgern gem. Art. 21 Abs. 4 ein allgemeines Akteneinsichtsrecht. Näheres soll ein Gesetz regeln, das es jedoch noch nicht gibt. Ein erster Ansatz ist allerdings in dem 1994 vom Bundestag verabschiedeten Umweltinformationsgesetz (UIG)[3] erkennbar, das jedoch nur den Zugang des Bürgers zu Umweltakten regelt. Das Aktenzugangsrecht der Brandenburgischen Verfassung soll nach dem Willen der Verfassungsgeber jedoch für alle Verwaltungsbereiche gelten. Ein solches Aktenzugangsrecht wäre ein Novum im deutschen Recht, bei dem das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht des ungehinderten Informationszugangs miteinander in Übereinstimmung gebracht werden müssen.

1.2.1 Das Recht auf informationelle Selbstbestimmung und das Informationszugangsrecht - zwei scheinbar konkurrierende Grundrechte

Das Recht auf informationelle Selbstbestimmung ist eine Ausformung des in Art. 2 Grundgesetz (GG) garantierten allgemeinen Persönlichkeitsrechts. Der einzelne ist grundsätzlich Herr der Informationen über seine Lebenssachverhalte. Er entscheidet über deren Preisgabe und Verwendung. Er bestimmt, wer sich von ihm welches Bild machen darf. Diese Verfügungsgewalt ist allerdings nicht absolut, vielmehr findet sie ihre Grenzen im überwiegenden Allgemeininteresse.

Der Schutz personenbezogener Daten definiert sich verfassungsrechtlich als Regel-Ausnahme-Verhältnis. Erhebung und Verarbeitung personenbezogener Daten sind nur zulässig, wenn entweder der Betroffene eingewilligt hat oder wenn eine Rechtsvorschrift sie eigens erlaubt. Keine öffentliche Stelle darf ohne Rechtsgrundlage den einzelnen beobachten, über ihn Erkundigungen einziehen und die Ergebnisse festhalten oder sonst verwenden.

Daraus folgt, daß jeder, der von einer Verwaltung Informationen über einen Dritten begehrt, an dessen Recht auf informationelle Selbstbestimmung scheitert, wenn dieser der Informationsübermittlung nicht vorher zugestimmt hat oder wenn ein Gesetz sie nicht gestattet.

Nun stellt das Grundgesetz den einzelnen nicht nur als schützenswertes Informationsobjekt dar, sondern auch als ein mit Rechten ausgestattetes Informationssubjekt. Art. 2 GG garantiert ihm das Recht auf die freie Entfaltung seiner Persönlichkeit, und Art. 5 GG stattet ihn mit dem Recht aus, seine Meinung in Wort, Schrift und Bild frei zu äußern, zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.

Zu der aus Art. 2 GG abzuleitenden allgemeinen Handlungsfreiheit gehört es, den Bereich, in dem man sich als Persönlichkeit entfalten will, selbst zu bestimmen, zu ermitteln und zu

---

[2] vom 20. August 1992, GVBl. I S. 298
[3] vom 8. Juli 1994, BGBl. I S. 1490

untersuchen, was der Entfaltung dienlich ist. Daraus folgt, daß jeder grundsätzlich das Recht hat, sich von jedem anderen ein eigenes Bild zu machen. Dieses Bild muß er auch nicht streng vertraulich bewahren, sondern er kann es an andere weitergeben. Datenschutzrechtlich ist das eine Übermittlung personenbezogener Daten an einen Dritten.

Die vorigen Ausführungen beziehen sich allerdings nur auf Informationen, die man aus eigener Wahrnehmung, Ermittlung oder Erschließung erhalten hat. Art. 2 und Art. 5 GG begründen keinen unmittelbaren Rechtsanspruch auf nicht allgemein zugängliche Informationen.

Grundsätzlich muß man feststellen, daß im Zuge der Entwicklung des Datenschutzrechts das Recht des einzelnen auf Informationsbeschaffung und Informationsverarbeitung ins Hintertreffen geraten ist. Mit dem berechtigten oder vorgeschobenen Hinweis auf den verfassungsrechtlich gebotenen Schutz personenbezogener Angaben Dritter wird demjenigen Bürger, der sich bei Behörden über öffentliche Belange informieren will, der Informationszugang verwehrt. Der mündige Bürger, der sich an der Gestaltung seiner Umwelt und der Gesellschaft beteiligen will, scheitert so häufig schon im Ansatz. Um die negativen gesellschaftlichen Auswirkungen dieses Prozesses aufzufangen und abzuwenden, bedarf es jetzt nach der Ausgestaltung des Datenschutzes einer fein abgestimmten Ausgestaltung des im Grundgesetz - und in der Brandenburgischen Verfassung - garantierten Informationszugangsrechts.

Dabei kann es nicht darum gehen, das Recht auf Nicht-Preisgabe von Informationen über eigene Lebenssachverhalte zugunsten des Informationszugangsrechts auszuhebeln, sondern es sind diejenigen Bereiche des öffentlichen Lebens zu bestimmen und festzulegen, in denen es das überwiegende Allgemeininteresse gebietet, das Recht auf informationelle Selbstbestimmung des einzelnen einzuschränken, um ein funktionierendes Informationszugangsrecht zu schaffen. Wegen des im Recht auf informationelle Selbstbestimmung begründeten Regel-Ausnahme-Verhältnisses müssen auch diejenigen personenbezogenen Angaben festgelegt werden, die im überwiegenden Allgemeininteresse zu offenbaren sind.

1.2.2 Unterschiedliche Auskunfts- bzw. Akteneinsichtsrechte

Das allgemeine Akteneinsichtsrecht könnte man als ein nicht-qualifiziertes Akteneinsichtsrecht bezeichnen. Der Unterschied zu qualifizierten Auskunfts- und Akteneinsichtsrechten besteht darin, daß dort der Auskunftsbegehrende eine bestimmte Rolle als Beteiligter oder Betroffener einnehmen muß. Anhand dieser "Qualifikation" entscheidet sich, auf welcher Rechtsgrundlage und mit welchen Beschränkungen die Auskunft erteilt wird.

Betroffene erhalten auf der Grundlage der Datenschutzgesetze bzw. der Spezialgesetze Einsicht in oder Auskunft aus Akten, Dateien oder anderen Verwaltungsunterlagen, soweit diese Informationen ihre eigene Person betreffen. Seine Grenzen hat dieses Recht u. a. da,

- wo es berechtigte Interessen Dritter berührt,

- wo die Aufgabenerfüllung der Behörde oder die öffentliche Sicherheit und Ordnung durch die Auskunft oder die Einsicht gefährdet wird.

Beteiligte an einem Verwaltungsverfahren haben auf der Grundlage des § 29 Verwaltungsverfahrensgesetz (VwVfGBbg)[4] sowie anderer Gesetze ein Einsichtsrecht in alle Verfahrensakten, soweit die Kenntnis der Information erforderlich ist, damit der Beteiligte

[4] vom 26. Februar 1993, GVBl. I S. 26

seine rechtlichen Interessen wahren kann. Die Verwaltung kann die Einsichtnahme verweigern,

- wenn ihre Aufgabenerfüllung dadurch beeinträchtigt würde und

- soweit sie sich auf verwaltungsinterne Unterlagen, wie Entwürfe zu Verwaltungsentscheidungen sowie Vorbereitungsarbeiten, bezieht.

Nicht-qualifizierte Auskunfts- bzw. Akteneinsichtsrechte sind Jedermann-Rechte. Entscheidend ist nicht die "Qualifikation" des Auskunftsbegehrenden für den Informationszugang und seine Beschränkungen, sondern die Art der Unterlagen. Der Auskunftsbegehrende braucht als Herr/Frau Jedermann sein Einsichts- bzw. Auskunftsinteresse nicht zu begründen, sein Interesse oder besser vielleicht seine "Neugier" allein genügt.

Der Idee eines nicht-qualifizierten Akteneinsichtsrechts am nächsten kommen die im Brandenburgischen Archivgesetz (BbgArchivG)[5] festgelegten Nutzungsrechte von Archivunterlagen. Grundsätzlich hat jedermann das Recht, die Aktenbestände eines Archivs einzusehen, soweit es sich um Vorgänge handelt, die nicht mehr im aktuellen Verwaltungsvollzug sind oder deren Schutzfrist abgelaufen ist bzw. bei denen keine Schutzfrist bestand.

Sonderfälle des Akteneinsichtsrechts stellen schließlich die im Stasi-Unterlagengesetz (StUG)[6] geregelte Nutzung der Stasi-Unterlagen sowie die in § 34 ff. Brandenburgisches Datenschutzgesetz (Bbg DSG)[7] bzw. dem Brandenburgischen Archivgesetz geregelten Einsichtsrechte in sonstige Verwaltungsakten der ehemaligen DDR dar, soweit letztere nicht von den nach 1990 entstandenen Verwaltungen benötigt werden.

Datenschutzrechtliche Gründe stehen somit der Umsetzung eines allgemeinen Aktenzugangsrechts für die brandenburgischen Bürger grundsätzlich nicht im Wege.

1.3 Technisch-organisatorische Maßnahmen bei der Einhaltung des Datenschutzes

1.3.1 Technisch-organisatorische Maßnahmen gem. § 10 Bbg DSG

Werden personenbezogene Daten automatisiert verarbeitet, sind gemäß § 10 Bbg DSG technisch-organisatorische Maßnahmen zu treffen, die je nach Art der Daten zu ihrem Schutze geeignet sind. Von mir durchgeführte Kontrollen in Kommunen und anderen öffentlichen Stellen ergaben, daß dabei noch erhebliche Defizite bei ihrer Durchsetzung bestehen. Sie sind teilweise auf Unkenntnis der Verantwortlichen, aber auch auf fehlende finanzielle Mittel zurückzuführen. Maßnahmen des Datenschutzes und der Datensicherheit werden bei der Einführung neuer Verfahren oft nur ungenügend berücksichtigt. Die datenschutzrechtlichen Anforderungen sollten schon bei der Erstellung eines Projektes einbezogen werden. Eine nachträgliche Integration von Sicherheitskomponenten erweist sich häufig als schwierig und außerdem als zu kostenintensiv.

Technisch-organisatorische Maßnahmen sind nach § 10 Abs. 1 nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die

---

[5] vom 7. April 1994, GVBl. I S. 94
[6] vom 20. Dezember 1991, BGBl. I S. 2272
[7] vom 20. Januar 1992, GVBl. I S. 2

Beurteilung, ob eine Maßnahme angemessen ist, ist nicht frei von einer subjektiven Einschätzung. Anhaltspunkte hierfür geben sog. Schutzstufenkonzepte. Näheres habe ich dazu in einer Informationsbroschüre[8] ausgeführt.

Im folgenden möchte ich auf die sog. "10 Gebote" über technisch-organisatorische Maßnahmen gemäß § 10 Bbg DSG näher eingehen und dazu detailliert praktische Hinweise geben.

1.3.1.1 Zugangskontrolle

In § 10 Abs. 2 Nr. 1 Bbg DSG wird gefordert, daß Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren ist. Folgende Maßnahmen sind dabei denkbar:

- Festlegung von Sicherungsbereichen,
- Festlegung von befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung),
- Festlegung von Besucherregelungen,
- Sicherung von Gebäuden und Räumen (s. unter 1.3.1.11),
- Anwesenheitsaufzeichnungen,
- Sperrung der Geräte und Netzwerke durch zusätzliche Hardwarebaugruppen (z. B. Schutz lokaler Netze durch Firewalls, Sternkoppler mit Sicherheitsmodulen zur Filterung der MAC-Adressen),
- Unterbringung von Netzknoten in verschlossenen Räumen oder Schränken,
- Einrichtung geschlossener Benutzergruppen.

[8] Broschüre: "Sicherheit am PC und in lokalen Netzen - Dateienregister", 1. Aufl. September 1993 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert"

1.3.1.2 Datenträgerkontrolle

In § 10 Abs. 2 Nr. 2 Bbg DSG wird gefordert, daß das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern verhindert werden soll. Folgende Punkte sind dabei zu berücksichtigen:

- Datenträgerverwaltung einschließlich Protokollierung der Befugten,
- Periodizität der Bestandskontrollen,
- datenschutzgerechte Datenträgervernichtung,
- Einschränkung von Softwaremöglichkeiten zum Kopieren von Dateien und Datenträgern,
- Festlegungen zum Kopieren von Dateien,
- Festlegungen zu Datensicherungsmaßnahmen,
- eventuell Datenverschlüsselung (s. unter 1.3.5),
- Festlegungen zur Aufbewahrung von Datenträgern,
- physisches Löschen nicht mehr benötigter Dateien (s. unter 1.3.1.12) ,
- Sperrung von Kopierbefehlen,
- hardwaremäßiges Deaktivieren der Diskettenlaufwerke (s. unter 1.3.1.13).

1.3.1.3 Speicherkontrolle

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist gem. § 10 Abs. 2 Nr. 3 Bbg DSG zu verhindern. Eine effektive Speicherkontrolle kann durch folgende Maßnahmen gewährleistet werden:

- Festlegung der Befugnisse für die Eingabe, Kenntnisnahme, Veränderung und Löschung der Daten,
- Festlegungen über die Zuordnung von Arbeitsplätzen (z. B. Systemverwalter, Arbeitsstationen),
- Festlegungen zur Programmfreigabe,
- Protokollierung der Dateienbenutzung,
- Richtlinien zur Dateiverwaltung,
- Festlegungen zur Wartung und Fernwartung,
- Festlegungen zur Arbeit des Systemverwalters.

1.3.1.4 Benutzerkontrolle

Gemäß § 10 Abs. 2 Nr. 4 Bbg DSG ist zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können. Die Benutzerkontrolle kann durch folgende Maßnahmen realisiert werden:

- Verschluß oder sogar Verplomben der Datenstationen,
- Verwendung von Benutzerkennungen und Paßwörtern (s. unter 1.3.1.15),
- Festlegungen zu Datenübertragungen bei Netzarbeit (Abschottung von anderen Netzen, Begrenzung der Netzverwaltung auf 1 oder 2 Nutzer, Festlegung, welche Daten sollen wie übertragen werden),
- revisionsfähige Dokumentation der Benutzerprofile,
- revisionsfähige Protokollierung (s. unter 1.3.4),
- Einsatz von Sicherheitssoftware,
- Einsatz von Verschlüsselungsverfahren (s. unter 1.3.5),
- Abweisung unberechtigter Benutzer.

1.3.1.5 Zugriffskontrolle

In § 10 Abs. 2 Nr. 5 Bbg DSG wird gefordert, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung

unterliegenden personenbezogenen Daten zugreifen können. Eine effektive Zugriffskontrolle wird u. a. durch folgende Maßnahmen erreicht:

- Eindeutige Identifizierung und Authentisierung bei Netzanschluß (Benutzerkennwort und Paßwort),
- Verwendung einer abgestuften Rechteverwaltung, Beschränkung auf die zur Aufgabenerfüllung erforderlichen Zugriffsmöglichkeiten (s. unter 1.3.1.14),
- Systemverwaltung u. U. nach dem Vier-Augen-Prinzip,
- Bildschirmverdunkelung bei Arbeitsunterbrechung (Weiterarbeit z. B. erst nach Wiedereingabe des Paßworts),
- regelmäßige Überprüfung der festgelegten Befugnisse bezüglich Zugriffsrechten,
- Wartung durch externe Firmen nur in Anwesenheit des Systemverwalters,
- eindeutige Identifizierung der Ein- und Ausgabegeräte im Netzverband,
- Sperren der Betriebssystemebene,
- Verwendung von Menüsystemen,
- Einsatz von Sicherheitssoftware.

1.3.1.6 Übermittlungskontrolle

Gemäß § 10 Abs. 2 Nr. 6 Bbg DSG ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit an wen durch Einrichtungen zur Datenübertragung übermittelt worden sind. Die Übermittlungskontrolle kann u. a. durch folgende Maßnahmen realisiert werden:

- Festlegung der zugelassenen Übermittlungsberechtigten (Sender), Übermittlungsempfänger und Übermittlungswege,
- Überprüfung der Authentizität des Empfängers,
- Dokumentation der Empfänger,
- Festlegung einer ausreichenden Benutzeridentifizierung (Zeiten, Personen, Verfahren, Geräte, Programme, welche Daten),
- Festlegungen zur Auswertung der Protokolle (Periodizität, Umfang),
- Fernwartung nur bei Sicherstellung, daß personenbezogene Daten nicht eingesehen werden können,
- Protokollierung der Datenübermittlung,
- Einsatz von Verschlüsselungsverfahren (s. unter 1.3.5),
- Einsatz von sicherheitsgeprüften Protokollen,
- Dokumentation der Abruf- und Übermittlungsprogramme,
- Netzwerkdokumentation,
- Dokumentation der Programmfreigabe von Übermittlungsprogrammen.

1.3.1.7 Eingabekontrolle

Gemäß § 10 Abs. 2 Nr. 7 Bbg DSG ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind. Die Eingabekontrolle kann durch folgende Maßnahmen realisiert werden:

- Einsatz von Sicherheitssoftware,
- Transaktionsprotokolle,
- Festlegung, wer Daten eingeben darf,
- Kennzeichnung von Erfassungsunterlagen mit Namen und Datum nach Vollzug der Eingabe,
- Protokollierung der Netzverwaltung, Zugriffsrechte auf Dateien und der gescheiterten Zugriffsversuche, der Programmaufrufe,
- Auswertung der Protokolle und Festlegung, zu welchen Zwecken sie verwendet und wie lange sie aufbewahrt werden dürfen,

- Festlegung zu Veränderungen von Zugriffsrechten,
- Festlegung zur Dateiverantwortlichkeit.

1.3.1.8 Auftragskontrolle

Nach § 10 Abs. 2 Nr. 8 Bbg DSG ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Die Auftragnehmer sind im Hinblick auf ihre Eignung mit größter Sorgfalt auszuwählen. Aufträge nach § 11 Abs. 1 Bbg DSG bedürfen der Schriftform (Vertrag). Sollen nichtöffentliche Stellen beauftragt werden, dann ist dazu bei öffentlichen Stellen gem. § 2 Abs. 1 Bbg DSG die Zustimmung der zuständigen obersten Landesbehörde bzw. bei Gemeinden und Gemeindeverbänden des Ministeriums des Innern erforderlich. Im Vertrag sollten u. a. folgende Punkte geregelt sein:

- die Festlegung der Kompetenzen und Pflichten von Auftragnehmer und Auftraggeber,
- Vereinbarungen über Kündigungsmöglichkeiten,
- Vertragsstrafen und Kontrollrechte für den Auftraggeber,
- bei Programmieraufträgen das Pflichtenheft, Testvorführungen und Programmfreigabe,
- Verfahrensweise bei nicht mehr benötigten personenbezogenen Daten beim Auftragnehmer (z. B. Vernichtung oder Rückgabe),
- nach Möglichkeit Ausschluß von Subunternehmern,
- Festlegung der Kontrollmöglichkeit durch den Landesbeauftragten für den Datenschutz.

1.3.1.9 Transportkontrolle

Nach § 10 Abs. 2 Nr. 9 Bbg DSG ist zu gewährleisten, daß personenbezogene Daten bei ihrer Übertragung sowie beim Transport von Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Dies kann bei

a) Übertragung über ein Netzwerk durch

- Festlegungen zum Abschirmen von Kabeln zwecks höherer Abhörsicherheit,
- Einsatz von Verschlüsselungsverfahren (s. unter 1.3.5),
- Festlegung der Übertragungswege,
- Schutz der Integrität der Daten (s. unter 1.3.5) und

b) Transport mit Hilfe von Datenträgern durch

- Festlegung der zum Transport berechtigten Personen,
- Festlegungen zu Begleitpapieren, zu Verpackungs- und Versandvorschriften,
- bei Rückgabe von magnetischen Datenträgern vorher physikalisches Löschen der nicht mehr benötigten personenbezogenen Daten,
- Direktabholung, Kurierdienst,
- Vollständigkeitsprüfung,
- Verwendung von Verschlüsselungsverfahren

erreicht werden.

1.3.1.10 Organisationskontrolle

Nach § 10 Abs. 2 Nr. 10 Bbg DSG ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Organisationskontrolle bedeutet primär die Schaffung organisatorischer Rahmenbedingungen, die sich in der Form von Dienstanweisungen widerspiegeln. Im Kapitel 1.3.2 gehe ich auf erforderliche Dienstanweisungen näher ein.

1.3.1.11 Sicherung von Gebäuden und Räumen

Es ist zu empfehlen, die erforderlichen Sicherheitsmaßnahmen durch eine Risikoanalyse zu ermitteln und in einem Sicherheitskonzept festzulegen. Besonders zu sichern sind die Räumlichkeiten, die der Unterbringung von ADV-Einrichtungen und Datenträgern dienen. An dieser Stelle können nur allgemeine Hinweise gegeben werden, die der konkreten Situation anzupassen sind.

Zunächst ist die unauffällige Unterbringung des zentralen Netzwerkrechners unter Verzicht auf Hinweisschilder, wie "Rechenzentrum" oder "Datenverarbeitung" zu beachten. Das Umfeld der Gebäude prägt ganz wesentlich die Sicherheitsanforderungen. Offenes, freies Gelände bedarf andersgearteter Sicherungsmaßnahmen und -techniken als Bauwerke innerhalb geschlossener Bebauung. So lassen sich durch eine geschickte Auswahl der Räumlichkeiten die Kosten für zusätzliche Sicherheitsmaßnahmen wesentlich reduzieren.

Bei der Festlegung der Sicherungsmaßnahmen sind insbesondere als Risikofaktoren Überfall, Einbruch, Sabotage, terroristischer Angriff, Brand, Wasser, Gas, Blitzschlag und Erdbeben zu berücksichtigen.

Einen optimalen Schutz für zentrale Netzwerkrechner bieten Räume, die in einem eigenen abgeschlossenen Sicherheitsbereich mit Zugangsüberwachungssystem untergebracht sind und über einen eigenen Brandabschnitt verfügen. Ungünstig für die Lage zentraler Netzwerkrechner oder PC ist der Außenbereich eines Gebäudes hinter einer allgemein zugänglichen Fensterfront.

Im Fensterbereich ist neben den üblichen Sicherungsmaßnahmen (Gitter, Stahljalousien usw.) für ausreichenden Sichtschutz Sorge zu tragen. Dies kann durch Folien, Jalousetten usw. realisiert werden. Durch Verwendung von Verglasungen einer bestimmten Widerstandsklasse kann die Sicherheit in leicht zugänglichen Bereichen erhöht werden. Auf Glas nachträglich aufgebrachte Folien wirken einwurfhemmend und sind besonders in nicht direkt zugänglichen Bereichen zu empfehlen. Die Widerstandsklassen sind in der DIN 52290 festgelegt. Welche Verglasung letztendlich zu wählen ist, richtet sich wiederum nach der konkreten Situation.

Ein weiterer Faktor bei der Außensicherung sind die Türen. Hier bieten Sicherheitstüren nach DIN 18103 mit entsprechenden Sicherheitsschlössern den geeigneten Schutz. Weiterhin sollte durch geeignete Techniken und organisatorische Maßnahmen eine geordnete Zugangskontrolle zu den Rechnerräumen gewährleistet sein.

Beim Einbau von Alarm- oder Feuermeldeanlagen ist darauf zu achten, daß in relativ kurzer Zeit Gegenmaßnahmen getroffen werden können. Solche Anlagen erfüllen diese Zwecke nicht, wenn Gegenmaßnahmen nicht oder zu spät eingeleitet werden.

Für die Aufbewahrung von Akten und Datenträgern sind Schränke oder Behältnisse nach VDMA 24991 (VDMA - Verband Deutscher Maschinen- und Anlagenbau e.V.) zu empfehlen, die ausreichend Schutz gegen Hitze, Feuchte und korrosive Gase bieten.

Weitere Maßnahmen zur Gebäude- und Raumsicherung sind die Videoüberwachung und der Einsatz von Wachschutzdiensten.

1.3.1.12 Löschen nicht mehr benötigter Daten

Löschen ist nach § 3 Abs. 2 Nr. 6 Bbg DSG das Unkenntlichmachen gespeicherter Daten. Prinzipiell unterscheidet man zwischen logischem und physischem Löschen. Beim logischen Löschen einer Datei wird lediglich im Verzeichniseintrag vermerkt, daß die Datei gelöscht wurde. Der Inhalt der Datei bleibt auf dem Speichermedium jedoch eine gewisse Zeit erhalten und kann deshalb noch mit Hilfe von Dienst- und Hilfsprogrammen (z. B. DOS: undelete;

NetWare: salvage; SCO-UNIX: Norton Utilities) unter bestimmten Bedingungen (z. B. der Speicherplatz auf dem Medium wurde noch nicht durch neue Dateien überschrieben; bei NetWare: der Nutzer hat sich noch nicht ab- oder erneut angemeldet) wieder rekonstruiert werden. Beim physischen Löschen einer Datei werden die Daten auf dem Datenträger mit einem festen Wert überschrieben (z. B. NetWare: Purge). Eine Wiederherstellung der Daten ist in diesem Fall nicht mehr möglich. Bei der Verwendung von Formatierungsprogrammen sollte man bedenken, daß nicht in jedem Fall alle Daten auf dem Medium gelöscht werden. In einigen Formatierungsprogrammen kann man durch Angabe von sog. Schaltern (z. B. DOS: format c:/u) das Löschen aller Daten erzwingen. Eine Rekonstruktion der Daten ist dann nicht mehr möglich.

Anwendungsprogramme legen während ihrer Abarbeitung eine ganze Reihe temporärer Daten im Arbeitsspeicher des Rechners ab. Werden diese Daten nicht mehr benötigt, sollte das Anwendungsprogramm diese Variablen, Strukturen, Objekte o. ä. physisch löschen. Dadurch wird nach Beendigung des Programms verhindert, daß Bereiche des Arbeitsspeichers ausgespäht werden können.

1.3.1.13 Deaktivieren von Diskettenlaufwerken

Wird ein Arbeitsplatzcomputer (APC) in einem Netzwerk betrieben, besteht bei einigen Netzwerkbetriebssystemen die Möglichkeit, das Betriebssystem des APC von einem Server zu laden. Die entsprechenden Netzwerkkarten müssen mit einem sogenannten Boot-PROM ausgestattet sein. Dieses Verfahren hat den Vorteil, daß Diskettenlaufwerke zur Installation und Konfiguration von Software auf dem Netzwerk-PC nicht mehr benötigt werden. Um zu verhindern, daß Daten unbefugt auf Diskette kopiert werden, unberechtigt Software ins System eingespielt wird oder virenverseuchte Dateien von der Diskette unbemerkt in den APC übertragen werden, können die Diskettenlaufwerke jetzt ausgebaut oder hardwaremäßig gesperrt werden. Im Netzwerk sollte eine Workstation als sog. "Schleuse" fungieren. Diese Workstation wird mit Virensuchprogrammen (mehrere verschiedene verwenden!) ausgerüstet. Nur auf diesem Rechner werden dann Dateien vom Netzwerk auf die Diskette oder von der Diskette in das Netzwerk kopiert. Bei Neuanschaffungen sollte man bei APC, die an ein Netzwerk angeschlossen werden, grundsätzlich auf Diskettenlaufwerke verzichten.

1.3.1.14 Verwendung einer abgestuften Rechteverwaltung

Die auf dem Markt verfügbaren Netzwerkbetriebssysteme ermöglichen eine differenzierte Vergabe von Rechten auf Verzeichnis- und Dateiebene. Rechte können u. a. an bestimmte Nutzer, Nutzergruppen und Verzeichnisse vergeben werden. So besteht z. B. die Möglichkeit, dem Nutzer A nur Leserechte und dem Nutzer B Lese- und Schreibrechte für bestimmte Dateien zuzuordnen. Durch Verwendung einer abgestuften Rechteverwaltung kann eine Abschottung der Anwendungen realisiert werden. Nach der Installation und Konfiguration des Netzwerkbetriebssystems sollten nur die Rechte an den jeweiligen Nutzer vergeben werden, die für seine Arbeit unbedingt erforderlich sind. Die Vergabe von Rechten muß revisionssicher dokumentiert werden.

Single-User-Betriebssysteme (z. B. DOS) verfügen im allgemeinen nicht über die Möglichkeit zur Vergabe von Rechten. Wenn mehrere Mitarbeiter gemeinsam einen Einzelplatz-PC mit verschiedenen Programmen nutzen, besteht die Möglichkeit, zusätzlich entsprechende Sicherheitssoftware zu installieren. Mit dieser Software können dann auch auf einem Einzelplatz-PC differenziert Rechte für die entsprechenden Nutzer vergeben werden.

1.3.1.15 Vergabe von Paßwörtern

Der Zugriff auf personenbezogene Daten kann durch Eingabe einer Benutzerkennung und eines Paßwortes geschützt werden. Bei der Gestaltung der Paßwortvergabe sollten die vorhandenen Möglichkeiten des Systems voll ausgeschöpft werden. Zum Beispiel mußte ich

bei der Kontrolle einer Behörde feststellen, daß selbst für den Supervisor eines NOVELL-Netzwerkes kein Paßwort vergeben wurde. Im folgenden möchte ich daher auf einige Möglichkeiten bei der Verwaltung und Verwendung von Paßwörtern hinweisen (13 Gebote der Paßwortverwaltung):

- Das System sollte so konfiguriert werden, daß der Nutzer gezwungen wird, ein Paßwort festzulegen (zwingende Paßworteingabe).

- Der Nutzer sollte vom System die Möglichkeit erhalten, daß er sein Paßwort bei Bedarf ändern kann (selbständiges Ändern).

- Die Paßwortlänge sollte auf mindestens sechs Zeichen festgelegt werden (Mindestlänge).

- Durch Verwendung einer History sollte der Nutzer nicht in der Lage sein, bei der Neuvergabe seines Paßwortes wieder das alte Paßwort zu verwenden (Einmaligkeit).

- Der Nutzer sollte automatisch in bestimmten Zeitabständen (ca. 4 - 6 Wochen) zur Änderung seines Paßwortes aufgefordert werden (periodische Änderung).

- Das System sollte so konfiguriert werden, daß keine Möglichkeit zur Eingabe sog. Trivialpaßwörter besteht (z. B. "xxxxxxxx"). In einigen Systemen kann festgelegt werden, daß ein Paßwort aus Buchstaben und Zahlen bestehen muß.

- Nach Ablauf der Gültigkeit des Paßwortes sollte dem Nutzer noch eine bestimmte Anzahl von Anmeldungen gestattet werden. Ist diese Anzahl abgelaufen, sollte der Nutzer vom System automatisch gesperrt werden. Das Entsperren kann nur vom Systemverantwortlichen durchgeführt werden.

- Paßwörter sollten grundsätzlich nur verschlüsselt über das Netz übertragen und verschlüsselt abgespeichert werden. Dadurch wird ein Ausspähen von Paßwörtern verhindert.

- Werden sensible personenbezogene Daten verarbeitet, ist bei der Systemverwaltung das Vier-Augen-Prinzip anzuwenden (geteilte Paßwörter).

- Nach einer bestimmten Anzahl erfolgloser Anmeldeversuche (ca. 3) sollte der Zugang des Nutzers zum System automatisch gesperrt werden.

- Paßwörter sollten grundsätzlich nicht auf dem Bildschirm angezeigt werden, auch dann nicht, wenn sie schon durch neue ersetzt wurden.

- Das Systempaßwort sollte in einem verschlossenen Briefumschlag in einem gesicherten Behältnis aufbewahrt werden.

- Die Nutzer sollten ihre Paßwörter an einem sicheren Ort aufbewahren, oder - besser noch - auswendig lernen.

1.3.2 Dienstanweisungen

Häufig wird in meiner Behörde angefragt, welche Fälle denn bei der praktischen Regelung des Datenschutzes in einer öffentlichen Verwaltung zu berücksichtigen seien. Es ist natürlich jedem freigestellt, die Fälle einzeln oder gebündelt in Dienstanweisungen zu behandeln. Für spezielle Verfahren und Anwendungen müssen ohnehin spezifische Dienstanweisungen entwickelt werden. Zumindestens sollten folgende Punkte geregelt werden:

a) Zugangskontrolle

- Schlüsselvergabe für Diensträume und Dienstgebäude,
- Zugangsberechtigungen zu Rechnerräumen

b) Software

- Dokumentation der zugelassenen Software,
- bei Eigenprogrammierung die Dokumentation von Programmen und die Programmfreigabe,
- Freigabe von Software,
- Wartung von Software

c) Hardware

- Dokumentation der eingesetzten Hardware einschließlich der Vernetzung,
- Einsatz von stationärer ADV-Technik,
- Einsatz mobiler Rechner wie Laptops, Notebooks u. a.,
- einheitliches Verfahren zur Installation und Wartung von Hardware

d) Zugriffskontrolle und Datensicherheit

- Paßwortvergabe,
- Einsatz von ADV-Sicherheitstechnik und Verschlüsselungsverfahren,
- Datensicherungsverfahren und Aufbewahrungsfristen für Sicherungsdateien,
- Schutzstufenkonzept zur Bewertung der Sensibilität personenbezogener Daten,
- Risikoanalyse,
- schriftliche Verpflichtung auf das Datengeheimnis

e) Störfallmaßnahmen

- Havariefälle bei der Datenverarbeitung,
- Störfälle in Rechnerräumen bezüglich Feuer, Wasser, Einbruch u. a.

f) Akten und andere Datenträger

- Festlegung des Aktenplanes,
- Ordnung der Aktenablage,
- Ordnung der sonstigen Datenträgerhaltung,
- kontrollierte Datenträgervernichtung entsprechend den Sicherheitsstufen der DIN 32757

g) Abschottungen

- Funktionstrennung bei Anwenderaufgaben bezüglich Verfahren,
- Funktionstrennung bei der Systemverwaltung

h) Meldungen

- Datenverarbeitung im Auftrag einschließlich Meldung an die zuständige Aufsichtsbehörde und ggf. an den Landesbeauftragten für den Datenschutz,
- Meldung automatisierter Abrufverfahren an den Landesbeauftragten für den Datenschutz

i) Stellung und Befugnisse des behördlichen Datenschutzbeauftragten

j) Arbeit des Systemverwalters

k) Mitbestimmung der Personalvertretung (Dienstvereinbarungen)

- Betrieb der internen TK-Anlage,
- Einsatz und Auswertung von Protokolldateien,
- automatisierte Verarbeitung von Personaldaten.

Diese Aufzählung ist nicht abschließend, sondern stellt eher eine Mindestanforderung an Festlegungen in Dienstanweisungen dar (vgl. auch die "Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik" mit Stand 1991, hrsg. vom Landesrechnungshof Brandenburg).

1.3.3 Die Macht des Systemverwalters

Bei den meisten Betriebssystemen ist es verhältnismäßig leicht, durch eine aufgabenbezogene Rechtevergabe eine effektive Zugriffskontrolle auf personenbezogene Daten für den Anwender zu erreichen. Das ist auch notwendig, weil § 10 Abs. 2 Nr. 5 Bbg DSG fordert, daß die zulässigen Nutzer von ADV-Systemen nur auf die Daten zugreifen dürfen, die sie für ihre Aufgabenerfüllung benötigen. Eine solche eher allgemeine Bestimmung ist schon ausreichend dafür, daß nicht jeder Anwender im Netz alles sehen und können muß. Meistens werden die zulässigen Zugriffe des Anwenders so zugelassen, daß ihm auf dem Bildschirm nur die Anwendungsprogramme in Form von Menüpunkten angeboten werden, zu deren Ausführung er aufgabenbedingt berechtigt ist. Ein Zugang auf das Betriebssystem muß ihm verwehrt sein.

Problematisch ist dagegen fast immer die Rolle des Systemverwalters, der auch als Systemadministrator, Supervisor oder Superuser bezeichnet wird. Einerseits ist er derjenige, der das gesamte System kennen, verwalten und bei Bedarf ändern muß, etwa bei dem Einsatz einer neuen Systemversion. Er muß den Anwendern Hilfe und Anleitung geben können, Datensicherungsmaßnahmen durchführen, bei Systemabstürzen den Nothelfer spielen und Programme, die sich "aufgehängt" haben, abbrechen können. Andererseits kann er in alle Verzeichnisse und Dateien einsehen und die Zugriffsrechte ändern oder neu vergeben. Das schafft ihm nicht immer Freunde. Der eine Anwender fühlt sich kontrolliert; ein anderer wirft ihm vielleicht sogar schon Schlimmeres vor, etwa daß er unberechtigterweise in abgespeicherte Unterlagen Einsicht nähme und Informationen weitergäbe.

Solchen Schwierigkeiten kann folgendermaßen begegnet werden:

a) mit der automatischen Führung einer Protokolldatei, in die das System z. B. Zugriffe auf Programme, Verzeichnisse, Dateien, Dateifelder und Rechtetabellen mit Nutzerkennung, Datum und Uhrzeit einträgt.

   (Eine solche Datei muß verschlüsselt abgespeichert werden, damit sie nicht manipulierbar ist; ihre Löschung muß in der Protokolldatei der nächsten Generation vermerkt werden. Auf diese Weise kann zumindest stets im nachhinein festgestellt werden, wer was wann getan hat. Dadurch kann sich auch der Systemverwalter erheblich entlasten und falscher Anwürfe erwehren. Die Einsicht in solche Protokolldateien ist durch eine Dienstanweisung einerseits und durch eine Dienstvereinbarung zwischen Behördenleitung und Personalvertretung andererseits zu regeln. Denn natürlich wäre eine solche Datei auch dazu geeignet, das Arbeitsverhalten oder die Leistung der Beschäftigten zu überwachen. Derartige Verfahren unterliegen deshalb auch der Mitbestimmung. Die Auswertung sollte folglich mindestens durch zwei Beschäftigte erfolgen und die Ergebnisse in einem Protokoll festgehalten werden. Empfehlenswert ist, daß der behördliche Datenschutzbeauftragte oder ein Mitglied des Personalrats einbezogen werden. Auch die Aufbewahrungsfrist einer solchen Protokolldatei wäre zu regeln.)

b) mit dem Herauslösen eines umstrittenen sensiblen Bereichs aus dem lokalen Netz.

(Der abgeschottete Anwender ist dann sein eigener Herr und nur für sich selbst und seine Daten verantwortlich. Datensicherungsmaßnahmen muß er dann allerdings selbst durchführen. Eine solche Abschottung durch Entflechtung aus einem Rechnernetz ist nicht nötig, wenn die umstrittenen speziellen Daten nach einem anspruchsvollen Verfahren verschlüsselt werden. In diesem Fall bietet sich eine sog. symmetrische Verschlüsselung an. Nur der Anwender kennt den Schlüssel, mit dem seine Daten verschlüsselt sind. Nur er kann diesen Schlüssel ändern. Die Ver- und Entschlüsselung erfolgt dann für ihn automatisch. Der Systemverwalter kann dann zwar diese Daten ansehen, aber nicht lesen im Sinne von verstehen. Der Anwender hat auch noch den Vorteil, daß er sich nicht um seine Backups kümmern muß. Sie erfolgen dann wie üblich bei der Gesamtsicherung des Systems.)

c) mit dem Einsatz solcher Betriebs- bzw. Netzsysteme, die Funktionseinschränkungen seiner Position zulassen.

(Sie gestatten die Aufteilung der Systemverwaltungsarbeiten und können damit ein Vier- oder Sechs-Augen-Prinzip realisieren. Zu solchen Systemen gehören Novell NetWare 4.xx oder Windows NT. Selbst bei älteren Systemen ließen sich bei einigem guten Willen noch Verbesserungen erreichen. Wenn der Systemverwalter seine Arbeit so organisieren könnte, daß er den größten Teil seiner routinemäßigen Verwaltungsarbeiten menügesteuert bewältigt, brauchte er nur in seltenen Fällen auf der Betriebssystemebene zu arbeiten. Um sich aber für diese Fälle abzusichern, könnte er das sog. Vier-Augen-Prinzip einführen, indem er und eine weitere Person sich das Supervisor-Paßwort aufteilen und keiner dem anderen sein Teilpaßwort mitteilt. Ist dann eine Arbeit auf Betriebssystemebene unumgänglich, müssen zumindest immer beide Personen anwesend sein, weil sonst die Arbeit auf dieser Ebene gar nicht gestartet werden könnte.)

1.3.4 Protokollierung und Nutzung von Protokolldateien

1.3.4.1 Protokollierung

Nach § 10 Abs. 2 Nr. 6 und Nr. 7 Bbg DSG besteht die Verpflichtung, zu Zwecken der Übermittlungs- und Eingabekontrolle einer automatisierten Datenverarbeitung nachträglich über entsprechende Informationen zu verfügen. Je nach Sensibilität der personenbezogenen Daten können dies handschriftliche Aufzeichnungen oder automatisch erzeugte Protokolldateien sein, die fortlaufend oder auf Wunsch ausgedruckt oder auf dem Bildschirm angezeigt oder als eigene Datei abgespeichert werden. Wie bereits unter Punkt 1.3.3 dargestellt, ist letzteres besonders zu empfehlen. Da Protokolldateien selbst erheblich schutzbedürftig sind, sollten sie - wie bereits empfohlen - verschlüsselt sein.

Protokolliert werden sollten alle wichtigen Systemveränderungen, wie Einrichten oder Löschen von Nutzerkennungen, Rechtevergabe, Ändern von Paßwörtern, Einsatz neuer Programme sowie das Löschen der aktuellen Protokolldatei. Beim routinemäßigen Datenverarbeitungsbetrieb wären aufzuzeichnen: alle Anmeldeversuche, Zugriffe auf Dateien mit personenbezogenem Inhalt, Programmaufrufe, temporäre Rechteveränderungen, Dateikopiermaßnahmen auf Disketten oder andere Datenträger außerhalb des Fileservers, Hardcopy-Bildschirmabzüge, Datenübertragungen über serielle und parallele Schnittstellen. Für diese Art der Protokollierung ist die zusätzliche Speicherung der personenbezogenen Inhaltsdaten (z. B. die Besoldungsgruppe, die Herr "X" erhalten hat) nicht erforderlich. Sie würde die Sensibilität der Protokolldatei nur zusätzlich erhöhen.

1.3.4.2 Nutzung

Zwar sind die Protokollaufzeichnungen auf die Zwecke der Übermittlungs- und Eingabekontrolle eindeutig festgelegt; trotzdem ist der Abschluß einer Dienstvereinbarung auf der Grundlage von § 65 Nr. 2 Landespersonalvertretungsgesetz (PersVG)[9] dringend zu empfehlen. In ihr sollten die Zwecke der ADV-Protokollierung (Datenschutz, Datensicherheit, Datensicherung, Ordnungsmäßigkeit der Datenverarbeitung), der inhaltliche Umfang der Protokolle, ihre Aufbewahrungsfristen, ihre Löschung, der Ausschluß der Verhaltens- und Leistungskontrolle der Beschäftigten, die für die Auswertung befugten Personen und die Einbeziehung der betroffenen Mitarbeiter fixiert werden.

1.3.5 Kryptographie

1.3.5.1 Warum personenbezogene Daten verschlüsseln?

Die Sinnhaftigkeit dieser technisch-organisatorischen Maßnahmen läßt sich am einfachsten an praktischen Beispielen verdeutlichen:

- Meine Mitarbeiter wurden im Berichtszeitraum in mehrere Ämter gerufen, in die eingebrochen worden war. In jedem Fall waren mehrere PC einschließlich die darauf befindlichen personenbezogenen Daten und Drucker gestohlen worden. Selbst wenn den Tätern primär nicht an den Daten, sondern lediglich an der Rechentechnik gelegen war, so waren jene vor dem Zugriff Unbefugter nicht geschützt. Viele Amtsgebäude in Brandenburg sind so beschaffen, daß trotz des Einbaus von Gebäudesicherungstechnik erneute Diebstahlversuche nicht ausgeschlossen werden können. Aus diesem Grunde habe ich gefordert, daß die personenbezogenen Dateien auf den PC-Servern zukünftig verschlüsselt gespeichert werden sollen. Bei erneutem Diebstahl wäre dann gleichwohl auch der materielle Schaden zu beklagen, jedoch wäre zumindest sichergestellt, daß die Daten nicht von Unbefugten mißbraucht werden können.

- Das Landesamt für Datenverarbeitung und Statistik (LDS) will bei der Erhebung der personenbezogenen Daten nach dem Mikrozensusgesetz den Einsatz von Laptops erproben. In meinem 2. Tätigkeitsbericht (s. unter 4.4, S. 88 ff.) hatte ich bereits darauf hingewiesen, daß Laptops als mobile und leicht tragbare Rechner natürlich höheren Risiken ausgesetzt sind als die üblichen APC in der geordneten Bürowelt der Verwaltung. Das LDS hat sich unseren Forderungen nach einer permanenten Verschlüsselung der Daten auf der Festplatte der Laptops angeschlossen und entsprechende Sicherheitssoftware eingesetzt, die auch die Disketten verschlüsselt ausgibt. Auf diese Weise würde bei einem Diebstahl wohl der wertmäßige Verlust des Geräts zu beklagen sein. Ein Mißbrauch der sensiblen personenbezogenen Daten wäre weder von der Festplatte, noch von der Diskette her möglich. Nicht einmal das gestohlene Gerät wäre ohne weiteres brauchbar, da das Paßwort zum Start des Systems ebenfalls verschlüsselt abgelegt und das Laden eines Programms von der Diskette oder über andere Schnittstellen nicht möglich ist.

1.3.5.2 Verschlüsselungsverfahren

Bei der Verschlüsselung von Informationen wird zwischen symmetrischer und asymmetrischer Verschlüsselung (Chiffrierung, Kryptographie) unterschieden.

Bei dem symmetrischen Verfahren wird für die Ver- und Entschlüsselung derselbe Schlüssel benutzt. Das bedeutet, daß jeweils immer zwei Kommunikationspartner einen geheimen Schlüssel vereinbaren müssen. Praktisch wird dies durch den Einsatz von ADV-Programmen zur Schlüsselgenerierung erreicht, wobei die geschützte Schlüsselübermittlung ein Problem darstellt. Sender und Empfänger besitzen also den gleichen Schlüssel k, den sonst niemand

[9] vom 15. September 1993, GVBl. I S. 358

kennen darf. Gibt es n Kommunikationspartner, sind folglich insgesamt n(n-1)/2 geheime Schlüssel erforderlich. Bereits 5 Partner benötigten danach 10 geheime Schlüssel, 10 Partner bereits 45, 100 Partner 4950 Schlüssel und 1000 Teilnehmer 499500 Schlüssel, so daß das Schlüsselmanagement bei steigender Teilnehmerzahl äußerst kompliziert wird. Für viele Anwendungen ist aber dieses Verfahren völlig ausreichend, etwa für die unter 1.3.5.1 geschilderten Fälle. Außerdem ist der Vorgang des Verschlüsselns recht schnell, besonders dann, wenn zusätzliche Hardware-Chips eingesetzt werden. Ein heute allgemein anerkannter Algorithmus dieses Verschlüsselungstyps ist der DES (Data Encryption Standard), der in den 70iger Jahren in den USA entwickelt wurde.

Ein asymmetrisches Verschlüsselungsverfahren, auch public-key-Verfahren genannt, verfügt pro Teilnehmer über zwei Schlüssel: einen öffentlichen und einen geheimen. Jeder Kommunikationspartner teilt seinen öffentlichen Schlüssel, vergleichbar einem Telefonbucheintrag, einer vertrauenswürdigen Schlüsselzentrale (trust center) mit, die diesen Schlüssel auch noch zertifizieren muß. Er ist also nicht geheim. Seinen geheimen Schlüssel kennt jeder Besitzer eines öffentlichen Schlüssels nur allein; er darf nicht bekannt werden. Zwischen dem öffentlichen und geheimen Schlüssel besteht eine komplizierte mathematische Beziehung. Sie ermöglicht es, daß der Absender eines geheimzuhaltenden Textes diesen mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und den so verschlüsselten Text dann an den Empfänger übermittelt. Dieser kann ihn mit seinem geheimen Schlüssel entschlüsseln, niemand sonst. Auf diese Weise benötigen n Kommunikationspartner auch nur n Schlüssel. Das bekannteste dieser Verfahren ist der RSA-Algorithmus (nach den Entwicklern Rivest, Shamir und Adleman). Allerdings arbeitet dieser Algorithmus ausgesprochen langsam.

1.3.5.3 Sicherheit der Schlüssel

Man kann davon ausgehen, daß die Verfahren nach dem DES- und dem RSA-Algorithmus unter gewissen Einschränkungen heute die sichersten Verschlüsselungsmethoden darstellen. Beim DES sollte nach Möglichkeit mit dem sog. Triple-DES (Schlüssellänge 112 Bit) gearbeitet werden, beim RSA-Verfahren mit einer Schlüssellänge von 1024 Bit. Unter diesen Bedingungen sind selbst bei massiv steigender Rechnerleistung für eine überschaubare Zeit keine erfolgreichen kryptoanalytischen Angriffe zu erwarten. Aus diesem Grund sollten andere Verschlüsselungsalgorithmen nicht genutzt werden, zumal die mathematischen Verfahren von DES und RSA veröffentlicht und somit also bekannt sind.

Allerdings nutzen die besten Verfahren nichts, wenn das Umfeld nicht stimmt, etwa, wenn die Geheimhaltung der geheimen Schlüssel leichtfertig aufgegeben wird oder das Personal nicht vertrauenswürdig oder das Schlüsselmanagement nicht sicher ist.

1.3.5.4 Praxis

Um die Geschwindigkeit der DES und das relativ einfache Schlüsselmanagement des RSA-Verfahrens zugleich zu nutzen, wird häufig eine Kombination beider Verfahren eingesetzt. Zunächst erzeugt der Absender mit einem Zufallsgenerator einen DES-Sitzungsschlüssel. Dadurch wird bei routinemäßigem Sendebetrieb bei jeder Sitzung ein neuer Schlüssel verwendet, was der Geheimhaltung dienlich ist. Mit diesem verschlüsselt er die zu übermittelnde Datei nach dem DES. Danach wird mit dem öffentlichen Schlüssel des Empfängers der soeben genutzte DES-Schlüssel nach dem RSA-Verfahren verschlüsselt. Darauf wird eine neue Datei erstellt, die aus folgenden Komponenten besteht: RSA-verschlüsselter DES-Sitzungsschlüssel, evtl. zusätzliche Informationen des Absenders und DES-verschlüsselte Nutzdatei. Diese Komplex-Datei wird dem Empfänger über das Netz zugestellt. Der Empfänger trennt nun die aus den drei Komponenten bestehende Datei wieder auf und entschlüsselt mit seinem geheimen Schlüssel mittels RSA den mit seinem eigenen öffentlichen RSA-Schlüssel verschlüsselten DES-Schlüssel des Absenders. Jetzt wird mit diesem DES-Schlüssel die eigentliche Nutzdatei entschlüsselt, so daß im Ergebnis diese Datei

als Klartext vorliegt.

Wird bei einer solchen Kommunikation zusätzlich noch Wert auf die Echtheit des Absenders gelegt, also auf seine Authentisierung, kann dazu dessen sog. elektronische Unterschrift genutzt werden. Diese Unterschrift ist allerdings keine Unterschrift im üblichen Sinn, sondern eine digitale Information des Absenders. Diese Nachricht verschlüsselt der Absender zusätzlich mit seinem eigenen geheimen RSA-Schlüssel. Der Empfänger entschlüsselt diese "Unterschrift" seinerseits wieder mit dem öffentlichen Schlüssel des Absenders. Erhält er den plausiblen Klartext, ist der Absender verifiziert. In allen anderen Fällen wird der Empfänger lediglich "Datenmüll" erhalten.

1.3.5.5 Weitere Probleme

Manchmal kann es wichtig sein, daß nicht nur der Inhalt einer Information (Datei) vertraulich bleiben soll, sondern auch die Nachvollziehbarkeit der Nachrichtenübermittlung (Verbindungsdaten) oder die Tatsache der Übermittlung überhaupt. In diesen Fällen sind weiter- führende Maßnahmen erforderlich.

Strafverfolgungsbehörden stören sich an Verschlüsselungsmethoden für den Fall, daß sie im Rahmen ihrer Ermittlungstätigkeit in begründeten Verdachtsfällen Informationen nicht entschlüsseln können. Allerdings kann man mit Hilfe von sog. Steganographie-Verfahren (griech. steganos: bedeckend, schützend, festschließend, dicht, bedeckt, verdeckt) in "normalen" unverschlüsselten Texten, Bildern oder telefonischen Gesprächen rechnergestützt Informationen übermitteln, die kein Dritter ohne geheimes Wissen entschlüsseln kann. Die einfachste Form der Steganographie ohne Rechnerunterstützung ist z. B. in einem "normalen" Telefonat zwischen zwei Partnern allein dadurch möglich, daß sie vorab mit bestimmten "normalen" Wörtern als Codes die Beschreibung von definierten Ereignissen oder Sachverhalten vereinbart haben. Benutzen sie diese nun ganz zwanglos während des Gesprächs, ist die geheime Information bereits übermittelt, ohne daß ein Außenstehender den Inhalt der Information noch überhaupt die Tatsache ihrer Übermittlung feststellen kann. Allein aufgrund dieser faktischen Möglichkeiten wird die Reglementierung von Verschlüsselungsverfahren absurd.

Die Einrichtung von vertrauenswürdigen Schlüsselzentralen ist problematisch, wenn diese die öffentlichen und geheimen Schlüssel selbst herstellen, was die Handhabung allerdings erheblich erleichtern würde. Aus datenschutzrechtlichen Gründen wäre es zu begrüßen, wenn der geheime Schlüssel in einer Chipkarte verschlüsselt gespeichert und durch ein Paßwort geschützt wäre. Dies würde außerdem das Verschlüsseln einer Datei wesentlich erleichtern. Allerdings dürfte sich der geheime Schlüssel stets nur auf der Chipkarte befinden und an keiner anderen Stelle sonst gespeichert werden.

1.3.6 Optische Datenträger

Unter den in § 19 Bbg DSG genannten Voraussetzungen muß eine Berichtigung, Löschung und Sperrung von Daten möglich sein. Dies ist bei der Auswahl und beim Einsatz von Datenträgern zu beachten.

Bei magnetischen Speichersystemen (z. B. Festplatten, Disketten, Magnetbändern) können die Forderungen des Datenschutzgesetzes in der Regel erfüllt werden. Zu beachten ist allerdings, daß magnetische Datenträger nicht zur Langzeitarchivierung verwendet werden können. Diese Datenträger sollten spätestens nach ca. drei Jahren kopiert werden, um Datenverluste zu vermeiden.

Anders verhält es sich mit optischen Datenträgern (z. B. CD-ROM, WORM, MOD). Magneto-optische Datenträger (MOD) ermöglichen das Ändern und Löschen der Daten und stellen damit in Bezug auf § 19 Bbg DSG kein Problem dar. Im Gegensatz dazu ist es bei CD-ROM (Compact Disc Read Only Memory) bzw. WORM (Write Once Read Many) nicht möglich, unrichtige Daten zu löschen oder zu verändern. Durch organisatorische Maßnahmen kann der Widerspruch zwischen der einerseits geforderten manipulationssicheren Speicherung von Daten und dem rechtlichen Anspruch des Betroffenen auf Änderung, Löschung oder Sperrung seiner Daten andererseits gelöst werden. Zum Beispiel könnten die Datenbestände auf den einmal beschreibbaren Datenträgern nach einem möglichst kurzen Zeitraum durch Umkopieren auf einen neuen Datenträger bereinigt werden. Beim Umkopieren werden dabei nur die noch benötigten Daten verwendet. Der ursprüngliche Datenträger ist dann unverzüglich zu vernichten (Vernichtung des Datenträgers unter Beachtung der DIN 32757). Aufgrund der Kostenentwicklung bei einmal beschreibbaren Datenträgern (z. B. bei CD-ROM derzeit ca. 40 DM) ist das Verfahren als verhältnismäßig

anzusehen.

Ein weiteres Problem bei der Verwendung einmal beschreibbarer optischer Datenträger ist die Anerkennung der Beweiskraft der elektronisch gespeicherten Daten. Im Gegensatz zur Mikroverfilmung, bei der Auszüge, Ausfertigungen und Abschriften von Mikrofilmaufnahmen gem. § 299 a Zivilprozeßordnung[10] (ZPO) im allgemeinen von den Gerichten anerkannt werden, gibt es zur Beweiswürdigung elektronisch-gespeicherter Dokumente derzeit noch keine gesetzlichen Regelungen. Es ist daher ratsam, die Originale, die zur Archivierung auf einmal beschreibbaren optischen Datenträgern abgelegt werden, zur Beweissicherung weiterhin aufzubewahren.

Aufgrund der datenschutzrechtlichen Probleme beim Einsatz von einmal beschreibbaren optischen Speichermedien sollten diese Datenträger möglichst nur zur Langzeitarchivierung verwendet werden. Dabei sollte man darauf achten, daß nur Daten mit gleichen Löschungsfristen auf dem gleichen Datenträger abgelegt werden.

1.3.7 Wann wird Wartung zur Datenverarbeitung im Auftrag?

In meinem 2. Tätigkeitsbericht[11] habe ich ausgeführt, daß die Wartung und Fernwartung von automatisierten Datenverarbeitungssystemen eine Form der Datenverarbeitung im Auftrag gem. § 11 Bbg DSG ist. Bei Kontrollen von ADV-Anwendungen im Land stieß dies gelegentlich auf Unverständnis. So wurde u. a. darauf hingewiesen, daß während einer Wartung gar keine personenbezogenen Daten auf den Rechnern seien, weil diese vorher durch Backup-Verfahren gesichert und auf der Serverplatte gelöscht würden. In anderen Fällen werde die Wartung im wesentlichen durch Mitarbeiter der Behörde selbst durchgeführt; defekte PC würden dabei aus dem Netz genommen und Daten auf der lokalen Festplatte gelöscht. In diesen Fällen lag tatsächlich keine Datenverarbeitung im Auftrag vor, da personenbezogene Daten nicht eingesehen werden konnten.

Allerdings mußten die ADV-Anwender einräumen, daß gleichwohl Situationen entstehen können, in denen - etwa bei einem Programmabsturz - dem Anwender praktisch nur noch eine Wartungsfirma helfen kann. In einigen Fällen ist dann nicht einmal mehr das Löschen der Festplatte möglich oder sachgerecht. Für diese Fälle, in denen es sich dann doch um eine Datenverarbeitung im Auftrag handeln würde, sollte bereits in den Wartungsverträgen nach Maßgabe der Bestimmungen des § 11 Bbg DSG Vorsorge getroffen werden (s. unter 1.3.1.8).

1.4 Neue Technologien

1.4.1 Die Datenautobahn

Der "G-7-Gipfel" der führenden Industriestaaten hat vor kurzem weltweit die Weichen für eine globale Informationsgesellschaft gestellt. Mehr und mehr wachsen Computertechnik, Telekommunikation, Unterhaltungselektronik und Medien zusammen. In Zukunft ermöglichen geeignete Zusatzeinrichtungen für Computer, Telefon und Fernsehgerät die Nutzung von Datenautobahnen, auf denen Informationen als Massengut in kürzester Zeit weltweit versandt werden können, für jeden Bürger von der Wohnung aus.

Der Einkaufsbummel wird durch Teleshopping - also die Bestellung von zu Hause aus -

---

[10] i. d. Fassung vom 12. September 1950, BGBl. S. 533, zul. geänd. 10. Oktober 1994, BGBl. I S. 2954

[11] s. unter 1.2.1.2, S. 11 ff.

ersetzt. Medizinische Beratungen, Recherchen in Bibliotheken und Anfragen bei den Behörden können künftig über die Glasfasern der Datennetze erfolgen. Videokonferenzen - bei denen man sich sieht und miteinander reden kann, ohne dabei sein Büro verlassen zu müssen - werden auch den Arbeitsalltag von zukünftigen Abgeordneten und Verwaltungsmitarbeitern verändern. Telelearning bietet völlig neue Dimensionen in der Aus- und Weiterbildung. Auch wird es das Angebot geben, Videofilme aus "digitalen Videotheken" abzurufen (Video on Demand), interaktive multimediale Bildungs- und Unterhaltungsangebote wahrzunehmen, mit Hilfe von Telebanking die Kontoführung von zu Hause aus zu realisieren, weltweit Nachrichten und Daten zu versenden oder durch Telearbeit sich den Weg ins Büro zu ersparen. Diese aufgezählten Möglichkeiten stellen nur einen Teil der angedachten Technologien dar. In absehbarer Zeit wird auf dem Gebiet der Kommunikations- und Informationstechnik eine Menge geschehen. Es werden zukünftig eine Vielzahl von neuen Techniken entstehen, die in unterschiedlichsten Pilotprojekten zum Teil jetzt schon technisch erprobt werden.

Viele der neuen Kommunikationstechniken beruhen auf dem Prinzip der Interaktivität. Das bedeutet, daß im Gegensatz zu den broadcast-orientierten Systemen, wie z. B. das Fernsehen, ein Rückkanal im System vorhanden sein muß. Der Anwender benötigt dazu ein interaktives Endgerät (z. B. Zusatzgerät für Fernseher oder Computer), mit dessen Hilfe über ISDN oder andere schnelle Netze ein Rückkanal zum Anbieter aufgebaut wird. Durch diesen Rückkanal werden Informationen über den Anwender übertragen, z. B. wer hat wann welche Filme gesehen oder wer hat an welchem Bildungsangebot teilgenommen. Neben den möglichen gesellschaftlichen Risiken einer sozialen Entfremdung wird auch der Datenschutz mit völlig neuen Interessenkonflikten konfrontiert. Werden personenbezogene Daten der Nutzer solcher interaktiven Dienste gespeichert, so besteht die Gefahr, daß daraus gezielt Kommunikationsprofile erstellt werden, deren Auswertung kommerzielle Bedeutung zukommt. Insoweit dürfte die Begehrlichkeit zum Mißbrauch an diesen Daten sehr hoch einzuschätzen sein.

Eine wichtige Voraussetzung für die Akzeptanz neuer Kommunikationssysteme sind deshalb der Schutz personenbezogener Daten, die Transparenz der Systeme und die Vertraulichkeit und Verbindlichkeit der Informationen. Das Recht auf informationelle Selbstbestimmung muß in jedem Fall gewahrt bleiben. Dazu ist es erforderlich, schon frühzeitig rechtliche Rahmenbedingungen zu schaffen, in denen die Verwendungsmöglichkeiten neuer Kommunikationstechniken klar definiert werden.

1.4.2 Sicherheit in Datennetzen

Während in den vergangenen Jahren der Schwerpunkt der DV-Anwendungen in vielen Bereichen der öffentlichen Verwaltung des Landes Brandenburg im Einsatz kleinerer Rechnersysteme unterschiedlicher Leistungsfähigkeit lag, sollen diese nun mehr und mehr flächendeckend vernetzt werden. Für viele lokale Netze, deren Reichweite sich bisher auf einzelne Abteilungen oder Gebäude beschränkte, wird zur Nutzung zentraler Datenbestände, zum elektronischen Austausch von Dokumenten und zur Übertragung von Mitteilungen oder Nachrichten in absehbarer Zeit eine Ausdehnung erforderlich. Einige Beispiele hierfür sind:

- die verstärkten Aktivitäten des Innenministeriums zum Aufbau des Landesverwaltungsnetzes Brandenburg,

- die Erweiterung des anfänglich überwiegend für die Sprachkommunikation genutzten Telekommunikationsverbundes der Obersten Landesbehörden auf den Datenaustausch,

- die von der Konferenz der Innenminister und Senatoren der Länder am 20.08.1993 beschlossene Nutzung eines elektronischen Mitteilungssystems für den Dokumentenaustauch zwischen dem Bund und den Ländern ab 1995.

Die flächendeckende Vernetzung bietet jedoch nicht nur die für einen übergreifenden Rechner- und Datenverbund dringend benötigte Infrastruktur, sie führt auch zu erheblichen Datensicherheitsproblemen, denen bereits bei der Konzeption der Netze durch geeignete Maßnahmen entgegengewirkt werden muß. Oft resultiert die fortschreitende Vernetzung der Systeme aus dem Interesse nach einer übergreifenden, verfahrensunabhängigen Funktions- und Datenintegration. Dabei kann noch nicht genau vorherbestimmt werden, welche personenbezogenen Daten in Zukunft im Netz verarbeitet werden sollen. Damit ist ihre Einordnung entsprechend ihrer Sensibilität in das für lokale Netze bewährte Schutzstufenkonzept[12] nicht möglich. Deshalb sollte für Netze von Anfang an ein gewisser Mindestschutz vorgesehen werden, der den mit typischen Anwendungen verbundenen Sicherheitsrisiken gem. § 10 Bbg DSG begegnet und damit in der Regel für die Speicherung sensibler personenbezogener Daten ausreicht. Dieser Grundschutz sollte im Einzelfall bei der Verarbeitung sehr sensibler personenbezogener Daten um zusätzliche Sicherheitsmaßnahmen erweitert werden. Selbst wenn zu Beginn keine personenbezogenen Daten verarbeitet werden sollen, muß das Netz für künftige Anwendungen ausgelegt sein, die höhere Sicherheitsstandards benötigen. Das gilt besonders für solche Netzkomponenten, die nachträglich nur sehr kostspielig modifiziert werden können.

Grundsätzlich abzulehnen sind deshalb auch die in brandenburgischen Verwaltungen erkennbaren Tendenzen, meine Forderungen zur Nutzung von Sicherheitskomponenten mit dem Argument zurückzuweisen, daß keine personenbezogenen Daten übertragen werden. So besteht die Gefahr, daß Netze mit erheblichen Sicherheitslücken in Betrieb gehen und aus Kostengründen bereits am Markt verfügbare Sicherheitsprodukte nicht genutzt werden. Dabei dient die Erhöhung der Sicherheit in Netzen nicht nur dem Schutz personenbezogener Daten. Die meisten Unternehmen der Wirtschaft haben bereits erkannt, daß technisch-organisatorische Maßnahmen, die der Datenschutz fordert, auch einen wirkungsvollen Schutz gegen Wirtschaftsspionage bieten und zu einer rechtsverbindlichen Kommunikation beitragen.

---

12 Broschüre: "Sicherheit am PC und in lokalen Netzen - Dateienregister", 1. Aufl. September 1993, S. 4, aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert"

Nach dem gegenwärtigen Stand der Technik ist davon auszugehen, daß Netze ohne zusätzliche Sicherheitsvorkehrungen grundsätzlich angreifbar sind. Die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete im März 1995 die in Anlage 11 abgedruckte Entschließung zum Datenschutz bei elektronischen Mitteilungssystemen. Die darin geforderten Sicherheitsaspekte lassen sich zum großen Teil auch auf andere Netzdienste übertragen.

1.4.3 Wie sicher ist die mobile Kommunikation?

Stark sinkende Preise und ständig handlicher werdende Telefonapparate lassen Mobiltelefone immer mehr zum Massenartikel werden. Die neuen mobilen Sprach- und Datenübertragungsdienste schaffen - für jeden nachvollziehbar - willkommene Mobilität, Erreichbarkeit an fast jedem beliebigen Ort und Bequemlichkeit. Weit weniger bekannt dürfte hingegen sein, daß damit neue Risiken für das nicht öffentlich gesprochene Wort verbunden sind.

1.4.3.1 Gefahren

Die Übertragung personenbezogener oder sonstiger vertraulicher Informationen mittels mobiler Kommunikationsdienste unterliegt besonderen Gefahren, die sich in erster Linie aus dem eingesetzten Übertragungsmedium "Luft" ergeben. Viel schwieriger als bei der leitungsgebundenen Übertragung können die Signale auf der "Luftschnittstelle" gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden. Ein weiteres Problem besteht darin, daß die ständig ihren Standort wechselnden Kommunikationspartner geortet werden müssen, um erreichbar zu sein. Falls sie selbst eine Verbindung aufbauen möchten, müssen sie Informationen über ihre aktuelle Position abgeben. Diese Standortinformationen können zur Bildung sog. "Bewegungsprofile" mißbraucht werden. Zusätzlich kompliziert und unübersichtlich wird die Situation dadurch, daß bei verschiedenen Netzbetreibern sog. "Serviceprovider", die die Dienste lediglich vermarkten und abrechnen, personenbezogene Daten speichern oder daß bei der internationalen Mobilkommunikation in solchen Staaten personenbezogene Daten anfallen, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen eine dem Fernmeldegeheimnis vergleichbare Regelung nicht existiert.

Die bei der mobilen Kommunikation anfallenden Daten lassen sich ganz grob in drei wesentliche Gruppen einteilen:

1.4.3.2 Bestandsdaten

Bestandsdaten sind solche Daten, die mit der Anmeldung des Anschlusses dauerhaft gespeichert und bereitgehalten werden. Dazu gehören u. a. Rufnummer, Name und Anschrift des Teilnehmers, Zahlungsart und abhängig davon die Bankverbindung oder die Daten der Kreditkarte, Nummern und Geheimzahlen der genutzten Telefonkarten, Art des Endgerätes, verfügbare Leistungsmerkmale und Berechtigungen. Ebenfalls registriert wird, ob und in welcher Form ein Eintrag in die Kundenverzeichnisse (Telefonbücher oder CD-ROM usw.) gewünscht wird und wie mit den Verbindungsdaten nach Rechnungslegung verfahren werden soll. Inzwischen ist es auch üblich, wenn ein entsprechender Telefonanschluß beantragt wird, eine SCHUFA-Auskunft einzuholen. Dabei werden personenbezogene Daten an die SCHUFA übermittelt und in Einzelfällen Bonitätsdaten bei Wirtschaftsauskunfteien abgefragt.

1.4.3.3 Verbindungsdaten

Die Verbindungsdaten geben Auskunft über die näheren Umstände jedes einzelnen Kommunikationsvorganges. Dazu gehören:

- Art der Verbindung (abgehender oder ankommender Ruf, Notruf usw.),
- Kennung des rufenden und des gerufenen Anschlusses,
- Kennung des Ursprungs- und des Zielstandortes,
- Zeitpunkt von Verbindungsbeginn und -ende,
- Dienstekennung (Telefon, FAX, usw.),
- aktivierte Zusatzdienste und
- Datenaufkommen.

Die Verbindungsdaten werden an das Abrechnungszentrum des jeweiligen Netzbetreibers geschickt, dort werden Entgeltdaten ermittelt und zusammen mit den Verbindungsdaten zur Rechnungserstellung verwendet oder an den zuständigen Serviceprovider übermittelt. In Abhängigkeit von der Form des Einzelentgeltnachweises erfolgt eine vollständige Speicherung der Zielnummer oder eine Kürzung um die letzten drei Ziffern. Je nach Wahl des Kunden können die Verbindungsdaten nach Rechnungslegung sofort gelöscht oder für weitere 80 Tage verkürzt oder komplett gespeichert werden.

1.4.3.4 Inhaltsdaten

Die Inhaltsdaten sind die den Kommunikationspartnern übermittelten Informationen, die eigentlichen Nutzdaten. Dazu gehören u. a. die gesprochenen Worte, codierte Texte oder Bilder und übertragene Daten. In analogen Netzen können Inhaltsdaten mit frei verkäuflichen Scannern relativ leicht abgehört werden. In den D- und E-Netzen dagegen ist dies wegen der Digitalisierung nicht ganz so einfach, aber prinzipiell möglich. Eine Verschlüsselung der digitalen Daten soll deshalb ein Mithören der Daten auf der Funkstrecke erschweren. Dabei ist kritisch anzumerken, daß der Schutz unter anderem auf der Geheimhaltung der Verschlüsselungsalgorithmen beruht. Diese Algorithmen sind allerdings zwangsläufig allen Herstellern von Mobiltelefonen und Basisstationen bekannt.

Das Fernmeldegeheimnis schützt nicht nur die Inhaltsdaten einer Kommunikation, sondern auch die näheren Umstände des Fernmeldeverkehrs. Darunter fallen insbesondere auch Angaben darüber, wer wann mit wem von welchem Ort aus kommuniziert hat. Das Fernmeldegeheimnis wird deshalb nicht nur dann verletzt, wenn Außenstehende, die nicht Urheber oder Adressat des Fernmeldeverkehrs sind, Kenntnis vom Inhalt der Kommunikation erhalten, sondern auch dann, wenn sie erfahren, daß eine Kommunikation zwischen den Teilnehmern stattgefunden hat oder unter welchen genaueren Umständen sie abgewickelt wurde.

Im folgenden werden einige spezielle datenschutzrechtliche Risiken, die sich bei der Nutzung von schnurlosen Telefonen und der einzelnen Mobiltelefonnetze ergeben, dargestellt:

1.4.3.5 Schnurlose Telefone

Schnurlose Telefone sind keine echten Mobiltelefone. Bei ihnen werden lediglich einige Teilfunktionen zwischen dem Telefonhörer mit der Wähleinrichtung und der am Festnetz angeschlossenen Grundeinheit in einem begrenzten Umfeld schnurlos übertragen. Die am häufigsten verbreitete Technik nutzt dazu analoge Funksignale, die in einem Umkreis von bis zu 500 m mit handelsüblichen Scannern problemlos abgehört werden können. Die Nutzer des schnurlosen Mobilteils eines Telefons sollten also stets beachten, daß das Gespräch mit einfachen Mitteln in ihrer Nachbarschaft mitgehört werden kann und deshalb empfiehlt es sich, vertrauliche Gespräche über ein verkabeltes Telefon zu führen. Mit schnurlosen Telefonen ist ein relativ abhörsicheres Telefonieren nur möglich, wenn Geräte eingesetzt werden, bei denen die Signale zwischen dem Funkteil und der Feststation digitalisiert und verschlüsselt sind. Von dieser Möglichkeit wird allerdings bei den meisten im Handel erhältlichen Geräten aus Kostengründen kein Gebrauch gemacht.

1.4.3.6 B- und C-Netze

Im B- und C-Netz erfolgt die gesamte Übertragung der Gespräche und der für den Verbindungsaufbau erforderlichen Daten analog. Daher ist ein Abhören auch auf der Funkstrecke mit inzwischen frei verkäuflichen Scannern relativ leicht möglich. Sensible Gespräche sollten von diesen Geräten nicht geführt werden.

1.4.3.7 D-Netze

In den D-Netzen werden sowohl die Gespräche, als auch die für den Verbindungsaufbau erforderlichen Daten - insbesondere die Wählinformationen - digitalisiert übertragen. Dies gilt sowohl für die Funkstrecke, als auch im Festnetz. Hierzu sind die D-Netze mit digitalen Stand- bzw. Mietleitungen der Telekom verbunden. Mehrere Basisstationen (BSS) sind über ein Mobil-Switching-Center (MSC) an das Festnetz angeschlossen. Der von einer BSS erfaßte Bereich wird als Funkzelle bezeichnet und hat abhängig von den örtlichen Gegebenheiten einen Radius von etwa 35 km. Im MSC findet der wesentlichste Teil der Verwaltung der D-Netze statt. Um eine Verbindung zu einem Mobiltelefon aufbauen zu können, muß der Netzbetreiber die momentanen Standorte der Teilnehmer kennen. Hierzu wird eine für jeden Mobilanschluß eindeutige Kennung verwendet, die auf einer Chipkarte, ohne die das Mobiltelefon nicht betrieben werden kann, vorliegt. Beim Einschalten des Gerätes meldet es sich mit seiner Chipkartenkennung bei der nächsten BSS an. Diese schickt die Information über den Aufenthaltsort des Mobiltelefons an das zuständige MSC. Dort wird auch die jeweilige Basisstation gespeichert, in deren Bereich das Mobiltelefon sich gerade befindet und festgehalten, ob das Gerät ein- oder ausgeschaltet ist. Obwohl die Übertragung auf der Funkstrecke in den D-Netzen digital und in verschlüsselter Form erfolgt, wird wegen der Nutzung von Festnetzen der Telekom bei D-Netzen insgesamt nur das Sicherheitsniveau von Festnetzen erreicht. Daher sollten Gespräche mit sehr sensiblen Inhalten nicht am Telefon geführt werden. Im übrigen ist auch zu beachten, daß durch die Speicherung der Verbindungsdaten und der Standortinformationen prinzipiell die Erstellung eines Bewegungsprofils des mobilen Fernsprechteilnehmers möglich ist.

1.4.3.8 E-Netz

Für das E-Netz gelten ebenfalls die zu den D-Netzen gemachten Aussagen entsprechend. Allerdings arbeiten die Mobiltelefone im E-Netz mit einer wesentlich geringeren Sendeleistung, so daß die daraus resultierenden kleineren Funkzellen eine genauere Ortung der Teilnehmer sogar zulassen, als dies in den übrigen Netzen möglich wäre.

1.4.3.9 Datenschutzrechtliche Forderungen

Die mit der Nutzung der mobilen Telekommunikationsdienste verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Von den Herstellern, Betreibern und Nutzern derartiger Dienste ist deshalb zu fordern, daß sie diesen Gefahren durch geeignete technische und organisatorische Vorkehrungen entgegenwirken. Aus datenschutzrechtlicher Sicht erscheinen folgende Forderungen notwendig:

- Die Teilnehmer von mobilen Kommunikationsdiensten müssen eindeutig über die mit der Nutzung verbundenen Risiken und den erreichten Sicherheitstandard aufgeklärt werden. Falls durch den Dienstbetreiber nicht das aus der Sicht des Teilnehmers erforderliche Sicherheitsniveau gewährleistet werden kann, muß eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst unterbleiben.

- Die Mobilkommmunikation ist dadurch gekennzeichnet, daß an verschiedenen Stellen (Netzbetreiber, Diensteanbieter, Serviceprovider) personenbezogene Daten heute in der Regel mehrfach gespeichert werden. In der bevorstehenden Überarbeitung des Telekommunikationsrechtes muß gesetzlich dafür Sorge getragen werden, daß die personenbezogene Datenverarbeitung bei diesen Stellen auf das erforderliche Maß beschränkt und daß der Nutzer darüber aufgeklärt wird, welche Stellen welche personenbezogenen Daten von ihm speichern und weiterverarbeiten dürfen.

- Problematisch ist es, wenn bei der internationalen Mobilkommunikation in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist und das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb sind auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei Nutzung mobiler Kommunikationsdienste auch dort gewährleisten.

- Die Nutzer der Mobilkommunikation, insbesondere Behörden und sonstige öffentliche Stellen, sollten sich vergegenwärtigen, daß auch im Bereich der Kommunikation viele Wege zum Ziel führen. Nicht immer ist der modernste oder kostengünstigste Weg auch der sicherste. Negativen Technikfolgen kann man dann am besten vorbeugen, wenn man die Fragen der Rechtmäßigkeit und Verarbeitungssicherheit entscheidet, bevor man sich der betreffenden Techniken bedient.

1.4.4 Kommt die elektronische Autobahnmaut?

Derzeit werden in der Bundesrepublik und in anderen europäischen Ländern Vorbereitungen getroffen, um ab 1998 den Verkehrsproblemen durch den Einsatz elektronischer Mautsysteme zu begegnen. Technische Lösungen und Einsatzkonzepte sind hierfür entwickelt worden. Beide werden in einem vom Bundesverkehrsministerium getragenen Feldversuch auf der A 555 zwischen Bonn und Köln zur Erhebung einer streckenbezogenen zeitabhängigen Autobahngebühr erprobt.

Bereits in meinem 2. Tätigkeitsbericht[13] habe ich von den Vorbereitungen auf Bundesebene

---

13 s. unter 1.4.3, S. 29 f.

berichtet und auf datenschutzrechtliche Probleme der beiden grundlegenden Verfahren Post-paid und Prepaid hingewiesen.

Im Berichtszeitraum haben Gespräche zwischen dem Bundesverkehrsministerium, der am Feldversuch beteiligten Firmen und Vertretern der dazu Beauftragten mit dem Ergebnis stattgefunden, daß nunmehr von keinem der daran Beteiligten der Grundsatz der Erforderlichkeit einer datenschutzgerechten Ausgestaltung sowohl bei elektronischen Autobahnmaut- als auch bei anderen Telematiksystemen im Verkehr in Zweifel gezogen wird. Wegen der Aktualität der Problematik hat die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder die als Anlage 12 abgedruckte Entschließung gefaßt. In Vorbereitung dazu wurden vom Arbeitskreis Technik der Konferenz die nachfolgenden Kriterien erarbeitet.

1.4.4.1 Anonymität

Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Je weniger personenbezogene oder personenbeziehbare Daten erhoben, verarbeitet oder genutzt werden, desto geringer ist auch die Gefahr einer mißbräuchlichen Datennutzung. Aus diesem Grund ist das Anonymitätskriterium die wichtigste Datenschutzanforderung. Jedenfalls sollten bei regelgerechter Straßenbenutzung keine personenbezogenen Daten entstehen. Das bedeutet, daß auch keine Angaben erhoben oder verarbeitet werden, aus denen sich im nachhinein ein Personenbezug herstellen läßt.

Grundsätzlich bieten Verfahren, bei denen Gebühren im voraus entrichtet werden (Prepaid-Verfahren), bessere Voraussetzungen für die Wahrung der Anonymität als solche Systeme, bei denen zunächst Verkehrsdaten erhoben und dann den Benutzern in Rechnung gestellt bzw. von deren Konto abgebucht werden (Postpaid-Verfahren).

Soweit die Speicherung von Benutzerdaten gleichwohl erforderlich ist (z. B. für den Nachweis der Richtigkeit der Gebührenerhebung), sollten diese Daten dezentral beim Benutzer gespeichert werden. Die Erhebung von Benutzerdaten im Regelbetrieb durch "Erhebungsstellen" und deren Übermittlung an Konzentratoren oder zentrale Abrechnungseinheiten sollte unterbleiben.

Die Überwachung der Gebührenerhebung sollte so gestaltet werden, daß die Identität des Benutzers nur dann aufgedeckt wird, wenn ein begründeter Mißbrauchsverdacht besteht. Die Überwachung, ob ein Mißbrauch vorliegt, sollte grundsätzlich nur stichprobenweise und nicht vollständig erfolgen, da Systeme mit flächendeckender Mißbrauchskontrolle eine Infrastruktur voraussetzen, die für eine vollständige Erfassung auch der regelrechten Straßenbenutzung "zweckentfremdet" werden können. Dabei sollte die Kontrolldichte so gering wie möglich sein und könnte sich an der bisherigen Kontrollpraxis bezüglich der Einhaltung von Geschwindigkeitsbegrenzungen orientieren.

1.4.4.2 Vertraulichkeit

Sofern personenbezogene Daten erhoben werden, müssen sie vertraulich behandelt werden. Die unbefugte Kenntnisnahme durch Dritte ist durch technische und organisatorische Maßnahmen auszuschließen. Insbesondere ist folgendes zu gewährleisten:

- Alle Komponenten, die sicherheitsrelevante Informationen austauschen, müssen sich partnerweise gegenseitig authentifizieren.

- Die Identität eines Straßenbenutzers sollte nur bei Mißbrauchsverdacht und nur vom Systembetreiber aufgedeckt werden können.

- Daten, die Aufschluß über die Identität oder den Aufenthaltsort des Benutzers geben, sind

durch kryptographische Verfahren gegen eine unbefugte Kenntnisnahme zu sichern.

- Bei dezentraler Datenspeicherung (z. B. auf einer Chipkarte) darf der Zugang nur nach Eingabe eines benutzerspezifischen Codes möglich sein.

- Soweit personenbezogene Daten bei vermutetem Mißbrauch zentral gespeichert werden, ist zu gewährleisten, daß die Daten von anderen - vom Systembetreiber verarbeiteten - Daten strikt abgeschottet und nach Rechnungsbegleichung, bzw. wenn ein Mißbrauch nicht nachgewiesen werden kann, unverzüglich gelöscht werden.

- Die Vertraulichkeit im Verhältnis Fahrzeughalter - Fahrzeugbenutzer muß gewahrt werden (benutzer- statt fahrzeuggebundene Erhebung).

1.4.4.3 Integrität

Es ist zu gewährleisten, daß die richtigen Daten jeweils den richtigen Benutzern zugeordnet werden und keine Über-, Unter- oder Doppelerfassung erfolgt. Der Abbuchungsimpuls darf nicht derart streuen, daß er etwa - z. B. beim Spurwechsel - andere Fahrzeuge erfaßt. Auch bei der Fahrzeug- bzw. Benutzeridentifizierung (z. B. durch Kennzeichenerfassung) im Falle vermuteten Mißbrauchs ist die Zuordnung zu den richtigen Fahrzeugen sicherzustellen. Alle sicherheitsrelevanten Informationen sind mit geeigneten Verfahren gegen Manipulationen zu schützen.

1.4.4.4 Transparenz

Das gesamte Verfahren muß für die Teilnehmer durchschaubar sein, d. h. die Benutzer müssen die realistische Chance haben, sich sowohl über den generellen Ablauf als auch über die Datenerhebung und -speicherung im Einzelfall umfassend zu informieren:

- Bei dezentraler Speicherung sollte der Benutzer nachvollziehen können, welche Entgelte wann wo abgebucht wurden.

- Das System sollte den Benutzer rechtzeitig darauf hinweisen, wenn das Guthaben erschöpft oder für die Abbuchung der Maut zu gering ist.

- Sofern im Rahmen von Überwachungsmaßnahmen eine Aufdeckung der ansonsten geheimen Fahrzeugidentität erfolgt, muß dies für den Fahrzeugbenutzer erkennbar sein.

- Abbuchungen, Funktionsstörungen und Manipulationsversuche müssen dem Benutzer angezeigt werden und sind dezentral (z. B. auf der Chipkarte) revisionssicher zu protokollieren. Über Zusatzeinrichtungen, etwa bei Tankstellen, sollte der Benutzer die Möglichkeit haben, den Speicherinhalt der Protokolldatei auszudrucken und die Buchungsdaten anschließend selbst zu löschen.

1.4.4.5 Stabilität gegen die Rücknahme von Datenschutzmaßnahmen

Die Systemkomponenten sind so zu gestalten, daß die Datenschutz- und Datensicherungsfunktionen stabil sind und nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen oder unterlaufen werden können. Alle zum Einsatz kommenden Geräte müssen der Qualitätssicherungsnorm ISO 9001 genügen.

Systeme, die eine generelle Videoüberwachung des fließenden Verkehrs voraussetzen, sind aus datenschutzrechtlichen Gründen abzulehnen, weil sie sich bei nur geringen Modifikationen auf eine Vollkontrolle umstellen lassen.

1.5 Schaffung einzelgesetzlicher Datenschutzregelungen im Land Brandenburg

Lediglich mit der Verabschiedung des Landesgleichstellungsgesetzes und des Brandenburgischen Gesundheitsdienstgesetzes ist es im Berichtszeitraum gelungen, in fachspezifischen Gesetzen weitere Datenschutzregelungen zu schaffen. Die Mehrzahl selbst der Gesetze, die ich in meinem 2. Tätigkeitsbericht[14] als bereits im Entwurf vorliegend aufgeführt hatte, sind bisher nicht einmal im Parlament behandelt worden. Diese - durch die Neukonstitution des Landtages bedingte - Verzögerung der Weiterentwicklung des Datenschutzes bedauere ich; sie läßt sich aus der nachfolgenden Auflistung der Einzelgesetze nachvollziehen:

- Landesgleichstellungsgesetz (s. unter 3.1.7)
- Entwurf eines Gesetzes zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg (s. unter 3.6.3)
- Entwurf eines Brandenburgischen Statistikgesetzes (s. unter 3.9.2)
- Entwurf eines Katastrophenschutzgesetzes[15]
- Entwurf eines Gesetzes über das Versorgungswerk der Rechtsanwälte im Land Brandenburg (s. unter 4.1.1)
- Entwurf eines Brandenburgischen Psychisch-Kranken-Gesetzes (s. unter 7.3.1)
- Brandenburgisches Gesundheitsdienstgesetz (BbgGDG)

Aus den laufenden Gesprächen sowie aus der Umfrage des Ministeriums des Innern über den Ablauf der in § 41 Abs. 2 Bbg DSG genannten Frist ist mir allerdings bekannt, daß die zuständigen Ressortministerien diesen noch nicht abgeschlossenen Gesetzesvorhaben nunmehr oberste Priorität beimessen.

Darüber hinaus sind auf der Grundlage von in Gesetzen bzw. in Rechtsverordnungen enthaltenen Ermächtigungsklauseln Verordnungen oder Verwaltungsvorschriften von der Landesregierung - insbesondere wiederum im Schulbereich - erlassen worden, die hier nur mehrheitlich aufgrund ihrer Bedeutung Erwähnung finden sollen:

- Errichtungsanordnung und Dienstanweisung zum Kriminalaktennachweis (s. unter 3.5.7.3)
- Entwurf einer Verordnung zur Durchführung der Gebäude- und Wohnungszählung (s. unter 3.9.3)
- Runderlaß des Ministeriums der Justiz und des Ministeriums des Innern über die Bestimmung der nach § 11 Abs. 1 Satz 1 GWG zuständigen Stelle zur Entgegennahme von Anzeigen (s. unter 4.1.3)
- Verwaltungsvorschriften Schulakten (s. unter 5.1.1)
- Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg (s. unter 5.1.2)
- Entwurf einer Nichtschülerprüfungsverordnung (s. unter 5.1.3)
- Entwurf von Verwaltungsvorschriften über die Durchführung von Hausunterricht (s. unter 5.1.4)
- Rundschreiben: Übergang aus der Jahrgangsstufe 6 der Primarstufe in die Jahrgangsstufe 7 einer Schule der Sekundarstufe 1 (§ 11 AO-GS vom 21. Juni 1991) - Stand: 05.12.1994 sowie zum Entwurf der "Verordnung zur Änderung der Ausbildungsordnung der Grundschule im Land Brandenburg" - Stand: 02.12.1994 (s. unter 5.1.5)
- Entwurf einer Verordnung für Hebammen und Entbindungspfleger im Land Brandenburg (s. unter 7.2.1.1)

---

[14]

[15] s. unter 1.3, S. 18 ff.

s. 2. Tätigkeitsbericht unter 3.10, S. 81

- Verwaltungsabkommen zum Krebsregister (s. unter 7.2.1.2)
- Entwurf einer Krankenhausdatenschutzverordnung (s. unter 7.3.2)

Eine grundsätzliche datenschutzrechtliche Bewertung zu dieser Vorgehensweise der Verwaltung habe ich bereits in meinem 2. Tätigkeitsbericht[16] vorgenommen. Immerhin hat es sich der Landtagsausschuß für Arbeit, Soziales, Gesundheit und Frauen vorbehalten, die Krankenhausdatenschutzverordnung (s. unter 7.3.2) vor Inkrafttreten zu beraten. Dieses Beispiel sollte Schule machen.

2 Brandenburgisches Datenschutzgesetz

2.1 Novellierung des Brandenburgischen Datenschutzgesetzes

Nach Maßgabe der Ausführungen des Bundesverfassungsgerichts im sog. Volkszählungsurteil[17] setzt die Verarbeitung personenbezogener Daten durch die Verwaltung im Vollzug gesetzlich bestimmter Aufgaben voraus, daß der Gesetzgeber den Verwendungszweck bereichspezifisch so normenklar und präzise bestimmt, daß für den Bürger erkennbar ist, welche Stelle zu welchem Zweck welche Angaben über ihn verarbeitet. Dementsprechend hat sich der Landesgesetzgeber mit den §§ 23 Abs. 2 Satz 2 und 41 Abs. 2 Bbg DSG den Erlaß der notwendigen bereichsspezifischen Regelungen zur Datenverarbeitung auch selbst zur Aufgabe gemacht und in § 41 Abs. 2 Bbg DSG vorgesehen, daß die zur Erfüllung der gesetzlichen Aufgaben der Verwaltung erforderlichen personenbezogenen Daten nur für eine Übergangszeit auf der Grundlage des allgemeinen Datenschutzgesetzes erfolgen darf.

Eine Umfrage des Ministeriums des Innern (MI) bei den einzelnen Ressorts hat jedoch ergeben, daß die Landesregierung bezüglich ihrer Verpflichtung zu entsprechenden Gesetzesvorlagen über Vorbereitungen noch nicht hinausgekommen ist. Dies muß angesichts der Fülle der Aufgaben und der vielfältigen Probleme, die mit einem Neuaufbau von Gesetzgebung und Verwaltung verbunden und nicht immer vorherzusehen sind, auch aus datenschutzrechtlicher Sicht auf Verständnis stoßen. Im Grundsatz halte ich deshalb das Vorhaben der Landesregierung für berechtigt, dem Landtag vorzuschlagen, die Frist des § 41 Abs. 2 Bbg DSG zu verlängern. Dies würde - für den Fall, daß sich die Bürger in Berlin und Brandenburg für eine Fusion ihrer beiden Länder entscheiden sollten - auch eine Doppel-Belastung der Gesetzgebung vermeiden und es ermöglichen, einem etwaigen fusionsbedingten Bedarf an Rechtsangleichung bereits in den Gesetzesvorlagen Rechnung zu tragen. Insbesondere für die Materie "Datenschutz" ist dies in Artikel 52 Abs. 1 Nr. 3 des Staatsvertrages der Länder Berlin und Brandenburg über die Bildung eines gemeinsamen Bundeslandes vom 27. April 1995 auch ausdrücklich als vorrangig vorgesehen.

Allerdings bin ich der Auffassung, daß eine Verlängerung der Frist des § 41 Abs. 2 Bbg DSG so bemessen sein muß, daß sie die Frage der bereichsspezifischen Regelungen der Datenverarbeitung nicht aufhebt, sondern lediglich bis spätestens Ende 1997 zurückstellt. Desweiteren sollte sie mit der ausdrücklichen Verpflichtung der Landesregierung verbunden sein, in jeder neuen Gesetzesvorlage - einschließlich solcher, mit denen bestehende Gesetze geändert werden sollen - Stellung zu der mit dem Vollzug des Gesetzes verbundenen Verarbeitung personenbezogener Daten zu nehmen und ggf. eine entsprechende bereichsspezifische Regelung in die Vorlage mit einzustellen.

16

17 s. unter 1.3, S. 18 ff.
BVerfGE 65,1 (46)

Das MI hat mir zugesagt, diesen Vorschlag aufgeschlossen zu prüfen. Ferner konnte mit ihm Einvernehmen darüber erzielt werden, daß mit dem wegen § 41 Abs. 2 Bbg DSG erforderlichen Änderungsgesetz zugleich auch das Bbg DSG redaktionell und inhaltlich "nachgebessert" wird. Änderungen, die grundsätzliche Fragen aufwerfen und einen entsprechenden Diskussionsbedarf auslösen würden, sollten dabei allerdings im Hinblick auf die für das Gesetzesvorhaben nur noch zur Verfügung stehende Zeit und die noch offene Entscheidung über die Bildung eines gemeinsamen Landes Berlin-Brandenburg ebenfalls vorläufig zurückgestellt werden. Ein Bedarf an ergänzenden bzw. neuen Regelungen wird übereinstimmend - insbesondere zur Datenverarbeitung im Auftrag und zum Dateienregister - gesehen. Die Konkretisierung der bisherigen Vorstellungen zu den angedachten Änderungen des Gesetzes wird derzeit vom Ministerium mit mir abgestimmt; dem Ergebnis der Gespräche soll hier nicht vorgegriffen werden. Gleichwohl halte ich weiterhin u. a. auch Regelungen zur Stellung eines behördlichen Datenschutzbeauftragten für erforderlich[18].

2.2 Vorläufige Verwaltungsvorschriften zum Brandenburgischen Datenschutzgesetz

Zu begrüßen war, daß das MI Anfang des Jahres Vorläufige Verwaltungsvorschriften zur Durchführung des Brandenburgischen Datenschutzgesetzes[19] erlassen hat, die insbesondere den Kommunalverwaltungen hilfreiche Erläuterungen zu den Bestimmungen über die technisch-organisatorischen Maßnahmen zum Datenschutz (§§ 7, 8, 10 und 24 Bbg DSG) an die Hand geben. Im wesentlichen offen gelassen hat das Ministerium in den Vorschriften die zum behördlichen Datenschutzbeauftragten bestehenden Fragen, für die derzeit im Zusammenhang mit der Novellierung des Brandenburgischen Datenschutzgesetzes (s. unter 2.1) nach sachgerechten Lösungen durch geeignete gesetzliche Vorgaben gesucht wird.

3 Inneres

3.1 Personaldatenverarbeitung

3.1.1 Personalaktenführung

Erhebliche Defizite bestehen noch immer bei der Führung von Personalakten in den Verwaltungen. Erste Prüfungen, die ich am Anfang des Berichtszeitraums vorgenommen hatte, habe ich alsbald wieder einstellen müssen, da die erforderlichen extensiven und oftmals über den Bereich der Anwendung datenschutzrechtlich relevanter Vorschriften hinausgehenden Beratungen von meiner Dienststelle schon allein zeitlich nicht geleistet werden konnten. Bloße Beanstandungen festzustellender Mängel schienen mir im Hinblick auf den Stand des Verwaltungsaufbaus und der Vermittlung des zur sachgerechten Aufgabenerfüllung erforderlichen Fachwissens unangebracht. Ich habe deshalb beim Ministerium des Innern (MI) dringlich Regelungen zur Personalaktenführung angemahnt. Obgleich diese - soweit sie nicht nur zur Ausführung des Landesbeamtengesetzes (LBG)[20] ergehen (vgl. § 156 LBG), sondern unbeschadet der Tarifautonomie in entsprechender Anwendung auch die Führung von Personalakten der Angestellten betreffen - unmittelbar nur

---

[18] s. 1. Tätigkeitsbericht unter 6.6, S. 42, 2. Tätigkeitsbericht unter 1.2.2, S. 18 f.

[19] vom 24. Januar 1995, ABl. S. 134

[20] vom 24. Dezember 1994, GVBl. I S. 506, geänd. durch Gesetz vom 15. Oktober 1993, GVBl. I S. 398

im Bereich der Landesverwaltung gelten können, würden sie doch auch den Kommunalverwaltungen eine geeignete Orientierung bieten. Ausführungsvorschriften und Erläuterungen zu den gesetzlichen Bestimmungen über die Personaldatenverarbeitung müssen im Rahmen ordnungsgemäßer Aufgabenerfüllung durch die Verwaltung selbst erfolgen und können nicht vom Landesbeauftragten für den Datenschutz durch einseitige Gestaltungsvorschläge in ein Regelungsvakuum hinein vorwegbestimmt werden. Mir ist daran gelegen, daß das MI nunmehr selbst die Initiative ergreift, so daß sich für mich die Möglichkeit einer der verfassungsrechtlichen und gesetzlichen Aufgabenzuweisung entsprechenden Beteiligung nach Maßgabe von §§ 23 Abs. 2, 7 Abs. 2 Bbg DSG ergibt.

An Regelungen zur Personalaktenführung sind mir aus dem Bereich der Landesregierung bislang lediglich ein Rundschreiben des Ministeriums für Bildung, Jugend und Sport[21] sowie ein Rundschreiben des Ministeriums für Wissenschaft, Forschung und Kultur[22] bekannt. Während letzteres auch im Januar 1994 noch das bereits im Dezember 1992 in Kraft getretene Landesbeamtengesetz unberücksichtigt läßt und ich entgegen § 7 Abs. 2 Bbg DSG hierzu nicht gehört wurde, gibt es zu ersterem nur in einer noch abschließend zu klärenden Detailfrage eine Meinungsverschiedenheit zwischen dem Ministerium und mir. Im übrigen hat sich mir das Rundschreiben als eine ausgesprochen bedarfsgerechte und aus datenschutzrechtlicher Sicht inhaltlich zutreffende Regelung dargestellt.

Das MI hat den Bedarf an erläuternden Ausführungsbestimmungen zur Personaldatenverarbeitung nicht in Abrede gestellt, jedoch um Verständnis dafür gebeten, daß es nicht alle wichtigen Aufgaben gleichzeitig erfüllen könne. Dem konnte ich mich in der Vergangenheit nicht verschließen; ich meine jedoch, daß es nunmehr möglich sein sollte, zügig eine Regelung zu finden, die noch in diesem Jahr in Kraft treten kann.

3.1.2 Personalinformationssysteme

Während über die Auswahl eines geeigneten Informationssystems für die Personalverwaltungen in den Geschäftsbereichen der Ministerien noch in einer interministeriellen Arbeitsgruppe unter Federführung des Innenministeriums beraten wird, hat das Ministerium für Bildung, Jugend und Sport für die Stellen- und Personalverwaltung bei den staatlichen Schulämtern bereits ein automatisiertes Datenverarbeitungsverfahren (Lehrerstellen- und Personalverwaltung - LSPV) eingeführt, daß nach einer längeren Erprobungsphase zur Zeit wegen des Umfangs der erforderlich gewordenen Weiterentwicklungen völlig neu programmiert wird. Zu kritisieren war bislang insbesondere, daß ich über das Vorhaben entgegen § 23 Abs. 2 Satz 3 Bbg DSG nicht so rechtzeitig informiert worden war, daß es dem Ministerium möglich gewesen wäre, meine Hinweise auf datenschutzrechtliche Mängel noch vor der Einführung des Systems zu berücksichtigen. Eine ins einzelne gehende Bewertung des Vorhabens, das keinen grundsätzlichen datenschutzrechtlichen Bedenken begegnet, stelle ich hier im Hinblick auf die mir angekündigte völlige Neuprogrammierung des Systems zurück. Ich gehe nach Maßgabe entsprechender Aussagen des Ministeriums davon aus, daß dabei auch meine bisherigen datenschutzrechtlichen Verbesserungsvorschläge zum LSPV und den seine Einführung anordnenden und regelnden Dienstanweisungen angemessen umgesetzt werden. Aktuelle Informationen zum gegenwärtigen Sach- und Verfahrensstand liegen mir leider nicht vor.

3.1.3 Noch einmal: Übergabe von Personalakten nach Übergang der Trägerschaft

In ihrer Stellungnahme zu meinem 2. Tätigkeitsbericht, in dem ich mich zu dieser Frage

---

[21] vom 8. November 1993 Nr. 110/93 i. d. Fassung d. Rschr. 83/94 vom 21. November 1994

[22] vom 10. Januar 1994

näher geäußert hatte[23], hat die Landesregierung ausgeführt[24], sie teile die von mir dort zu § 29 Abs. 1 Satz 3 Bbg DSG vertretene Auffassung nicht, daß der Begriff des künftigen Arbeitgebers auf die Begründung eines neuen Arbeitsverhältnisses abstelle und deshalb auf den Fall des Trägerwechsels bei fortbestehendem Arbeitsverhältnis keine Anwendung finde. Nachdem ich meine Auffassung gegenüber dem MI noch einmal im einzelnen ausführlich begründet habe, hat mir dieses jedoch zwischenzeitlich mitgeteilt, die Stellungnahme der Landesregierung beruhe insoweit auf einem Mißverständnis und die von mir vertretene Auffassung werde geteilt.

3.1.4 Weitergabe von Ermittlungsergebnissen an die Personalstelle des Polizeipräsidiums

Bei Ermittlungen gegen ein Unternehmen hatte sich ergeben, daß auch ein Beschäftigter des ermittelnden Polizeipräsidiums für die Gesellschaft tätig war. Dies teilten die Ermittlungsbeamten der Personalstelle des Polizeipräsidiums mit, die daraufhin dienstrechtliche Maßnahmen gegen den betroffenen Mitarbeiter veranlaßte. Nachdem das Polizeipräsidium die Datenweitergabe innerhalb des Präsidiums zunächst auf die Mitteilungen in Strafsachen (MiStra)[25] auf Bestimmungen des öffentlichen Dienstrechts sowie des allgemeinen Brandenburgischen Datenschutzgesetzes gestützt hatte, habe ich sie beanstandet, da die behaupteten rechtlichen Voraussetzungen nicht vorlagen. Fraglich war bereits im Hinblick auf § 3 Abs. 3 Satz 2 Bbg DSG, ob das Brandenburgische Datenschutzgesetz überhaupt Anwendung finden konnte, da die Weitergabe von Ermittlungsergebnissen grundsätzlich abschließend in den MiStra geregelt sind. Als bloße Verwaltungsvorschriften genügen diese zwar nicht den rechtsstaatlichen Anforderungen; die Rechtsprechung hält die Übergangsfrist für den Erlaß eines Justizmitteilungsgesetzes jedoch noch immer nicht für abgelaufen[26]. Nach Nr. 29 Abs. 2 MiStra hätte die Information der Personalstelle nur vom Richter oder Staatsanwalt angeordnet werden können. Die Voraussetzungen für eine Datenweitergabe nach § 14 Abs. 5 i. V. m. §§ 14 Abs. 1, 13 Abs. 2 Satz 1 Buchst. a) Bbg DSG lagen für sich genommen ebenfalls nicht vor, und auch auf die beamtenrechtlichen Aufgabenbestimmungen ließ sich die Datenweitergabe nicht stützen.

Das Polizeipräsidium war in seiner Stellungnahme zu Unrecht davon ausgegangen, daß sich die Rechtslage bei der Frage, ob die Erkenntnisse aus den polizeilichen Ermittlungen an die Personalstelle des Präsidiums weitergegeben werden durften, für diese grundsätzlich anders darstelle als für die Personalstellen anderer Verwaltungen. Weder die datenschutzrechtlichen Bestimmungen einschließlich der MiStra, noch die beamtenrechtlichen unterscheiden jedoch zwischen Polizeibeamten und sonstigen Beamten.

In inhaltlicher Auswertung der vom Polizeipräsidium vorgetragenen Gesichtspunkte kam es deshalb allenfalls in Betracht, die Maßnahme auf die Bestimmungen der Gefahrenabwehr des allgemeinen Polizeirechts (§ 43 Abs. 3 Nr. 3 Polizeigesetz (PolG) i. V. m. § 1 Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg (VGPolGBbg))[27] zu stützen. Nachdem ich das MI darauf hingewiesen hatte, hat es mir zwischenzeitlich nachvollziehbar begründet, daß die Voraussetzungen dieser Rechtsgrundlage im konkreten Fall vorlagen. Im Ergebnis war die Datenweitergabe deshalb als rechtmäßig zu beurteilen.

23

24 s. unter 3.2.1, S. 42 f.

25 LT-Drs. 2/169

26 vom 15. März 1985, BAnz. Nr. 60

27 vgl. OLG Frankfurt a. M, Beschl. v. 19. Mai 1994 - 3 VAs 31/93 - = NJW 1995, Heft 16 S. 1102 m. w. N.

vom 11. Dezember 1991, GVBl. S. 636

3.1.5 Vermerk über Telefonwahlverbindungen in der Personalakte

Bei einer öffentlichen Stelle im Geschäftsbereich des Ministeriums der Finanzen (MdF) war zur Fehlersuche im Rahmen der technischen Wartung der dortigen ISDN-Telefonanlage durch einen privaten Auftragnehmer der Ausdruck sämtlicher gespeicherter Verbindungsdaten zu Dienst- und Privatgesprächen erfolgt. Die Ausdrucke wurden anschließend auch inhaltlich ausgewertet; dabei entstand ein später nicht bestätigter Verdacht, daß von einem Mitarbeiter Privatgespräche nicht ordnungsgemäß abgerechnet worden waren. Auf einem Schreiben des Mitarbeiters an die Personalstelle wurde im weiteren Verlauf der Angelegenheit seitens der Dienststelle das Ergebnis der Auswertung unter namentlicher Nennung eines der Gesprächspartner des Mitarbeiters vermerkt. Das Schreiben wurde anschließend zur Personalakte genommen.

Problematisch war zunächst schon die Erstellung der vollständigen Ausdrucke, die nach Maßgabe von § 29 Abs. 1 Bbg DSG i. V. m. Ziffer 3.1.3 der Dienstanschlußvorschriften (DAV)[28] zu beurteilen war. Bei einem Ziff. 3.1.3 Abs. 2 DAV i. V. m. § 5 Abs. 2 der Dienstvereinbarung über die Nutzung der ISDN-Telekommunikationsanlagen des Telekommunikationsverbundes der obersten Landesbehörden des Landes Brandenburg (Musterdienstvereinbarung) entsprechenden Verfahren[29] hätten die gem. Absatz 1 der Bestimmung erfaßten Daten unmittelbar nach Beendigung des Gesprächs automatisch gelöscht werden müssen. Lediglich die Verbindungsdaten zu Dienstgesprächen hätten entsprechend § 7 Abs. 1 der Musterdienstvereinbarung im Umfang von in der Regel monatlich zehn Stichproben überhaupt gespeichert sein dürfen, soweit nicht vom einzelnen Beschäftigten gem. § 6 Abs. 3 der Musterdienstvereinbarung die Speicherung der Verbindungsdaten zu Privatgesprächen ausdrücklich gewünscht worden war. Das MdF geht selbst davon aus, daß auch in dem vorliegenden Fall nicht nur die Auswertung, sondern bereits die Fertigung des Ausdrucks zur technischen Fehlersuche bezüglich der Privatgespräche generell nur mit Einwilligung der Mitarbeiter hätte erfolgen dürfen. Erstellung und Auswertung von Datenausdrucken haben sich in einem solchen Fall jedoch strikt auf den technischen Zweck zu beschränken. Anschließend müssen diese Ausdrucke unverzüglich vernichtet werden.

Der handschriftliche Vermerk auf dem Schreiben des Mitarbeiters hätte bei vorschriftsmäßiger Verfahrensweise bereits gar nicht erstellt werden können und im übrigen schon deswegen nicht zur Personalakte genommen werden dürfen, weil es sich bei ihm zum einen materiell nicht um Personalaktendaten im Sinne von § 57 Abs. 1 Landesbeamtengesetz (LBG)[30] handelte und er zum anderen Angaben auch über einen Dritten enthielt.

Noch ehe ich das Ministerium um Stellungnahme zu der zeitgleich bei mir eingegangenen entsprechenden Eingabe bitten konnte, erhielt ich von diesem bereits eine Durchschrift seiner Antwort an den Petenten, in der ihm die Sach- und Rechtslage ausführlich erläutert, die festgestellten Verstöße gegen die Vorschriften über den Datenschutz eingeräumt und die Maßnahmen, die zur Behebung der Mängel ergriffen worden waren, mitgeteilt wurden. Zu der Eingabe selbst waren deshalb von mir keinerlei weitere Maßnahmen mehr zu veranlassen. Allerdings wird noch die Umsetzung der erforderlichen Maßnahmen bezüglich der Telekommunikationsanlage zu prüfen sein.

---

[28] vom 30. November 1993, ABl. S. 1775

[29] s. hierzu auch unter 11.6 sowie 2. Tätigkeitsbericht unter 11.1, S. 143 ff.

[30] vom 24. Dezember 1992, GVBl. I S. 506, geänd. durch Gesetz vom 15. Oktober 1993, GVBl. I S. 398

Der Vorgang beleuchtet im übrigen beispielhaft die unter 3.3 erneut angesprochene Problematik der Datenverarbeitung im Auftrag[31] und unterstreicht den diesbezüglichen Regelungs- und Handlungsbedarf. Es ergibt sich nämlich, daß hier sämtliche im Verhältnis zum Dienstherrn selbst durch besondere Regelungen eigens geschützte Daten durch dessen privaten Auftragnehmer im Rahmen von Wartungsarbeiten letztlich unkontrollierbar zur Kenntnis genommen werden können und diesem also entgegen den gesetzlichen Beschränkungen im Rahmen der Auftragsdurchführung ggf. uneingeschränkt offenbart werden.

3.1.6 Gefährdung des Adoptionsgeheimnisses bei Überprüfung des Kindergeldanspruchs

Mit Hilfe eines vom Bundesministerium für Familie, Senioren, Frauen und Jugend bundeseinheitlich vorgegebenen Formulars hatte die Zentrale Bezügestelle des Landes Brandenburg (ZBB) nach Maßgabe von Art. 5 des Ersten Gesetzes zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms (1. SKWPG)[32] in einer einmaligen Aktion sämtliche Kindergeldzahlungen zu überprüfen. Dabei sah das Formular bezüglich der Angaben auch vor, daß Auskunft darüber zu erteilen war, ob es sich um ein leibliches oder um ein Adoptivkind handele. Darin habe ich in Übereinstimmung mit den Datenschutzbeauftragten der übrigen Länder einen Verstoß gegen das Verbot gesehen, ohne besondere im öffentlichen Interesse liegende Gründe, Tatsachen auszuforschen, die geeignet sind, die Annahme als Kind und ihre Umstände aufzudecken (§ 1758 Abs. 1 BGB). Das Bundesministerium hat daraufhin festgestellt, die Differenzierung zwischen leiblichen und Adoptivkindern sei kindergeldrechtlich unerheblich und datenschutzrechtlich unzulässig, und angewiesen, daß deshalb gleichwohl erfolgte Angaben - soweit durch sie eine Adoption erstmalig offengelegt wurde - spätestens bei der nächsten Fallbearbeitung zu löschen sind. Dies war mir seitens der ZBB bereits zuvor zugesagt worden.

Eine weitere Gefährdung des Adoptionsgeheimnisses ergab sich daraus, daß sich die ZBB zur Vermeidung von Doppelzahlungen davon überzeugen muß, daß nicht bereits eine andere Person aus dem Kreis der nach §§ 1 bis 3 Bundeskindergeldgesetz (BKGG)[33] Anspruchsberechtigten Leistungen erhält. Wird für ein nicht neugeborenes Kind Kindergeld beantragt, so tauscht sie dazu ggf. mit anderen Kindergeldstellen Vergleichsmitteilungen aus. Ergibt sich aus diesen nicht, daß der Antragsteller für das betreffende Kind bereits früher Leistungen nach dem Bundeskindergeldgesetz bezogen hat, stellt sich die Frage, weshalb er seinen Anspruch nicht schon eher geltend gemacht hat. Dies kann der Antragsteller ggf. nur dadurch nachvollziehbar erklären, daß er die Annahme des Kindes aufdeckt. Das Bundesministerium hat zwar darauf hingewiesen, daß es zu einer solchen erstmaligen Offenlegung der Adoption nur ausnahmsweise dann kommen kann, wenn die Annahme der Kindergeldstelle nicht bereits durch eine im Regelfall vorangehende Adoptionspflege bekannt ist. Dennoch hat es zur bestmöglichen Wahrung des Datenschutzes angewiesen, daß nur das Ergebnis der in Rede stehenden Nachforschungen in der Akte zu vermerken ist und die Nachweise, soweit es sich nicht um Originale des Antragstellers handelt, nach der Prüfung zu vernichten sind.

31

32 s. 2. Tätigkeitsbericht unter 1.2.1, S. 9 ff.

33 vom 21. Dezember 1993, BGBl. I S. 2353
i. d. Fassung d. Bek. v. 31. Januar 1994, BGBl. I S. 168

3.1.7 Weitreichende Rechte der Gleichstellungsbeauftragten

Im Berichtszeitraum hat der Landtag das Landesgleichstellungsgesetz (LGG)[34] verabschiedet. Das Gesetz berücksichtigt die von mir in meinem 2. Tätigkeitsbericht[35] dargestellten Gesichtspunkte. Es ermöglicht es der Gleichstellungsbeauftragten insbesondere, auch ohne Zustimmung der Betroffenen die für eine sachgerechte Erfüllung ihrer Aufgaben erforderlichen Personaldaten zu verarbeiten (§ 22 Abs. 1 Satz 2, Abs. 4 LGG). Für die Einhaltung der Vorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten durch die Gleichstellungsbeauftragte ist diese - unbeschadet der Verpflichtungen ihrer Dienststelle - in erster Linie selbst verantwortlich (§ 22 Abs. 8 LGG). Als bereichsspezifische Regelung der Befugnisse der Gleichstellungsbeauftragten zur Verarbeitung personenbezogener Daten entspricht § 22 LGG den Anforderungen, die das Bundesverfassungsgericht dafür im sog. Volkszählungsurteil[36] aufgestellt hat.

Im übrigen ist zu beachten, daß erst wenn und soweit die Kommunen die entsprechenden Regelungen des LGG in ihre Hauptsatzungen übernehmen, die in § 22 LGG bestimmten Befugnisse der Gleichstellungsbeauftragten zur Verarbeitung von Personaldaten auch ohne Einwilligung der Betroffenen gelten.

3.2 Meldewesen

3.2.1 Umsetzung des Brandenburgischen Meldegesetzes

3.2.1.1 Weitere Verwendung von Daten der ehemaligen Volkspolizeikreisämter

Noch immer nicht befriedigend gelöst ist die Problematik der Altdaten im Meldebereich[37]. Meine Umfrage bei den Meldebehörden Ende Juni 1994 ergab, daß dort mit der Umsetzung des Rundschreibens des MI zur weiteren Verwendung von Daten der ehemaligen Volkspolizeikreisämter (VPKA) Bereich Meldewesen[38] noch nicht einmal begonnen worden war, obgleich die nach dem Rundschreiben vorgesehene Vernichtung der Datenbestände möglichst bis zum 30. Juni 1994 zu realisieren war. In ihrer Stellungnahme zu meinem 2. Tätigkeitsbericht[39] hat die Landesregierung mitgeteilt, daß die Vernichtung noch immer nicht abgeschlossen sei. Der gegenwärtige Stand des Vollzugs ist mir nicht bekannt.

Probleme ergaben sich insbesondere daraus, daß sich die Datenbestände überwiegend noch bei den Kreisen befanden und vor der Vernichtung zunächst von den zuständigen Meldebehörden übernommen werden sollten. Die Aufteilung der Dateien nach einzelnen Ämtern führt jedoch zu erheblichen praktischen Schwierigkeiten. Die Unterlagen sollten daher bei den Landkreisen verbleiben und dort vernichtet werden.

Ferner wurde vielfach deshalb von einer Vernichtung der Unterlagen Abstand genommen, weil die Meldebehörden der Auffassung waren, daß sie sich für die Betroffenen zu

---

34

35 vom 4. Juli 1994, GVBl. I S. 254

36 s. dort S. 100 ff

37 vom 15. Dezember 1983, BVerfGE 65, 1 (46)

38 s. 2. Tätigkeitsbericht unter 3.1.3, S. 38

39 vom 9. Dezember 1993, ABl. 1750
LT-Drs. 2/169 S. 6

Nachweiszwecken in Verfahren nach dem Zweiten SED-Unrechtsbereinigungsgesetz[40] und dem Vertriebenenzuwendungsgesetz[41] eignen könnten. Obwohl ich es grundsätzlich nicht für richtig halten kann, daß derartige Gesichtspunkte entgegen den Anweisungen der Fach- und Kommunalaufsicht Berücksichtigung finden, will ich gleichwohl nicht ausschließen, daß sie möglicherweise Veranlassung geben könnten, die nach dem Rundschreiben für die Vernichtung vorgesehene Frist noch einmal zu überprüfen. Seitens des Innenministeriums sind die Bedenken der Meldebehörden jedoch bislang nicht aufgegriffen worden, so daß ich davon ausgehen muß, daß sie auch dort im Ergebnis nicht für begründet gehalten werden. Deshalb meine ich, daß die Umsetzung des Rundschreibens nunmehr - ein Jahr nach Ablauf der dazu gesetzten Frist - zügig abgeschlossen werden muß.

3.2.1.2 Kreismeldekarteien

Ähnlich stellt sich die Problematik bezüglich der alten Kreismeldekarteien dar, die rechtlich betrachtet zwar Bestandteil des Melderegisters sind, jedoch eine Vielzahl von Angaben enthalten, deren weitere Speicherung melderechtlich unzulässig ist, und die deshalb in den Melderegistern gem. § 38 Abs. 3 Brandenburgisches Meldegesetz (BbgMeldeG)[42] bereits bis zum 31. Dezember 1993 zu löschen waren. Auch sonst hat die Meldebehörde gem. § 11 Abs. 1 BbgMeldeG gespeicherte Daten zu löschen, wenn sie zur Erfüllung der den Meldebehörden obliegenden Aufgaben nicht mehr erforderlich sind oder ihre Speicherung unzulässig war. Karteien, die von den Meldebehörden auf Grund der Einführung der automatisierten Datenverarbeitung nicht mehr zur Erfüllung ihrer Aufgaben benötigt werden, sind jedoch gem. § 38 Abs. 4 Satz 1 BbgMeldeG abzuschließen und zu archivieren. Dabei sind dann einerseits die Löschungsverpflichtungen, andererseits aber auch die Archivierungsfristen des § 11 BbgMeldeG zu beachten. Dies führt dazu, daß die Meldebehörden eigentlich aus allen Karteikarten die Personenkennzahl der ehemaligen DDR sowie etwaige andere vermerkte Angaben wie z. B. über eine Republikflucht des Betroffenen oder seiner Verwandten herausschneiden müßten; eine Verfahrensweise, die mit einem Aufwand verbunden wäre, von dem geprüft werden sollte, ob sie noch im Verhältnis zum angestrebten Zweck steht. Zu überlegen wäre, ob nicht für die Vernichtung der Kreismeldekarteien besondere, gegenüber der 50jährigen Archivierungsfrist des § 11 Abs. 4 BbgMeldeG deutlich reduzierte Fristen gesetzt und die abgeschlossenen und gesperrten (vgl. § 19 Abs. 3 Bbg DSG) Karteien dann bis zur Vernichtung unverändert archiviert werden können. Auf jeden Fall ist es erforderlich, den Meldebehörden eindeutig und verpflichtend ein derart praktikables und datenschutzgerechtes Verfahren vorzuschreiben, daß die Einhaltung solcher Vorschriften über den Datenschutz von mir auch gem. § 23 Abs. 1 Bbg DSG sinnvoll kontrolliert werden kann. Dies ist zur Zeit nicht der Fall.

3.2.1.3 Melderegisterauskünfte und regelmäßige Datenübermittlungen

Bei der Bearbeitung der Anfragen und Eingaben im Bereich des Meldewesen hatte es zunächst Verständigungsschwierigkeiten mit dem MI gegeben, die inzwischen erfreulicherweise jedoch ausgeräumt werden konnten. Das Ministerium ist der Ansicht, es sei auch meinerseits darauf hinzuwirken, daß sich die Kommunalverwaltungen die benötigten Auskünfte zur Anwendung melderechtlicher Bestimmungen auf dem Dienstweg einholen. Dies scheint auch mir grundsätzlich sachgerecht zu sein, zumal es insoweit inhaltlich abweichende Auffassungen zwischen dem Ministerium und mir in der Regel nicht gibt und die Möglichkeiten der Fach- und Kommunalaufsicht zur breiteren Vermittlung des melderechtlichen Fachwissens den Möglichkeiten meines Amtes deutlich überlegen sind.

40

41 vom 23. Juni 1994, BGBl. I S. 1311

42 vom 27.September 1994, BGBl. I S. 2624

vom 25. Juni 1992, GVBl. I. S. 236

Unsicherheiten der Meldebehörden bei der Erteilung von Auskünften aus dem Melderegister z. B. an private Inkasso-Unternehmen, Versandhäuser u. ä. sowie bei meist regelmäßigen Datenübermittlungen z. B. an entsorgungspflichtige Körperschaften und ihre Beauftragten sowie insbesondere an die ehrenamtlichen Bürgermeister der amtsangehörigen Gemeinden haben zu zahlreichen Anfragen geführt.

Das zuletzt genannte Problem beschränkt sich keinesfalls nur auf die Übermittlung von Meldedaten. Die ehrenamtlichen Bürgermeister wollten nicht nur "informationshalber" vom Meldeamt die Übermittlung der Angaben zu Name, Geburtstag, Anschrift, Umzug u. ä. von sämtlichen Einwohnern ihrer Gemeinde. Vielmehr wurden die Ämter u. a. auch dazu aufgefordert, ihnen eine Aufstellung der Namen von Steuerschuldnern (z. B. der Zweitwohnungs- und der Hundesteuer), der Steuereinnahmen von einzelnen Betrieben sowie derjenigen Eltern, die mit ihren Kitabeiträgen im Rückstand waren, zur Verfügung zu stellen. Das Interesse der ehrenamtlichen Bürgermeister an den Datenübermittlungen begründete sich in allen Fällen mit der Auffassung, die den Ämtern durch Gesetz zugewiesenen Aufgaben besser erfüllen zu können als diese selbst. Ohne die Berechtigung dieser Auffassung näher beurteilen zu wollen, ist jedoch nachdrücklich darauf hinzuweisen, daß sich ihr der Gesetzgeber bei der Funktionalreform jedenfalls nicht angeschlossen hat.

Bislang habe ich leider noch nicht einmal die Fälle weiterverfolgen können, in denen ich die Ämter dazu veranlassen konnte, ihre Anfrage auch schriftlich an mich zu richten. Ich bezweifle jedoch auch, daß sich das Problem mit den Möglichkeiten meines Amtes wird lösen lassen. Vielmehr werden auch hier entschiedene Maßnahmen der Kommunalaufsicht erforderlich sein, mit denen den Kommunalverwaltungen die gesetzlichen Aufgabenzuweisungen und Datenverarbeitungsbefugnisse verdeutlicht und die Einhaltung des geltenden Rechts durchgesetzt werden muß. Hierzu und zu anderen melderechtlichen Fragen finden seit Anfang des Jahres Gespräche zwischen dem MI und meiner Behörde statt.

3.2.2 Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden

Mit der Zweiten Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (2. MeldDÜÄV)[43] sollte in erster Linie der in meinem 2. Tätigkeitsbericht[44] dargestellten Problematik der Mitteilungen über Geburten an den Kinder- und Jugendgesundheitsdienst Rechnung getragen werden. Gem. Art. 1 Ziff. 1 2. MeldDÜÄV dürfen die Meldebehörden den Gesundheitsämtern nunmehr zur Erfüllung der Betreuungsaufgaben des Kinder- und Jugendgesundheitsdienstes wöchentlich aus Anlaß der Geburt Familienname, Vornamen und Geburtsdatum des Neugeborenen sowie Familienname, Vornamen, Geburtsdatum und Anschrift seiner Mutter übermitteln. Obgleich ich bezweifle, daß eine wöchentliche Meldung den angestrebten Zweck erfüllen wird, habe ich die mit ihm verbundene Datenverarbeitung im Ergebnis doch als einen noch vertretbaren Ausgleich des Interesses an einer zweckentsprechenden Erfüllung der Aufgaben des Kinder- und Jugendgesundheitsdienstes einerseits und den vom Schutzbereich des Grundrechts auf informationelle Selbstbestimmung erfaßten Belangen der Betroffenen andererseits beurteilt. Im übrigen beabsichtigt das MI, die erforderliche Zweckbindungs- und Löschungsverpflichtung der Empfänger in der bereits im Entwurf vorliegenden 3. MeldDÜÄV nachzuholen.

3.3 Datenverarbeitung im Auftrag

43

44 vom 13. Februar 1995, GVBl. II S. 239

s. unter 7.2.2.3, S. 106 f.

Eine Umfrage zur Datenverarbeitung im Auftrag bei den öffentlichen Stellen im Land Brandenburg, die ich bislang nur für den Bereich der Kommunalverwaltungen auswerten konnte, hat nicht nur große Schwankungen im zur Beantwortung erforderlichen Fachwissen offenbart, sondern auch einen sehr unterschiedlichen Stand des Verwaltungsaufbaus ergeben. Während einige Landkreise einen vollständigen Rücklauf auch von den ihrer Aufsicht unterliegenden Verwaltungen sicherstellen konnten, ist dies anderen nur mehr oder weniger lückenhaft gelungen. Die Landkreise Barnim, Havelland, Oberspreewald-Lausitz und Teltow-Fläming haben mir trotz meiner eindringlichen und unter Hinweis auf die entsprechenden gesetzlichen Verpflichtungen begründeten Bitte die erforderliche Amtshilfe verweigert und die Umfrage offensichtlich noch nicht einmal an die kreisangehörigen Verwaltungen weitergeleitet. Der Landkreis Barnim hat zudem auch selbst die Umfrage nicht beantwortet.

Ungeachtet dessen hat die Umfrage bestätigt, daß rund 80% der Verwaltungen ihre ADV-Systeme durch private Auftragnehmer warten lassen. Dabei handelt es sich um eine letztlich begrenzte Anzahl von Firmen, die ihren (Haupt-)Sitz zum großen Teil im Land Berlin haben. Protokolle von Prüfungen, die die Aufsichtsbehörde für den Datenschutz beim MI nach § 38 Bundesdatenschutzgesetz (BDSG)[45] bei einigen Firmen durchgeführt hat, lassen vermuten, daß das in Rede stehende Problem nichts mit der Auswahl der Auftragnehmer zu tun hat.

Im Zusammenhang der Gespräche zur Novellierung des Brandenburgischen Datenschutzgesetzes (s. unter 2.1) werden zur Zeit Möglichkeiten geprüft, die Frage der Wartung und Fernwartung von ADV-Systemen gesetzlich zu regeln. Ich könnte mir dies in der Weise vorstellen, daß bei Gewährleistung gewisser Mindeststandards die Wartung und Fernwartung im Brandenburgischen Datenschutzgesetz grundsätzlich zugelassen wird, dazu jedoch eine besondere bereichsspezifische Rechtsvorschrift erforderlich ist, soweit davon auch Daten betroffen sind, die einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis unterliegen. Ferner sollte das Ministerium des Innern ermächtigt und verpflichtet werden, die Mindestanforderungen an Auftragsverhältnisse nach § 11 Bbg DSG einschließlich der Wartungsverträge durch Rechtsverordnung zu regeln. In eine solche Rechtsverordnung könnten als Anlage Musterverträge mit aufgenommen werden, die die wesentlichsten Vertragsbestimmungen zum Datenschutz vorformulieren. Unter dieser Voraussetzung könnte dann auf die Verpflichtung verzichtet werden, mich bei Wartungsverträgen über die Auftragserteilung zu unterrichten. Die mir bislang übersandten Verträge entsprechen durchweg nicht den Bestimmungen des Brandenburgischen Datenschutzgesetzes.

Die Umfrage hat ferner ergeben, daß - ohne Einbeziehung von Wartungsverträgen - rund 50% aller Kommunalverwaltungen personenbezogene Daten durch Stellen verarbeiten lassen, auf die das Brandenburgische Datenschutzgesetz keine Anwendung findet. Dies bestätigt den von mir in meinem 2. Tätigkeitsbericht[46] dargelegten Handlungs- und Regelungsbedarf, den auch die Landesregierung in ihrer Stellungnahme dazu[47] grundsätzlich anerkannt hat.

Bestätigt hat die Umfrage außerdem, daß von Datenverarbeitungen im Auftrag - einschließlich Wartungsverträgen - bestimmte Bereiche besonders betroffen sind. So beziehen sich die Auftragsverhältnisse in rund 73% der Fälle auf Lohn- und Gehaltsdaten, in rund 60% auf Meldedaten, in rund 36% auf Sozialdaten und in rund 42% auf andere Daten, die einem besonderen Amtsgeheimnis, in der Regel dem Steuergeheimnis, unterliegen. Dabei ist zu erinnern, daß in diesen Fällen die Datenverarbeitung im Auftrag in der Regel mit einer

---

45 vom 20. Dezember 1990, BGBl. I S. 2954, zul. geänd. durch Gesetz vom 14. September 1994, BGBl. I S. 2321

46 s. dort unter 1.2.1.5, S. 16

47 LT-Drs. 2/169

unbefugten Offenbarung der Daten verbunden ist (s. hierzu auch unter 1.3.7 und 3.1.4).

Aus datenschutzrechtlicher Sicht scheint mir eine grundlegende gesetzliche Neuregelung der Datenverarbeitung im Auftrag letzlich unvermeidlich zu sein. Dies setzt jedoch sorgfältige Vorarbeiten voraus und wird sicherlich nicht kurzfristig ermöglicht werden können. Ich habe dem Ministerium des Innern deshalb vorgeschlagen, einerseits nach Übergangslösungen zu suchen, die zumindest in Teilbereichen die gegenwärtige Praxis befristet auf eine gesetzliche Grundlage stellen, und andererseits zusammen mit dem Land Berlin eine Arbeitsgruppe aus Vertretern jedenfalls der beiden Innenverwaltungen und der Datenschutzbeauftragten zu bilden, die auch unabhängig von der Frage der Fusion der beiden Länder ein Eckpunktepapier für eine insoweit einheitliche Gesetzgebung erarbeiten sollte. Das Ministerium hat mir mitgeteilt, es sei bereit, meinen Vorschlag aufzugreifen, und werde ihn beim nächsten Gesprächstermin mit der Senatsverwaltung für Inneres des Landes Berlin erörtern. Es wäre zu wünschen, daß der Vorschlag auch im weiteren politischen Umfeld die erforderliche Unterstützung erfährt.

3.4 Befugnisse der Gemeindevertretungen und ihrer Ausschüsse zur Verarbeitung personenbezogener Daten

Eine Vielzahl von Anfragen hat es dazu gegeben, ob und ggf. in welchem Umfang der Gemeindevertretung, ihren Ausschüssen oder einzelnen Gemeindevertretern Unterlagen der Verwaltung mit personenbezogenen Daten zur Verfügung gestellt werden dürfen. So hatte in einem Fall (1) der Hauptausschuß einer Stadtverordnetenversammlung darum gebeten, ihm die Unterlagen über ein bestimmtes Gewerbesteuerverfahren vorzulegen, um über einen Antrag des Betroffenen auf Stundung der Steuerschuld entscheiden zu können. In einem anderen Fall (2) sollten der Gemeindevertretung für eine bestimmte Personalentscheidung sämtliche Bewerbungsunterlagen vorgelegt, in einem weiteren Fall (3) dem Rechnungsprüfungsausschuß zur Überprüfung der Eingruppierungen sämtliche Lohn- und Gehaltsunterlagen zugänglich gemacht werden. In einem vierten Fall (4) begehrte ein Gemeindeverteter Einsicht in die Gewerbesteuerlisten und in einem fünften Fall (5) hatte die Gemeindevertretung einen "Untersuchungsausschuß" eingesetzt, der sich mit dem (außerdienstlichen) Verhalten eines Gemeindevertreters befassen sollte.

Die Problematik kann hier nicht abschließend behandelt werden; die angesprochenen Fälle sollen jedoch exemplarisch einen entsprechenden Bedarf an für die Praxis geeigneten Erläuterungen durch die oberste Kommunalaufsichtsbehörde verdeutlichen.

In allen Fällen war zunächst darauf hinzuweisen, daß das Verhältnis zwischen Gemeindevertretung und Gemeindeverwaltung nicht dem von Landtag und Landesregierung entspricht, sondern sich von letzterem wesentlich dadurch unterscheidet, daß die Gemeindevertretung selbst Teil der Gemeindeverwaltung ist. Davon ausgehend ist dann an den Grundsatz der Erforderlichkeit der Datenverarbeitung zur Erfüllung der der datenverarbeitenden Stelle durch Gesetz zugewiesenen Aufgaben anzuknüpfen (vgl. §§ 12 Abs. 1, 14 Abs. 1 und 5 i. V. m. § 13 Abs. 2 Buchst. a Bbg DSG). Daraus ergibt sich, daß die Unterlagen der Gemeindevertretung, ihrem jeweiligen Ausschuß oder einem einzelnen Gemeindevertreter dann vorgelegt werden dürfen, wenn und soweit dies erforderlich ist, damit der Empfänger eine ihm durch Gesetz zugewiesene Aufgabe sachgerecht erfüllen kann.

Im Fall 1 war dies in Übereinstimmung mit einer vom MI dazu erbetenen Stellungnahme als unzweifelhaft zu beurteilen, weil die Entscheidung über die Stundung der jenseits der festgelegten Wertgrenze liegenden Steuerschuld in der Hauptsatzung gem. § 35 Abs. 3 Satz 2

Gemeindeordnung (GO)[48] ausdrücklich dem Hauptausschuß vorbehalten war.

Im Fall 2 war die Weitergabe der gesamten Bewerbungsunterlagen dagegen unzulässig, weil sie für die konkrete Personalentscheidung nicht erforderlich war. Zu prüfen ist in diesen Fällen stets, ob die jeweilige Personalentscheidung wirklich in vollem Umfang durch die Gemeindevertretung oder den Personalausschuß getroffen wird oder es lediglich darum geht, eine Auswahlentscheidung der Gemeindeverwaltung anhand begrenzter Kriterien zu bestätigen. Dann dürfen nur die für die Bestätigung erforderlichen Angaben weitergegeben werden. Ferner muß überlegt werden, ob nicht eine tabellenmäßige Zusammenstellung der relevanten Bewerberdaten völlig ausreicht; insbesondere die Weitergabe von vollständigen Lebensläufen, Ausbildungsnachweisen usw. dürfte nur ganz ausnahmsweise in Betracht kommen. So könnte statt des genauen Geburtsdatums lediglich das Lebensalter aufgeführt werden, statt der genauen Anschrift nur der Wohnort, statt der genauen Bezeichnung früherer Arbeitgeber lediglich die Branche und Unternehmensart, statt der einzelnen Zeugnisnoten nur die Durchschnittsnote. Besondere Zurückhaltung ist vor allem auch bei Angaben mit Drittbezug (z. B. zum Ehegatten und anderen Familienangehörigen) geboten sowie bei "Sozialdaten" (z. B. über einen Bezug von Sozialhilfe u. ä.). Gesundheitsdaten schließlich dürfen grundsätzlich überhaupt nicht weitergegeben werden; hier sollte vielmehr das amtsärztliche Zeugnis über die gesundheitliche Eignung des Bewerbers für den konkreten Dienstposten genügen.

Im Fall 3 habe ich zu der Anfrage nach Maßgabe von § 13 Abs. 3 Satz 2 Bbg DSG im Ergebnis ablehnend Stellung genommen. Im Hinblick auf das gesetzliche Personalaktendatengeheimnis (vgl. § 57 Abs. 3 LBG) und unter Berücksichtigung dessen, daß den Rechnungsprüfungsausschüssen der Gemeindevertretungen mit § 50 GO keine § 95 Landeshaushaltsordnung (LHO)[49] entsprechende Rechtsgrundlage zur Verfügung steht, meine ich, daß den Rechnungsprüfungsausschüssen die Aufgabe der Rechnungsprüfung weder der Qualität der Tätigkeit nach noch nach dem Umfang ihrer Befugnisse in einer dem Auftrag der Staatlichen Rechnungsprüfungsämter vergleichbaren Weise zugewiesen ist und daß ihnen deshalb auch kein grundsätzlich unbegrenzter Zugriff auf die Unterlagen der Verwaltung zusteht. Zu berücksichtigen war auch, daß den Rechnungsprüfungsausschüssen regelmäßig auch Bürger der Gemeinde angehören, die nicht Gemeindevertreter sind (vgl. § 50 Abs. 7 GO). Insbesondere Unterlagen mit solchen personenbezogenen Angaben, die einem besonderem Amtsgeheimnis unterliegen, können deshalb vom Rechnungsprüfungsausschuß in der Regel nicht eingesehen werden, da die von ihm wahrzunehmenden Belange insoweit hinter dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung zurücktreten müssen. Angesichts der Institution der Staatlichen Rechnungsprüfungsämter und ihrer Befugnisse zu einer effektiven Kontrolle der Haushalts- und Wirtschaftsführung scheint mir dieses Ergebnis mit § 7 Abs. 1, Abs. 3 Satz 2 LHO durchaus vereinbar, zumal dem Interesse der Rechnungsprüfungsausschüsse zumeist auch mit anonymisierten listenmäßigen Zusammenstellungen dürfte angemessen entsprochen werden können.

Im Fall 4 habe ich darauf verwiesen, daß es sich bei den Unterlagen, in die Einsicht begehrt wird, zunächst überhaupt um solche handeln muß, die "im Zusammenhang mit der Vorbereitung oder Kontrolle von Beschlüssen der Gemeindevertretung oder von Ausschüssen stehen" (§ 36 Abs. 3 Satz 1 GO). Ist dies der Fall, so können der Akteneinsicht gleichwohl schutzwürdige Belange Betroffener oder Dritter entgegenstehen (§ 36 Abs. 3 Satz 3 GO), so daß eine Abwägung der kollidierenden Belange erforderlich wird. Dabei muß immer geprüft

---

[48] vom 15. Oktober 1993, GVBl. I S. 398, geänd. durch Gesetz vom 30. Juni 1994, GVBl. I S. 230

[49] vom 7. Mai 1991, GVBl. I S. 46, geänd. durch Gesetz vom 3. Juni 1994, GVBl. I S. 197

werden, ob dem Interesse an der Akteneinsicht nicht bereits durch Erteilung einer Auskunft, durch (anonymisierte) listenmäßige Zusammenstellungen (Geschäftsstatistiken; s. unter 3.9.7) oder durch eine Vorlage von Teilakten ausreichend entsprochen werden kann.

Im Fall 5 schließlich war festzustellen, daß Untersuchungsausschüsse mit Befugnissen, wie sie das Untersuchungsausschußgesetz (UAG)[50] vorsieht, nur vom Landtag eingesetzt werden können (§ 2 UAG, Art. 72 Landesverfassung)[51] und deshalb eine Weitergabe von Unterlagen der Verwaltung mit personenbezogenen Angaben an den "Untersuchungsausschuß" der Gemeindevertretung nicht der gesetzlichen Aufgabenzuweisung entsprochen hätte.

Hinzuweisen ist auch darauf, daß die Vorlage personenbezogener Akten an die Gemeindevertretung, ihre Ausschüsse oder an einzelne Gemeindevertreter auch verfahrensmäßig abgesichert werden kann und ggf. muß. So sollten derartige Unterlagen den Gemeindevertretern grundsätzlich nicht zur Vorbereitung der Sitzungen nach Hause übersandt werden; ggf. könnten ihnen die Akten auch erst in der jeweiligen Sitzung selbst vorgelegt werden. Bei den Sitzungen muß nach Maßgabe der Hauptsatzungen die Öffentlichkeit ausgeschlossen werden und in den Sitzungsprotokollen sollte möglichst nicht personenbeziehbar auf den Akteninhalt Bezug genommen werden.

3.5 Polizei

3.5.1 Europa

3.5.1.1 Das Schengener Informationssystem (SIS)

Bereits 1985 hatten sich Belgien, Luxemburg, Frankreich und Deutschland im sog. "Schengener Abkommen" (benannt nach dem luxemburgischen Grenzort, in dem das Abkommen unterzeichnet wurde) verpflichtet, die Grenzkontrollen an ihren gemeinsamen Landesgrenzen schrittweise abzubauen. Am 26. März 1995 ist das auf der Grundlage des Schengener Abkommens ausgehandelte Schengener Durchführungsübereinkommen (SDÜ)[52] in Kraft getreten, dem unterdessen neben den o. g. Vertragsstaaten auch Italien, Portugal, Spanien und Griechenland beigetreten sind. Mit dem Inkrafttreten des SDÜ entfallen nunmehr die Grenzkontrollen innerhalb "Schengenlands". Um die befürchteten Sicherheitsdefizite aufzufangen, sieht das SDÜ in Art. 6 vor, daß an den jeweiligen Außengrenzen (in Brandenburg sind das die Übergänge nach Polen, Tschechien und Slowakei sowie der Flughafen Schönefeld) eine lückenlose Kontrolle der Ein- und Ausreisen erfolgt. Trotz umfangreicher Vorkehrungen, die von der baulichen Umgestaltung der Abfertigungsschalter bei der Ein- und Ausreise in Flughäfen bzw. an Grenzübergängen bis zum Ausbau des SIS reichten, läßt sich eine lückenlose Kontrolle in der Praxis nicht durchsetzen, so daß häufig Ein- und Ausreisende aus Drittländern kontrolliert werden, während bei "Schengen-Bürgern" nur stichprobenartige Überprüfungen erfolgen.

Das Kernstück der Sicherheitsmaßnahmen ist das SIS, das am 26. März 1995 in Straßburg seine Arbeit aufgenommen hat. Damit stehen Polizei und Justizbehörden der Schengener Vertragspartner eine Datenbank für Fahndungsdaten on-line europaweit zur Verfügung. Das System besteht aus einer zentralen Komponente (CSIS) in Straßburg und den nationalen Teilen (NSIS) der einzelnen Vertragsstaaten mit jeweils identischem Datenbestand, der durch

---

50 vom 17. Mai 1991, GVBl. I S. 86, zul. geänd. durch Gesetz

51 vom 4. Juli 1994, GVBl. I S. 263

52 vom 20. August 1992, GVBl. I S. 298

vom 23. Juli 1993, BGBl. II S. 1013

einen ständigen Abgleich der NSIS mit CSIS gewährleistet wird. Abfragen der zugriffsberechtigten Stellen laufen an die NSIS (in der Bundesrepublik Deutschland ist das das Bundeskriminalamt), die Informationen nur über das Straßburger CSIS, die diese jedoch nicht untereinander austauschen können.

Die Arten der im Schengener Informationssystem gespeicherten Daten - neben Name, Geburtsdatum und -ort, Staatsangehörigkeit, auch besondere körperliche Merkmale und personenbezogene Hinweise wie "bewaffnet" oder "gewalttätig" - sind abschließend festgelegt. Zur Zeit sind ca. 2 Mio. Datensätze im SIS eingestellt, ausgelegt ist die Datenbank für 10 Mio.

Voraussetzung für eine Speicherung im SIS sind folgende Ausschreibungen:

- zur Festnahme mit dem Ziel der Auslieferung,

- zur Einreiseverweigerung eines sog. Drittausländers (Bürger eines Staates, der dem Schengener Abkommen nicht beigetreten ist),

- zur Aufenthaltsermittlung von vermißten Personen, Zeugen oder angeklagten Personen,

- zur polizeilichen Beobachtung,

- von Gegenständen, die beschlagnahmt werden sollen oder als Beweismittel in Strafverfahren dienen.

Maßgeblich für eine Ausschreibung ist das nationale Recht der jeweiligen Vertragspartner.

Neben dem Datenaustausch der Vertragspartner mit Hilfe des SIS sieht das Schengener Durchführungsübereinkommen auch den umfänglichen Informationsaustausch der sog. fahndungsbegleitenden Daten zwischen den nationalen Zentralstellen ("SIRENEN") vor, der in der Bundesrepublik Deutschland ebenfalls über das BKA läuft. Der umfangreiche Datenaustausch innerhalb "Schengenland" bleibt datenschutzrechtlich äußerst problematisch, da die in Deutschland geltenden relativ strengen Datenverarbeitungsregelungen nicht "schengenweit" durchgesetzt werden konnten.

Obwohl das Schengener Durchführungsabkommen einen gewissen datenschutzrechtlichen Standard vorschreibt, haben noch nicht alle Beitrittsstaaten entsprechende Vorschriften in ihr nationales Recht aufgenommen. Neben der Verpflichtung, einen Datenschutzstandard zu verwirklichen, der zumindest dem Übereinkommen des Europarates über den Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 entspricht, enthält das SDÜ immerhin weitere Regelungen, die die Persönlichkeitsrechte der Betroffenen stärken:

- So müssen die Mitgliedsstaaten eine unabhängige Kontrollinstanz, die den nationalen Datenbestand in NSIS überwacht (in der Bundesrepublik Deutschland ist das der Bundesbeauftragte für den Datenschutz) sowie eine gemeinsame Kontrollinstanz für CSIS einrichten. Letzteres hat unterdessen ihre Arbeit aufgenommen.

- Jeder Bürger hat ein grundsätzliches Auskunftsrecht über die im SIS zu seiner Person gespeicherten Daten sowie das Recht zur Berichtigung unrichtiger bzw. zur Löschung unrechtmäßiger Daten. Diese Rechte kann er in jedem Vertragsstaat geltend machen. Dazu sowie zu Schadensersatzansprüchen steht ihm in jedem Vertragsstaat der Klageweg offen.

Es bleibt abzuwarten, ob diese Vorkehrungen ausreichen, die Rechtsansprüche des Betroffenen angemessen durchsetzen zu können.

3.5.1.2 EUROPOL

Im Vertrag über die Europäische Union vom 7. Februar 1992 haben die unterzeichnenden Minister vereinbart, ein Europäisches Polizeiamt einzurichten. Darüber, wie das im einzelnen aussehen sollte, herrschten höchst unterschiedliche Auffassungen: Während der Bundesrepublik Deutschland eine gesamteuropäische Polizeibehörde - eine Art europäisches FBI - vorschwebte, wollte Frankreich eher ein Büro ohne Eingriffsbefugnisse, das den Informationsaustausch zwischen den europäischen Polizeibehörden koordiniert. Gegenwärtig ist EUROPOL eher letzteres.

Das in Den Haag eröffnete Europäische Polizeiamt besteht in seiner ersten Ausbauphase aus einem Kooperationsstab, der unter der Bezeichnung EDU (European Drug Unit), den Informationsaustausch für den Bereich des internationalen Drogenhandels koordinieren soll.

Der unter der deutschen Präsidentschaft nicht mehr verabschiedete Entwurf eines Übereinkommens über die Errichtung eines Europäischen Polizeiamtes[53], die sog. EUROPOL-Konvention, weist der Europäischen Polizeibehörde folgende Aufgaben zu:

- Informationen zu sammeln, zu analysieren und auszuwerten,

- über die nationalen Zentralstellen (in der Bundesrepublik das BKA) die zuständigen Behörden der Mitgliedsstaaten über sie betreffende Informationen und Kenntnisse über Zusammenhänge von Straftaten zu unterrichten,

- Ermittlungen in den Mitgliedsstaaten durch die Übermittlung aller sachdienlichen Informationen an die nationalen Stellen zu unterstützen,

- eine automatisiert geführte Sammlung von Informationsbeständen zu unterhalten, die nationale, aber auch von EUROPOL selbst erhobene Daten enthält.

Grundsätzlich soll EUROPOL die Zusammenarbeit der europäischen Polizeibehörden im Rahmen der Ermittlungen gegen die organisierte, international auftretende Kriminalität unterstützen.

Zur Aufgabenerfüllung stehen EUROPOL gemäß Konventionsentwurf die Befugnisse zu,

- eigene Dateien zu führen, die sich aus Datenübermittlungen der Mitgliedsstaaten speisen, zu denen sie jedoch keinen Zugang haben,

- unabhängig von den Mitgliedsstaaten Informationen in dem o. g. Informationssystem zu speichern und abzurufen,

- nach eigenem Ermessen regelmäßig Daten an Dritte - darunter auch an Geheimdienste - zu übermitteln,

- in den Mitgliedsstaaten bereits gelöschte Daten weiter zu speichern,

- ohne Mitwirkung der anliefernden Polizeibehörden Auskunft an die Betroffenen zu erteilen.

Insgesamt erhält EUROPOL durch den Konventionsentwurf den Status einer internationalen zwischenstaatlichen Institution, der äußerst problematisch ist. In der EUROPOL-Konvention

---

53 BR-Drs. 909/94

fehlen Regelungen, die die Einbindung in das rechtsstaatliche Gefüge mit seinen demokratisch-legitimierten Kontrollinstanzen, wie Gerichte, Parlamente oder ministeriale Fachaufsicht, gewährleisten.

Diese erhebliche verfassungsrechtliche Problematik hat auch datenschutzrechtliche Auswirkungen, die die Datenschutzbeauftragten veranlaßt haben, die materielle Verantwortlichkeit der zuständigen Polizeibehörden zur wesentlichen Anforderung an die EUROPOL-Konvention zu erheben. Nur die Polizeibehörde, die personenbezogene Daten rechtmäßig erhoben hat sowie zu eigenen Zwecken speichert und nutzt, kann die Erforderlichkeit ihrer weiteren Verwendung im europäischen Zusammenhang beurteilen. Nur sie ist aufgrund ihrer Erkenntnisse und Unterlagen in der Lage, die Richtigkeit und Vollständigkeit der an andere europäische Polizeien übermittelten Daten zu gewährleisten[54]. Aus dem Grundsatz der materiellen Verantwortlichkeit ergeben sich aus datenschutzrechtlicher Sicht folgende Forderungen:

- EUROPOL muß eine klare, abschließende Aufgabenzuweisung erhalten. Alle an EUROPOL übermittelten Daten dürfen nur im Zusammenhang mit Straftaten genutzt werden, zu deren Verfolgung EUROPOL gemäß der Konvention zuständig ist. Voraussetzung für die Zuständigkeit von EUROPOL ist eine Straftat, von der mehrere Mitgliedsstaaten betroffen sind und die aufgrund des Umfangs, der Bedeutung und der Folgen ein gemeinsames Vorgehen erfordert.

- Alle Schritte der Datenverarbeitung im Informationssystem von EUROPOL können nur durch die Stelle veranlaßt werden, die materiell für die ihr zugrunde liegende Aufgabe der Strafverfolgung oder Gefahrenabwehr zuständig ist. Dies gilt auch für die Auskunft an Betroffene, die Berichtigung und die Löschung von Daten.

Die Beratungen über den Konventionsentwurf zu EUROPOL sind unter der derzeitigen Präsentschaft Frankreichs erneut aufgenommen worden.

3.5.2 Konsequenzen aus dem 2. Tätigkeitsbericht

3.5.2.1 Videoaufnahmen anläßlich einer Pressekonferenz

Zum Zeitpunkt der Vorlage meines 2. Tätigkeitsberichts[55] sowie der Stellungnahme der Landesregierung[56] war die Frage noch nicht geklärt, ob die Datenerhebung mittels Videokamera anläßlich der Pressekonferenz in einem besetzen Haus rechtmäßig gewesen war. Ich gehe weiterhin davon aus, daß dies nicht der Fall war. Die Polizeibehörde, die bereits mitgeteilt hatte, daß sie die Videoaufnahme vernichten wolle, war von dieser Absicht abgerückt, weil zwei Betroffene vor dem Verwaltungsgericht auf Vernichtung der erhobenen Daten geklagt hatten. Zur Frage, ob die Datenerhebung erforderlich und damit rechtmäßig gewesen war, brauchte das Verwaltungsgericht sich jedoch nicht mehr zu äußern, weil die Polizeibehörde von sich aus bereit war, die Videoaufnahme zu vernichten.

In einem Gespräch, das der grundsätzlichen Erörterung dieser sowie anderer strittiger Fragen diente, stellte die Polizei klar, daß es einen solchen Einsatz in Zukunft nicht mehr geben werde. In der strittigen Frage der Rechtmäßigkeit ist zwar keine Übereinstimmung, jedoch eine Annäherung der gegensätzlichen Standpunkte erreicht worden.

54

55 s. Anlage 6

56 s. unter 3.6.4, S. 73 ff.
LT-Drs. 2/169

3.5.2.2 Prüfung der Polizeipräsidien

Die Polizeipräsidien haben im vergangenen Jahr in vielfältiger Weise Konsequenzen aus den im meinem 2. Tätigkeitsbericht[57] dargestellten Prüfungen gezogen. Ich begrüße die darin zum Ausdruck kommende Bereitschaft der Polizeibehörde und des Ministeriums des Innern (MI), datenschutzrechtlichen Belangen einen hohen Stellenwert bei der Aufgabenerfüllung einzuräumen, ausdrücklich. Insgesamt betrachtet ist das datenschutzrechtliche Niveau bei der Datenverarbeitung deutlich angehoben worden.

Das ist vor allem auf die Bereinigung der Kriminalakten (KA) zurückzuführen, die bis Jahresende mit Hilfe eines vom MI erarbeiteten Maßnahmekatalogs abgeschlossen wurde. Damit stehen diejenigen KA und -bestandteile, die aufgrund der darin vermerkten Informationen rechtswidrig tief in die Persönlichkeitsrechte der Betroffenen eingegriffen haben, nicht mehr zur Aufgabenerfüllung der brandenburgischen Polizei zur Verfügung (s. 3.5.3).

Im gleichen Zeitraum erfolgte auch die Bereinigung der Fingerabdruck-Blätter der Volkspolizei sowie die Erfassung des nach der Maßnahme übriggebliebenen Bestandes im Automatisierten Fingerabdruck-Informationssystem (AFIS) beim Bundeskriminalamt.

Um die Rückmeldung der Staatsanwaltschaft (StA) über den Verfahrensstand zu vereinfachen - ich hatte deren Fehlen im 2. Tätigkeitsbericht[58] moniert -, hat ein Polizeipräsidium ein Formblatt erarbeitet. Dem Vernehmen nach ist in diesem Polizeipräsidium das Problem fehlender Rückmeldungen dadurch behoben.

Die von mir im 2. Tätigkeitsbericht[59] bemängelten Errichtungsanordnungen, Dateibeschreibungen bzw. Dateienregistermeldungen sind entsprechend den Rechtsvorschriften verbessert bzw. ergänzt worden. Bei den Errichtungsanordnung sowie Dateienregistermeldungen, die mir im Berichtszeitraum des vorliegenden Tätigkeitsberichts zu neu eingerichteten Dateien zugesandt wurden, traten diese Mängel im allgemeinen nicht mehr auf. Erfreulich ist in diesem Zusammenhang auch, daß das MI nicht nur die Betriebsaufnahme einer neuen Datei frühzeitig anzeigt, sondern auch regelmäßig mitteilt, wenn nicht mehr erforderliche Dateien eingestellt und die Datenbestände gelöscht werden.

57

58 s. unter 3.6.2, S. 62 ff.

59 s. unter 3.6.2.2, S. 65

s. unter 3.6.2.1, S. 63 ff.

3.5.3 Unterlagen der Volkspolizei der ehemaligen DDR

3.5.3.1 DORA: Kein Ende, aber ein Abgesang

Mit der abgeschlossenen Bereinigung der KA hat DORA - das dialogorientierte Recherche- und Auskunftssystem der Volkspolizei - auch seine Funktion als "Findex-Datei" (Aktenhinweissystem) für den KA-Bestand bei den Polizeipräsidien und dem LKA verloren. Sie wird daher bei den o. g. Behörden gem. § 47 Abs. 4 Polizeigesetz (PolG) i. V. m. § 1 Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg (VGPolGBbg)[60] als gesperrte Datei auf Disketten aufbewahrt. Ein Zugriff ist derzeit nicht möglich, weil die dafür vorgesehenen PC nicht mehr zur Verfügung stehen. Obwohl DORA ebenso wie die ausgesonderten Kriminalakten bzw. -teile zur Aufgabenerfüllung der Polizei nicht mehr erforderlich sind, können sie nicht gelöscht bzw. vernichtet werden, weil § 47 Abs. 4 PolG i. V. m. § 1 VGPolGBbg festlegt, daß Löschung und Vernichtung unterbleiben, wenn

- Grund zu der Annahme besteht, daß schutzwürdige Belange der Betroffenen beeinträchtigt würden,

- die Daten zur Behebung einer bestehenden Beweisnot unerläßlich sind oder

- die Nutzung der Daten zu wissenschaftlichen Zwecken erforderlich ist.

Der fragliche Datenbestand erfüllt alle drei Voraussetzungen für die Sperrung anstelle einer Löschung bzw. Vernichtung.

Das MI schlägt daher vor, die ausgesonderten KA sowie -bestandteile und DORA gem. § 47 Abs. 5 PolG i. V. m. § 1 VGPolGBbg dem Landeshauptarchiv als Gesamtpaket zur Übernahme in das Zwischenarchiv (s. § 2 Abs. 4 Brandenburgisches Archivgesetz - BbgArchivG)[61] anzubieten. Diesen Vorschlag habe ich begrüßt, weil so sichergestellt ist,

- daß anfragende Bürger nicht von einer Stelle zur nächsten verwiesen werden und

- die Verantwortung für diesen Datenbestand gem. § 5 Abs. 5 i. V. m. § 2 Abs. 4 BbgArchivG bei der Polizei verbleibt.

Damit kann eine Auskunftserteilung in absehbarer Zeit realisiert werden. Der Antragsteller muß nicht warten, bis das Archiv die Unterlagen gesichtet und nach archivfachlichen Gesichtspunkten zur Einsichtnahme aufbereitet hat (s. auch unter 3.5.3.3).

3.5.3.2 Verwaltungsarchive der ehemaligen Bezirksdirektionen der Volkspolizei (BdVP) und Volkspolizeikreisämter (VPKÄ)

Solche Archive befinden sich in fast allen Schutzbereichen sowie Polizeipräsidien der brandenburgischen Polizei. Nach der für die Volkspolizei der ehemaligen DDR verbindlichen Archivordnung wurden Vorgänge archiviert, wenn sie für die aktuelle Aufgabenerfüllung nicht mehr erforderlich waren. Diese erste Archivierung erfolgte normalerweise in einer extra dafür ausgewiesenen Abteilung der Aktenhaltung. Nach fünfjähriger Lagerung in den Archiven der VPKÄ wurden sie in das Archiv der BdVP abgegeben. Dort blieben die Vorgänge mindestens fünf Jahre, in den meisten Fällen jedoch zehn Jahre.

Mit dem 30. Oktober 1990 wurden die Archive geschlossen und versiegelt, so daß sie seither

---

60

61 vom 11. Dezember 1991, GVBl. S. 636
vom 7. April 1994, GVBl. I S. 94

weder betreten noch Unterlagen hinzugefügt oder entnommen werden konnten. Die räumliche Unterbringung war stets gesichert, da die Archive ausschließlich in polizeieigenen Gebäuden aufbewahrt wurden. Vor der Entscheidung, wie mit den Archivunterlagen verfahren werden sollte, hat sich das MI in zwei Schutzbereichen einen Überblick über die dort aufbewahrten Unterlagen verschafft. Darüber hinaus sind Bestandsverzeichnisse angelegt worden. Sichtung und Bestandsverzeichnis ergaben, daß bei den fraglichen Unterlagen kein Grund zu der Annahme besteht, daß durch eine Vernichtung schutzwürdige Belange der Betroffenen beeinträchtigt würden bzw. daß die Unterlagen zur Behebung einer bestehenden Beweisnot unerläßlich wären. Soweit in den Archiven Unterlagen aus dem Strafvollzug sind, wurden sie dem Ministerium der Justiz Brandenburg zur Übernahme angeboten. Das Justizministerium hat die Übernahme jedoch abgelehnt. Da nicht auszuschließen ist, daß die Unterlagen für wissenschaftliche Zwecke von Nutzen sein könnten, sind sie dem Landeshauptarchiv Brandenburg angeboten worden, das einen Teil für archivwürdig erklärt hat. Danach hat das MI den Polizeipräsidien in einem Rundschreiben diejenigen Unterlagen mitgeteilt, die vernichtet werden können.

Das MI hat mich an dem Verfahren beteiligt. Datenschutzrechtliche Bedenken stehen dem Verfahren einschließlich der Vernichtung nicht entgegen.

3.5.3.3 Problematische Auskunftserteilung gem. § 49 PolG i. V. m. § 1 VGPolGBbg

Die seit Jahresanfang durch das "Datenscheckheft"[62] ausgelösten Anfragen vieler Bürger über evtl. zu ihrer Person in DORA gespeicherten Daten sowie über evtl. vorhandene KA werfen vielfältige Probleme auf. Gem. § 49 PolG i. V. m. § 1 VGPolGBbg hat jeder das Recht, gebührenfrei Auskunft zu erhalten über

- die zu seiner Person gespeicherten Daten,

- die Herkunft der Daten und die Empfänger von Übermittlungen (soweit dies noch feststellbar ist) sowie

- den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verwendung.

Durch ein redaktionelles Versehen bei der Erstellung des Datenscheckheftes ist bedauerlicherweise sowohl in den "gelben Seiten" als auch auf der Antragskarte selbst der vorgesehene Hinweis entfallen, daß die Antragsteller die Art der Daten, über die sie Auskunft wollen, näher bezeichnen müssen (§ 49 Abs. 1 Satz 2 PolG). Ohne diese Angaben kann die Polizei den Antrag aber gem. § 49 Abs. 1 Satz 4 PolG ablehnen.

Um trotz der fehlenden Hinweise dennoch Auskunft erteilen zu können, hat das MI unterdessen ein Musterschreiben entworfen, in dem die Bürger gebeten werden anzugeben, in welchem Zusammenhang die Polizei personenbezogene Daten über sie registriert haben könnte. Das Ministerium ist meiner Anregung gefolgt, in einem besonderen Absatz des Schreibens darauf hinzuweisen, daß die Angaben sowie die evtl. zur Verfügung gestellten Unterlagen nur zur Auskunftsbearbeitung verwendet werden. Die durch das Auskunftsersuchen entstandene Akte wird zwei Jahre aufbewahrt. Nach meiner Beobachtung verwenden leider nicht alle Polizeipräsidien dieses Musterschreiben.

Diese von den Polizeipräsidien und dem LKA als erste Reaktion an den antragstellenden Bürger versandte Schreiben löst dort oft beträchtliche Irritationen aus. Immer wieder muß meine Behörde anfragende Bürger darauf hinweisen, daß die Polizeibehörden nähere

---

62 Broschüre der Informationsreihe: "Der Datenschutzbeauftragte für das Land Brandenburg informiert"

Angaben benötigen, weil sie ohne diese mit vernünftigem Verwaltungsaufwand nicht in der Lage sind, die den anfragenden Bürger betreffenden Unterlagen aufzufinden.

Ungeachtet dieser Umstände wirft die Auskunftserteilung zu DORA aber auch aufgrund des Dateizustandes besondere Probleme auf. Schon vor dem 3. Oktober 1990 ist DORA mehreren Bereinigungsaktionen[63] unterzogen worden. Dabei sind diejenigen Datensätze gelöscht worden, für die es nach bundesrepublikanischem Recht keine Speicherungsbefugnis gab, weil sie nach Strafgesetzbuch (StGB)[64] keine Straftatbestände sind. Gelöscht wurden so z. B. personenbezogene Daten der wegen Republikflucht oder Rowdytums beschuldigten Personen. Häufig wurden auch die dazugehörigen KA vernichtet. Als Folge aus diesen Löschungs- bzw. Vernichtungsaktionen werden zahlreiche antragsstellende Bürger mit einer Negativauskunft rechnen müssen, obwohl sie wissen, daß ihre Daten zu DDR-Zeiten von der Polizei erfaßt worden sind. Daß derzeit DORA zur Auskunftserteilung nicht abgefragt werden kann, ist nur solange hinnehmbar, als noch nicht über die Abgabe an das Brandenburgische Landeshauptarchiv entschieden ist (s. unter 3.5.3.1).

Grundsätzlich kann die Polizei eine Auskunftserteilung aber auch ablehnen, wenn das Recht des Antragstellers hinter dem überwiegenden Geheimhaltungsinteresse des Bundes oder des Landes zurücktritt. Einer Auskunftserteilung kann auch das Recht einer anderen Person (eines Dritten) entgegen stehen, das durch die Auskunft unzulässig beeinträchtigt würde. Diejenigen Antragsteller, denen eine Auskunft verweigert worden ist, können sich an mich wenden, um den Vorgang datenschutzrechtlich überprüfen zu lassen.

3.5.4 Prüfung der Unterlagen zur Polizeilichen Beobachtung im Landeskriminalamt und in den Polizeipräsidien

Im Berichtszeitraum habe ich die im Landeskriminalamt (LKA) sowie in den Polizeipräsidien vorhandenen Vorgänge zur Polizeilichen Beobachtung (pB) geprüft.

Die pB ist eine typische Vorfeldmaßnahme, die sowohl zur Strafverfolgung als auch zur Gefahrenabwehr eingesetzt wird. Ziel ist dabei nicht die Verhinderung einer konkreten Straftat, sondern die Sammlung von Informationen im Vorfeld vermuteter Straftaten, die für die spätere Strafverfolgung nützlich sein können. Sie dient der vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung. Die meisten Ausschreibungen zur pB erfolgen daher auf der Grundlage der Polizeiaufgabengesetze der Länder.

Einschlägige Rechtsvorschrift für das Land Brandenburg ist § 40 PolG i. V. m. § 1 VGPolGBbg. Danach kann die Polizei personenbezogene Daten (Personalien des Betroffenen sowie Kennzeichen des von ihm benutzten oder eingesetzten Fahrzeugs) zur pB ausschreiben, wenn die Gesamtwürdigung des Betroffenen und der von ihm bisher begangenen Straftaten erwarten läßt, daß er auch künftig Straftaten von erheblicher Bedeutung begehen wird. Soweit im Zusammenhang mit einer bereits begangenen Straftat von erheblicher Bedeutung der Sachverhalt aufgeklärt werden soll, wird gem. § 163 e Strafprozeßordnung (StPO)[65] ausgeschrieben. Sowohl Polizeigesetz als auch StPO regeln, daß die Maßnahme sich nicht nur gegen ausgeschriebene Tatverdächtige bzw. Beschuldigte richten kann, sondern auch gegen Kontakt- bzw. Begleitpersonen. Zum Verfahren der Ausschreibung legt § 40 Abs. 3 PolG i. V. m. § 1 VGPolGBbg fest, daß sie durch einen Richter angeordnet werden muß und

---

63

64 s. 2. Tätigkeitsbericht unter 3.6.1.2, S. 61

65 i. d. Fassung vom 10. März 1987, BGBl. I S. 945, ber. S. 1160

i. d. Fassung vom 7. April 1987, BGBl. I S. 1074, ber. S. 1319

auf ein Jahr zu befristen ist. Sie kann um ein weiteres Jahr verlängert werden, wobei im Halbjahresrhythmus geprüft werden muß, ob die Voraussetzungen für die Anordnung noch bestehen.

Gem. § 40 Abs. 4 der genannten Vorschrift sind die Betroffenen von der Ausschreibung zur pB zu unterrichten, sobald der Zweck der Maßnahme dadurch nicht unterlaufen wird und kein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden ist. Auch das Verfahren der pB ist dem Polizeigesetz zu entnehmen. Danach darf die Polizei die zur pB ausgeschriebenen Personen gem. § 40 Abs. 1 in einer Datei speichern und gem. § 40 Abs. 2 der genannten Rechtsvorschrift den Betroffenen bzw. das von ihm benutzte oder eingesetzte Kraftfahrzeug sowie Kontakt- und Begleitpersonen und mitgeführte Sachen an die ausschreibende Polizeidienststelle übermitteln, wenn diese im Zuge einer polizeilichen Maßnahme angetroffen bzw. aufgefunden werden.

Wegen der ohne Wissen der Betroffenen ablaufenden Maßnahmen, die es ermöglichen, Bewegungsprofile nicht nur über Störer, sondern auch über Nichtstörer zu erstellen und die tief in die Persönlichkeitsrechte der Betroffenen eingreifen, bedarf es der besonderen Beachtung der Verfahrensregelungen, um so den Grundrechtsschutz zu wahren. Die Prüfung der Datenverarbeitung zur pB im LKA sowie den Polizeipräsidien ergab keine datenschutzrechtlichen Bedenken. Da das gesamte Verfahren - soweit es sich nicht aus dem PolG bzw. der StPO ergibt - der Geheimhaltung unterliegt, kann hier auf Einzelheiten der Prüfung nicht eingegangen werden.

3.5.5 Überprüfung von Personen zur Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung

3.5.5.1 Hintergrund

Zweck der Überprüfung ist der Schutz der öffentlichen Sicherheit und Ordnung sowie die Vorsorge für die Verfolgung von Straftaten - beides originäre Polizeiaufgaben gem. § 1 PolG i. V. m. § 1 VGPolG - bei Anlässen wie z. B. Staatsbesuchen. Vor dem Hintergrund, daß die eingeladenen Gäste solcher Veranstaltungen aufgrund bestimmter Merkmale Opfer von Straftaten werden könnten, darf die Polizei die Daten derjenigen Personen, die "von Amts wegen" mit den gefährdeten Personen in Verbindung treten, mit polizeilichen Datensammlungen abgleichen. Damit soll ausgeschlossen werden, daß sich Personen, die bereits in der Vergangenheit als "Störer" in ähnlichen Zusammenhängen polizeilich in Erscheinung getreten sind, im Umkreis der eingeladenen Gäste aufhalten können. Rechtsgrundlage der Überprüfung ist § 33 a Abs. 1 Nr. 1 i. V. m. § 33 PolG i. V. m. § 1 VGPolG. Diese Vorschrift befugt die Polizei, personenbezogene Daten nicht nur über Störer oder Tatverdächtige zu erheben, sondern auch über solche Personen, die bisher weder als Störer noch als Tatverdächtige polizeilich bekanntgeworden sind, und nach § 41 Abs. 1 PolG i. V. m. § 1 VGPolG zum Abgleich mit Polizeidateien - wie z. B. dem INPOL-Fahndungsbestand - zu nutzen.

3.5.5.2 Überprüfung bestimmter Mitarbeiter und Mitarbeiterinnen der Koordinierungsstelle 50. Jahrestag

Eine Petentin, die zur Betreuung der anläßlich der Feierlichkeiten zur Befreiung der brandenburgischen Konzentrationslager eingeladenen Zeitzeugen und Zeitzeuginnen eingesetzt werden sollte, hat mir ein mit "Einwilligungserklärung" überschriebenes Schriftstück der Koordinierungsstelle 50. Jahrestag zugesandt und gebeten zu klären,

- zu welcher Art von Überprüfung sie ihr Einverständnis erklären solle und

- ob die Einwilligungserklärung den gesetzlichen Anforderungen entspräche.

Bei den Feierlichkeiten zum 50. Jahrestag der Befreiung der Konzentrationslager im Land Brandenburg handelt es sich zweifellos um Anlässe, bei denen Gefahren für die öffentliche Sicherheit und Ordnung nicht mit hinreichender Sicherheit auszuschließen sind, so daß die Polizei befugt ist, geeignete Maßnahmen zum Schutz der Veranstaltungen durchzuführen. Die Überprüfung des Personenkreises, der mit der Betreuung der eingeladenen Gäste betraut ist, kann sowohl als erforderlich als auch geeignet betrachtet werden, um den angestrebten Zweck zu erreichen. Die von dieser Maßnahme Betroffenen müssen die Überprüfung jedenfalls dann im überwiegenden Allgemeininteresse an einem geordneten Ablauf der in Rede stehenden Veranstaltungen hinnehmen, wenn sie "von Amts wegen" an den Veranstaltungen teilnehmen wollen. Soweit die Koordinierungsstelle dazu Daten von ihren Mitarbeitern erhob und an die Polizei übermittelte, erfolgte die Datenerhebung und -verarbeitung auf der Grundlage des § 4 Abs. 1 b Bbg DSG, also mit Einwilligung des Betroffenen. Dazu bedurfte es gem. § 4 Abs. 2 Bbg DSG einer schriftlichen Einwilligungserklärung.

Die von der Koordinierungsstelle ausgehändigte Einverständniserklärung entsprach jedoch nicht den in § 4 Abs. 2 Bbg DSG festgelegten Anforderungen an eine solche Erklärung. Das uns durch die Petentin übersandte Formular informierte die Betroffenen weder über die Art der Überprüfung oder die Stelle, die die Überprüfung vornehmen sollte, noch enthielt es einen Hinweis, ob die Datenerhebung und Überprüfung auf freiwilliger Basis oder aufgrund einer Rechtsvorschrift erfolgte. Ebenso fehlte eine Aussage über die Folgen einer Einverständnisverweigerung. Es war so wegen seiner Unbestimmtheit im höchsten Maße geeignet, die Betroffenen zu verunsichern.

Ich habe mich deshalb an das Ministerium für Wissenschaft, Forschung und Kultur im Land Brandenburg gewandt, das die Koordinierungsstelle mit der Abwicklung der Feierlichkeiten betraut hatte und gefordert, die Einverständniserklärung den gesetzlichen Vorschriften des § 4 Abs. 2 Bbg DSG anzupassen. Das Ministerium hat daraufhin die Einverständniserklärung so geändert, daß sie alle erforderlichen Angaben enthielt.

Im vorliegenden Fall wurden die Daten der Betreuer/-innen mit dem INPOL-Fahndungsbestand abgeglichen. Im "Trefferfall", d. h. wenn eine Notierung vorlag, erfolgte eine Prüfung des Sachverhalts. Erst wenn das Ergebnis nahelegte, daß der Betroffene nicht zur Betreuung eingesetzt werden sollte, erging eine entsprechende Empfehlung der Polizei ohne Angabe der Gründe an die Koordinierungsstelle.

3.5.6 Platzverweis, erkennungsdienstliche Behandlung und die Folgen

Zur Abwehr einer Gefahr für die öffentliche Sicherheit kann die Polizei eine Person vorübergehend von einem Ort verweisen oder ihr das Betreten eines Ortes verbieten. Verfassungsrechtlich ist das ein Eingriff in das Grundrecht auf körperliche Bewegungsfreiheit gem. Art. 2 Abs. 2 GG, der einer gesetzlichen Grundlage bedarf. Diese findet sich sowohl in § 19 PolG i. V. m. § 1 VGPolBbg, als auch in § 64 StPO. Unter der Voraussetzung, daß die Anwesenheit einer Person an einem bestimmten Ort eine Gefahr für die öffentliche Sicherheit darstellt, kann die Polizei Personen in Gewahrsam nehmen, wenn der Platzverweis auf andere Weise nicht durchzusetzen ist. Ähnlich verhält es sich, wenn der Platzverweis im Zusammenhang mit polizeilichen Maßnahmen auf der Grundlage der Strafprozeßordnung erteilt wird. § 164 StPO enthält die Befugnis zur Festnahme, wenn jemand die Amtshandlungen der Polizei vorsetzlich stört.

Die erkennungsdienstliche Behandlung (ed-Behandlung) ist eine Sonderform der Identitätsfeststellung. Die Identitätsfeststellung als typische polizeiliche Standardmaßnahme geht fast immer mit anderen polizeilichen Maßnahmen einher, geht ihnen voran oder folgt ihnen nach. Umgekehrt findet sich kaum ein polizeiliches Handeln, das nicht auch von einer Identitätsfeststellung begleitet wird. Das Polizeigesetz stellt dazu eine Reihe von Maßnahmen zur Verfügung. So darf der Betroffene angehalten und nach seinen Personalien gefragt werden (§ 14 Abs. 1 und § 15 Abs. 2 PolG i. V. m. § 1 VGPolGBbg). Die Polizei kann

verlangen, daß mitgeführte Ausweispapiere zur Prüfung ausgehändigt werden. Sie darf den Betroffenen festhalten, ihn und die mitgeführten Sachen nach Gegenständen, die zur Identitätsfeststellung dienen, durchsuchen, ihn zur Dienststelle bringen sowie - als letzte Möglichkeit - erkennungsdienstlich behandeln (§ 15 Abs. 2 und § 16 Abs. 2 PolG i. V. m. § 1 VGPolgG) - ein sauber abgestuftes Verfahren, bei dem die nächste Stufe stets beschritten werden darf, wenn die vorhergehende erfolglos war. Der Gesetzessystematik entsprechend ist die Befragung und Überprüfung der Ausweispapiere das für den Regelfall festgelegte Verfahren und die ed-Behandlung (z. B. Abnahme von Finger- und Handflächenabdrücken, Aufnahme von Lichtbildern, Feststellung äußerer körperlicher Merkmale, Messungen und ähnliche Maßnahmen) die Ausnahme.

Als Voraussetzung für die als letztes Mittel vorgesehene ed-Behandlung legt § 16 Abs. 2 PolG i. V. m. § 1 VGPolGBbg fest, daß eine nach § 15 zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich oder daß die ed-Behandlung zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil der Betroffene verdächtigt ist, eine Tat begangen zu haben, die mit Strafe bedroht ist.

Daß in der polizeilichen Praxis dieses Regel- und Ausnahmeverhältnis häufig umgekehrt wird, belegt die Eingabe eines Petenten, die mich im Berichtszeitraum erreichte. Er gab an, daß er während einer Demonstration von der Polizei in Gewahrsam genommen und im Polizeipräsidium fotografiert worden sei, obwohl er sich schon am Festnahmeort mittels Paß ausgewiesen hätte.

Die Polizei teilte zu dem Sachverhalt mit, daß gegen eine Personengruppe, zu der der Petent gehörte, ein Platzverweis gem. § 19 PolG ergangen war, zu dessen Durchsetzung es erforderlich gewesen sei, die Personen gem. § 20 Abs. 1 Ziff. 3 PolG in Gewahrsam zu nehmen. Die Personengruppe habe damit den Tatbestand der unerlaubten Ansammlung (§ 113 Gesetz über Ordnungswidrigkeiten - OWiG[66]) erfüllt. Die anschließende ed-Behandlung (hier: Anfertigung eines Lichtbildes) sei gem. § 16 Abs. 2 Ziff. 1 PolG erfolgt.

Ich habe die Erforderlichkeit der ed-Behandlung bestritten, weil sie nach der von der Polizei angegebenen Rechtsgrundlage als Ausnahmeregelung nur für den Fall vorgesehen ist, daß eine nach § 15 PolG zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Diese Voraussetzung war im vorliegenden Fall nicht erfüllt, da der Petent bereits am Festnahmeort ein Ausweisdokument vorgewiesen hatte. Die Erforderlichkeit läßt sich auch nicht mit dem dem Petenten vorgeworfenen Verstoß gegen § 113 OWiG begründen, da der Tatvorwurf keine Straftat betraf. Die Polizei hat sich dieser Auffassung angeschlossen.

Neben der Klärung des Sachverhalts war auch zu prüfen, ob die Polizei sowie andere Sicherheitsbehörden, an die die Unterlagen eventuell zwischenzeitlich übermittelt worden waren, diese nach Einstellung des Verfahrens vernichtet hatten.

Die Überprüfung ergab, daß bei der Polizei keine Unterlagen mehr vorhanden waren. Zuvor hatte die Polizei den Vorgang jedoch gem. § 14 Abs. 2 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[67] an die Brandenburgische Verfassungsschutzbehörde übermittelt (s. unter 3.6.2.3). Damit kamen zum ersten rechtswidrigen Grundrechtseingriff noch weitere. Die Verfassungsschutzbehörde löschte bereits vorhandene Erkenntnisse - ungeachtet der abgelaufenen Aufbewahrungsfrist - nicht, weil die neue relevante Information hinzugekommen war. Dies war für sich genommen zulässig.

66

67 i. d. Fassung vom 19. Februar 1987, BGBl. I S. 602
vom 5. April 1993, GVBl. I S. 78

Da aber bereits die Erhebung der Daten schon ohne ausreichende Rechtsgrundlage erfolgte, war auch die Übermittlung an die Brandenburgische Verfassungsschutzbehörde unzulässig, so daß ich gefordert habe, die Unterlagen zu vernichten. Dem ist die Brandenburgische Verfassungsschutzbehörde nachgekommen.

3.5.7 Stellungnahmen zu Gesetzen und Verwaltungsvorschriften

3.5.7.1 Verbrechensbekämpfungsgesetz

Am 1. Dezember 1994 ist das Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz)[68] in Kraft getreten.

Damit hat die lange Auseinandersetzung über dieses Gesetz mit seinen verfassungs- und datenschutzrechtlich bedenklichen Regelungen für den Bundesnachrichtendienst (BND) ein Ende gefunden. Nachdem sich im Bundesrat noch die Mehrheit der Länder gegen den vom Bundestag verabschiedeten Regierungsentwurf ausgesprochen hatte, einigte man sich im Vermittlungsausschuß doch auf eine Fassung, mit der die bisherigen Nutzungsbeschränkungen der strategischen Telefonüberwachung durch den BND aufgehoben werden.

Bisher war die strategische Telefonüberwachung vom BND durchgeführt worden, um Erkenntnisse über das Ausland von außen- und sicherheitspolitischer Bedeutung zu gewinnen. Das Verbrechensbekämpfungsgesetz legt nun in Art. 12 fest, daß der BND im Rahmen der strategischen Telefonüberwachung auch zur Bekämpfung von Straftaten in den Bereichen Terrorismus, Betäubungsmittel, Geldfälschung und Geldwäsche eingesetzt wird. Diese Regelung verwischt das Trennungsgebot zwischen Polizei und Nachrichtendiensten. Ihm kommt insoweit Verfassungsrang zu, als die Westalliierten im sog. Polizeibrief vom 25. Mai 1949 ihre Zustimmung zum Grundgesetz mit dem Gebot verknüpft haben, daß in der entstehenden Bundesrepublik Deutschland Polizei und Nachrichtendienste klar voneinander getrennte Einrichtungen bleiben müssen, um so zu verhindern, daß je wieder ein staatlicher Machtapparat - wie die Geheime Staatspolizei - entstehen kann.

Zur Telefonkontrolle verwendet der BND einen variablen Katalog von Suchbegriffen, der in Datenbanken abgespeichert ist. Wenn im Verlauf des Ferngesprächs ein in dem Katalog aufgeführter Suchbegriff erwähnt wird, wird das Gespräch automatisch aufgenommen. Die jetzt in Kraft getretenen Regelungen des Verbrechensbekämpfungsgesetzes sehen vor, daß in dem Katalog auch bestimmte, für die Strafverfolgung interessante Suchbegriffe aufgenommen werden. Die so ermittelten Erkenntnisse leitet der BND an die Strafverfolgungsbehörden weiter.

Die Datenschutzbeauftragten haben diese Mitwirkung des BND an der Verbrechensbekämpfung abgelehnt (s. Anlage 7). Sie vertreten die Auffassung, daß die Verbrechensbekämpfung strikt vom Einsatzbereich der Geheimdienste zu trennen ist. Im Gegensatz zu Geheimdiensten sind Strafverfolgungsbehörden einer Vielzahl rechtsstaatlicher Verfahrensregelungen unterworfen, die neben dem Recht des Beschuldigten auf Verteidigung auch dessen Recht auf informationelle Selbstbestimmung sichern. Dazu gehören u. a. der Grundsatz der offenen Datenerhebung, die Benachrichtigung des Betroffenen über besonders intensive Eingriffsmaßnahmen und der Richtervorbehalt. Durch eine Ausdehnung nachrichtendienstlicher Mittel in den Bereich der Verbrechensbekämpfung wird die Trennlinie zwischen Geheimdiensten und Strafverfolgungsbehörden verwischt.

---

68 vom 28. Oktober 1994, BGBl. I S. 3186

3.5.7.2 Bundeskriminalamtgesetz

Im Dezember 1993 hat die Bundesregierung einen ersten Entwurf zu dem Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG) vorgelegt. Unterdessen ist im Bundesrat eine überarbeitete Fassung[69] beraten worden. Im Gegensatz zum Vorentwurf einhält die Bundesratsfassung eine Reihe von Verbesserungen, wie z. B.

- die Beachtung landesgesetzlicher Löschungsfristen,

- einen Einwilligungsvorbehalt für die Speicherung von Daten über Zeugen und mögliche Opfer,

- den Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts",

- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen.

Dies habe ich in meiner Stellungnahme ausdrücklich begrüßt. Dessen ungeachtet bestehen weiterhin schwerwiegende datenschutzrechtliche Bedenken gegen eine Reihe von Vorschriften. Diese richten sich vor allen Dingen auf

- die Befugnisse der Zentralstelle BKA zu selbständigen Datenerhebungen und -übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Berücksichtigung des Verantwortungsbereichs der Länderpolizeien,

- die Vermischung von Befugnissen zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und zur Vorsorge für künftige Strafverfolgung ohne ausreichende Zweckbindung der damit verbundenen Datenverarbeitung,

- die Verwendung des Begriffs "Straftaten von erheblicher Bedeutung", ohne daß im Entwurf definiert ist, welche Tatbestände unter diesem Begriff zu rechnen sind, so daß nicht mehr vorhersehbar ist, wann die - an diesen Begriff anknüpfenden - Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind,

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Festlegung auf den Schutz des sich dort befindenden verdeckten Ermittlers.

Obwohl § 12 BKAG-Entwurf (BKAG-E) die datenschutzrechtliche Verantwortung im INPOL-System grundsätzlich regelt, ist die Vorschrift insgesamt so unklar, daß die datenschutzrechtliche Verantwortung der Stellen in den Ländern, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen, nicht mehr eindeutig festgelegt ist. Nach dem vorliegenden Entwurf sind zwar die anliefernden Stellen für die von ihnen eingegebenen Daten verantwortlich, das BKA kann jedoch sämtliche Daten verändern, nutzen, ergänzen und übermitteln. Hierbei ist es nicht an seine materiellen Aufgaben nach § 3 bis § 5 BKAG-E gebunden, sondern die von diesen Regelungen weitestgehend losgelöste Zentralstellenfunktion ermächtigt das BKA, ohne daß ihm Schranken gesetzt sind, sich über die in den Ländern geltenden Bindungen hinwegzusetzen.

Ebenso wie im Vorentwurf richtet sich auch in diesem die Kontrollzuständigkeit für das

---

69 BR-Drs. 94/95, Stand Februar 1995

INPOL-System allein nach § 24 BDSG. Dagegen habe ich bereits in meiner Stellungnahme zu dem Vorentwurf erhebliche Bedenken vorgetragen[70]. Diese Bedenken sind - trotz einiger Verbesserungen - auch im vorliegenden Entwurf nicht ausgeräumt. Dazu habe ich dem MI einen Änderungsvorschlag zur Beratung im Bundesrat unterbreitet, der von den Datenschutzbeauftragten einiger Bundesländer in einer Arbeitssitzung, an der auch meine Dienststelle teilnahm, abgestimmt worden war.

Das MI hat sich in seiner Antwort auf meine Stellungnahme erfreut darüber gezeigt, daß die Bundesregierung im Verlauf des Gesetzgebungsverfahrens den weitaus überwiegenden Teil der von den Ländern geäußerten Kritik aufgenommen und den Entwurf dementsprechend geändert hat. Es hat auch ausdrücklich klargestellt, daß der vorliegende Gesetzentwurf keine Befugnis zum Einsatz technischer Mittel innerhalb von Wohnungen enthält. Zu den in meiner Stellungnahme angesprochenen Kritikpunkten teilt das MI folgendes mit:

- Das Land Brandenburg hat in der zuständigen Ausschußsitzung eine Fassung des die datenschutzrechtliche Kontrolle im INPOL-System regelnden § 12 Abs. 3 BKAG-E unterstützt, die inhaltlich deckungsgleich mit dem von einigen Datenschutzbeauftragten und mir unterbreiteten Änderungsvorschlag ist.

- Es teilt meine Auffassung, daß die Verwendung des Begriffs "Straftat von erheblicher Bedeutung" äußerst problematisch ist.

- Es vertritt ebenso wie ich die Auffassung, daß das BKA grundsätzlich nicht im Bereich der Gefahrenabwehr tätig werden soll.

- Es hält die Befugnis zur verdeckten Datenermittlung aus Wohnungen zum Schutz des in der Wohnung befindlichen verdeckten Ermittlers für unverzichtbar, meint jedoch, daß die entsprechende Vorschrift in § 16 Abs. 2 BKAG-E anders als vorgesehen gefaßt werden könnte.

3.5.7.3 Errichtungsanordnung zum Kriminalaktennachweis Land Brandenburg (KAN-BB)

Im Zuge der im Berichtszeitraum durchgeführten Bereinigung der Kriminalakten ist auch der automatisierte Kriminalaktennachweis neu gestaltet worden. Das MI hat mich an der Erstellung der Errichtungsanordnung sowie der Dienstanweisung frühzeitig beteiligt.

Der KAN-BB ist ein automatisiertes Verzeichnis von Kriminalakten, die die Polizei des Landes Brandenburg über Verurteilte, Beschuldigte, Verdächtigte oder Gesuchte sowie über Vermißte und über Personen, die der Anlage einer Kriminalakte zugestimmt haben, führt. Daneben gibt es den KAN-Bund, in dem als Bestandteil des Informationssystems der Polizei (INPOL) das Land Brandenburg ebenso wie die anderen Bundesländer und das BKA diejenigen Kriminalakten registriert, die beim Bundeskriminalamt oder bei den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder Tatverdächtige geführt werden. KAN-Bund und KAN-BB ermöglichen die dezentrale Auskunft, bei welchen Polizeidienststellen des Landes Brandenburg, des Bundes oder der Länder Kriminalakten über eine Person geführt werden. Der KAN-BB wird beim BKA als Datenverarbeitung im Auftrag betrieben.

Zum Betrieb des KAN-BB befinden sich in jedem Polizeipräsidium insgesamt fünf INPOL-Endgeräte, die in der Abteilung Einsatz/Ermittlung installiert sind. Der Kriminalaktenhaltung stehen zwei INPOL-Endgeräte zur Verfügung, von denen eines ausschließlich der Erfassung

---

70 s. 2. Tätigkeitsbericht unter 3.7, S. 78

der Altakten (s. 3.5.3.1) dient. In Pkt. 5.1 "Erfassung" der Dienstanweisung KAN-BB und KAN-Bund ist festgelegt, daß die Erfassung zum KAN bei der Polizeibehörde erfolgt, die für die Führung der Kriminalakte zuständig ist. Dabei fällt dem Sachbearbeiter die Aufgabe zu, anhand der jeweiligen Errichtungsanordnung sowie anderer Rechtsgrundlagen zu entscheiden, ob die Daten lediglich im KAN-BB oder auch im KAN-Bund eingestellt werden sollen. Die Belegung eines besonderen Datenfeldes sichert, daß der KAN-BB nur von Polizeidienststellen des Landes Brandenburg abgefragt werden kann. Die technische Realisierung des KAN-BB wird datenschutzrechtlichen Anforderungen gerecht.

In einigen Punkten habe ich jedoch sowohl die Dienstanweisung als auch die Errichtungsanordnung zum KAN-BB kritisiert. In der Dienstanweisung werden dem Sachbearbeiter u. a. Erläuterungen an die Hand gegeben, welche Straftaten als "überregional bedeutsam" einzustufen und damit in den KAN-Bund einzustellen sind. Darunter wird auch die Begehung fremdenfeindlicher Straftaten genannt. Dazu habe ich geltend gemacht, daß im KAN-Bund eine Speicherung einer fremdenfeindlichen Straftat allein wegen dieser Qualität nicht vorgenommen werden darf. Vielmehr müssen immer die allgemeinen Voraussetzungen für die bundesweite Speicherung einer Straftat vorliegen. Erst wenn diese allgemeinen Voraussetzungen zur bundesweiten Speicherung gegeben sind, kann die Tat - ggf. auch die mit einer anderen Straftat - zum Ausdruck kommende Motivation des Straftäters zum Anlaß genommen werden, die Speicherung unter dem Gesichtspunkt "fremdenfeindliche Straftat" im KAN-Bund vorzunehmen. Das MI teilt diese Auffassung. Ich habe vorgeschlagen, diese Problematik in der Schulung der mit der Dateneingabe betrauten Polizeibediensteten anzusprechen.

Sowohl in der Dienstanweisung als auch in der Errichtungsanordnung werden die Datenfelder "Personengebundene Hinweise (PHW)" angesprochen. U. a. können die Hinweise "Ansteckungsgefahr", "Freitodgefahr", "Prostitution" und "Fremdenfeindlich" vergeben werden.

Bei den beiden ersten PHW habe ich darauf hingewiesen, daß die Polizei nur in einer verschwindend geringen Anzahl von Fällen auf rechtmäßigem Weg Kenntnis vom dem zur Vergabe des PHW führenden Sachverhaltes erlangen kann. Informationen, die unter die ärztliche Schweigepflicht (§ 203 StGB) fallen, sind im allgemeinen als polizeifest zu betrachten. Wie die Dienstanweisung zum KAN-BB richtig feststellt, ist eine Durchbrechung der ärztlichen Schweigepflicht nur auf der Grundlage des Bundesseuchengesetzes möglich, so daß beispielsweise ein Hinweis auf eine Aids-Erkrankung (keine meldepflichtige Krankheit gem. § 3 Abs. 1 Bundesseuchengesetz[71]), die in der Vergangenheit häufig als Begründung für die Vergabe des PHW "Ansteckungsgefahr" genannt wurde, nur dann möglich sein dürfte, wenn der Betroffene selbst diese Angabe macht. Entsprechendes gilt für den PHW "Freitodgefahr". Grundsätzlich fällt auch diese Information unter die ärztliche Schweigepflicht, so daß der PHW nur vergeben werden kann, wenn die Information von dem Betroffenen selbst - oder bei vermißten Personen von einem Angehörigen - kommt. Weiterhin ist darauf hinzuweisen, daß der PHW dann wieder zu löschen ist, wenn die Ansteckungs- bzw. Freitodgefahr entsprechend der medizinischen Lehre nicht mehr besteht.

Insgesamt läßt sich feststellen, daß - vorausgesetzt, die Vergabe der PHW's erfolgt nur, wenn die Hinweise rechtmäßig erlangt worden sind - diese nur in so wenigen Fällen vorliegen, daß der Zweck dieser Datenspeicherung nicht erreicht wird. Auch wenn KAN-BB oder KAN-Bund keinen entsprechenden Hinweis enthält, müssen die einschreitenden Polizeibediensteten im Einzelfall ihre Aufgabenerfüllung darauf abstellen, daß bei den Betroffenen Ansteckungs- oder Freitodgefahr bestehen könnte.

---

71 i. d. Fassung vom 18. Dezember 1979, BGBl. I S. 2262

Zum PHW "Prostitution" habe ich ausgeführt, daß nach ihrer Zweckbestimmung die Speicherung von Daten im KAN-Bund bzw. KAN-Land der vorsorgenden Bereitstellung von sächlichen Hilfsmitteln für die Wahrnehmung der Aufgaben dient, die der Polizei zur Erforschung und Aufklärung von Straftaten durch § 163 StPO sowie im übrigen durch § 1 PolG i. V. m. § 1 VGPolGBbg zugewiesen sind.

Entsprechend dieser Zweckbestimmung ergibt sich die Notwendigkeit der Speicherung daraus, ob der festgestellte Sachverhalt nach kriminalistischer Erfahrung angesichts aller Umstände des Einzelfalls Anhaltspunkte für die Annahme bietet, daß der Betroffene künftig oder anderwärts mit guten Gründen als Verdächtiger in den Kreis potentiell Betroffener an einer noch aufzuklärenden strafbaren Handlung einbezogen werden könnte und daß die gespeicherten Daten die dann zu führenden Ermittlungen fördern könnten. Daraus ergibt sich, daß der PHW "Prostitution" nicht nur vergeben werden kann, weil nach allgemeiner polizeilicher Auffassung das Umfeld der Prostitution erheblichen kriminellen Einflüssen ausgesetzt ist. Vielmehr müssen auch hier im Einzelfall die o. g. Voraussetzungen erfüllt sein, um die Vergabe des PHW's zu ermöglichen.

Zum PHW "Fremdenfeindlich" habe ich ausgeführt, daß nicht jede gegen einen Ausländer gerichtete Straftat - auch wenn sie gelegentlich mit ausländerfeindlichen Äußerungen des Täters begleitet wird - mit diesem Hinweis versehen werden darf. Vielmehr muß der Täter mit der Zielrichtung im Kern zum Ausdruck bringen, daß sich die Tat gegen die andere Person (oder eine Sache) richtet, weil er die betroffene Person wegen ihrer Andersartigkeit in Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe usw. treffen will.

In einer Besprechung sind meine Ausführungen zu diesen Punkten erörtert worden. Das Innenministerium hält jedoch - ebenso wie andere Bundesländer - die Speicherung der in Rede stehenden personengebundenen Hinweise für erforderlich und hat sich daher meiner Anregung, sie zu streichen, nicht angeschlossen.

Des weiteren habe ich gefordert, in der Errichtungsanordnung verbindlich festzulegen, daß für alle Neuerfassungen im KAN-BB als erste Aussonderungsprüffrist grundsätzlich ein Jahr vergeben wird. Dieser Anregung ist das MI erfreulicherweise gefolgt.

Das MI hat vorgeschlagen, die Fragen, zu denen noch gegensätzliche Auffassungen bestehen, zu einem späteren Zeitpunkt, nachdem sich die Anwendung in der Praxis bewährt hat, erneut zu diskutieren. Dies begrüße ich ausdrücklich. Insgesamt ist festzustellen, daß datenschutzrechtliche Belange in der Errichtungsanordnung sowie der Dienstanweisung für den KAN-BB im allgemeinen berücksichtigt sind, so daß zu erwarten ist, daß die Datei auf einem angemessenen datenschutzrechtlichen Niveau betrieben wird.

3.6 Verfassungsschutz

3.6.1 Aufgabe der brandenburgischen Verfassungsschutzbehörde

Aufgabe der brandenburgischen Verfassungsschutzbehörde ist es in erster Linie, bestimmte Entwicklungen zu beobachten, die Gefahren für die in § 4 Abs. 3 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[72] aufgezählten Schutzgüter, wie z. B. die im Grundgesetz konkretisierten Menschenrechte, das freie und geheime Wahlrecht oder der Ausschluß jeder Gewalt und Willkürherrschaft, bedeuten können. Schwerpunkt der Aufgabe des Verfassungsschutzes ist somit die politische Feldbeobachtung, die allgemeine Auswertung und Erstellung von Lageberichten und Situationsanalysen, auf deren Grundlage

72 vom 5. April 1993, GVBl. I S. 78

die im Grundgesetz vorgesehenen Verfahren zur Abwehr einer Gefahr für die freiheitlich-demokratische Grundordnung (Art. 5 Abs. 2, Art. 18 und Art. 21 Abs. 2 GG), also Partei- bzw. Vereinsverbote, eingeleitet werden können.

Aus der Aufgabenzuweisung in § 3 Abs. 1 BbgVerfSchG ergibt sich eine prinzipielle Orientierung der Sammlung und Aufbewahrung der Unterlagen an Sachgebieten und an Personenzusammenschlüssen (Bestrebungen). Einzelpersonen sollten im allgemeinen nur dann in das Blickfeld der Verfassungsschutzbehörde treten, als sie durch aktive Unterstützung für einen Personenzusammenschluß handeln bzw. als Einzelpersonen durch Anwendung von Gewalt oder in sonstiger Weise ein Schutzgut des Verfassungsschutzgesetzes erheblich beschädigen (siehe § 4 Abs. 1, 2 und 4 BbgVerfSchG).

Daraus folgt, daß das Informationsaufkommen einschließlich personenbezogener Daten überwiegend in Sachakten abgelegt wird. Nur in Ausnahmefällen erfolgt eine Informationsverarbeitung in Personenakten. Befugnisnorm für grundsätzlich jede Speicherung, Veränderung und Nutzung personenbezogener Daten ist § 8 BbgVerfSchG. § 9 BbgVerfSchG regelt die Speicherung, Veränderung und Nutzung personenbezogener Daten von Minderjährigen. Soweit Informationen über Betroffene, die das 16. Lebensjahr noch nicht vollendet haben, in einer Personenakte gesammelt oder in eine Datei eingestellt werden sollen, gelten strengere Voraussetzungen als bei Erwachsenen bzw. bei Heranwachsenden über 16 Jahren.

3.6.2 Prüfungen bei der brandenburgischen Verfassungsschutzbehörde

Anlaß der Prüfungen, die ich im Berichtsjahr durchgeführt habe, ist die beabsichtigte Einführung des vom Landesamt für Verfassungsschutz (LfV) Hamburg übernommenen Verfahrens "Automation der Referatsarbeitskarteien (RAK)", über die mich der Hamburgische Landesbeauftragte für den Datenschutz informiert hatte. Ziele der Prüfung waren

- die Festlegung datenschutzrechtlicher Kriterien, die bei der Überführung der manuell betriebenen Personenarbeitskartei (PAK) in die automatisierte Referatsarbeitskartei (RAK) berücksichtigt werden sollten sowie

- die Festlegung der technisch-organisatorischen Maßnahmen in dem Verfahren gem. § 10 Bbg DSG.

Die Prüfungen, die noch nicht abgeschlossen sind, dienten in erster Linie dazu,

- einen Überblick über die Prüfungsgegenstände manuelle PAK und über das automatisierte Verfahren (RAK) zu erhalten,

- festzustellen, welche amtsinternen Vorschriften zur Datenverarbeitung in der Verfassungsschutzbehörde angewandt werden, und

- die Hardware und - soweit vorhanden - Software des Verfahrens "RAK" in Augenschein zu nehmen.

3.6.2.1 Technisch-organisatorische Maßnahmen, Stand des Automationsprojekts RAK sowie amtsinterne Vorschriften

Die Überprüfung der technisch-organisatorischen Maßnahmen gem. § 10 Bbg DSG im Zusammenhang mit dem Prüfungsgegenstand gab keinen Anlaß zu datenschutzrechtlichen Bedenken. Die für das Automatisierungsvorhaben benötigte Hard- bzw. Software stand zwar unterdessen zur Verfügung, in das Verfahren selbst waren aber noch keine Datensätze eingegeben worden. Amtsinterne Vorschriften zur Datenverarbeitung sind in der

Verfassungsschutzbehörde bislang noch nicht erstellt worden. Es besteht jedoch Einvernehmen darüber, daß solche Vorschriften mit der Arbeitsaufnahme des Automatisierungsprojekts zur Verfügung stehen müssen, um eine datenschutzgerechte Informationsverarbeitung zu garantieren.

3.6.2.2 Grundsätzliche Probleme zur Einstellung in die PAK

Vor dem Hintergrund der geplanten Automation habe ich meine ersten Prüfungen zunächst auf die PAK beschränkt und bei Mängelfunden die Verfassungsschutzbehörde gebeten, den Sachverhalt anhand der Akte zu prüfen und mir zu erläutern. Mit der Verfassungsschutzbehörde besteht Einvernehmen darüber, daß alle Registrierungen in der PAK geprüft werden müssen, ob sie zur Aufgabenerfüllung noch erforderlich sind, ehe sie in die RAK eingestellt werden.

In der Frage, welche Voraussetzungen vorliegen müssen, damit Daten über einzelne Personen aus Sachakten herausgezogen und mit Hinweisen zu den vorhandenen Erkenntnissen in die PAK eingestellt werden, ließ sich noch kein grundsätzliches Einverständnis mit der Verfassungsschutzbehörde erzielen. Diese Frage ist jedoch für den Inhalt der Datei RAK von Bedeutung, da grundsätzlich dieselben Informationen, die jetzt in der PAK zur Verfügung stehen, in die RAK aufgenommen werden sollen. Mit Verweis auf § 8 BbgVerfSchG führt die Verfassungsschutzbehörde an, daß diese Rechtsgrundlage grundsätzlich jede Form der Speicherung zuläßt. Sie macht darüber hinaus geltend, daß die PAK nichts anderes als einen erweiterten Aktenfundstellennachweis mit stark verkürzten schlagwortartigen Zusammenfassungen der zu der betreffenden Person in Sachakten vorhandenen Informationen darstellt. Vor allen Dingen aber hat die Verfassungsschutzbehörde betont, daß aus der PAK grundsätzlich keine Informationen verwendet oder gar übermittelt werden. Die Sachbearbeitung erfolge ausschließlich auf der Grundlage der Vorgangsakte.

Ich habe demgegenüber angeführt, daß durch das Anlegen einer Karteikarte der Betroffene aus der Masse der personenbezogenen Informationen einer Sachakte herausgehoben wird. Dieses "Herausheben" stellt einen tieferen Eingriff in die Persönlichkeitsrechte der Betroffenen dar, der einer höheren Voraussetzungsschwelle bedarf, als die Registrierung in einer Sachakte. Daher bin ich der Meinung, daß "Mitläufer" bzw. Begleit- und Kontaktpersonen sowie Personen, die nur einmal in Erscheinung getreten sind, wenn überhaupt nur mit sehr kurzen Speicherungsfristen in die PAK eingestellt werden sollten. Ich teile die Auffassung der Verfassungsschutzbehörde, daß § 8 BbgVerfSchG grundsätzlich jede Form der Speicherung zuläßt. Dennoch muß vor jedem Anlegen einer Karteikarte zu einem Betroffenen geprüft werden, ob diese Maßnahme den Verhältnismäßigkeitsgrundsatz nicht verletzt. Anhaltspunkte dazu finden sich nicht nur in dem vorstehend erwähnten § 8, sondern auch in § 4 Bbg VerfSchG in den Begriffsbestimmungen verfassungsschutzrelevanter Bestrebungen bzw. Einzelpersonen. Wenn schon die dem Informationseingriff zugrunde liegende Verfassungsschutzrelevanz eines Personenzusammenschlusses im Regelfall an die Voraussetzung "gewaltbereit" oder "kämpferisch aggressiv" (siehe § 4 Abs. 2 BbgVerfSchG) geknüpft ist, müssen diese Eingriffsschwellen - neben der "aktiven Unterstützung" (siehe § 4 Abs. 4 BbgVerfG) -erst recht bei der Verkartung eines Betroffenen erreicht sein.

Ergibt die Abwägung, daß der Erkenntnisstand über einen Betroffenen die Aufnahme in die PAK rechtfertigt, müssen Verfahrensvorkehrungen zum Grundrechtsschutz - wie regelmäßige Erforderlichkeitsprüfung und Löschungsverpflichtung - getroffen werden.

Dies stellt hohe Anforderungen an die Bestandspflege der PAK, die mit vertretbarem Verwaltungsaufwand bei einer manuell geführten Kartei nur schwer leistbar sind. Kurzfristige regelmäßige Erforderlichkeitsprüfungen sowie Vernichtung der nicht mehr erforderlichen Karteikarten sind jedoch nicht nur datenschutzrechtlich unabdingbare Vorkehrungen: Die Führung einer PAK macht nur Sinn, wenn die Sammlung aus gesicherten und nachgeprüften Erkenntnissen besteht.

Bei der Prüfung habe ich im oben ausgeführten Zusammenhang Mängel bei der PAK festgestellt und der Verfassungsschutzbehörde mitgeteilt, daß - ungeachtet ihrer Funktion als Aktenfundstelle - die PAK in der gegenwärtigen Form nur für den Zeitraum bis zur endgültigen Arbeitsaufnahme der RAK hinnehmbar ist.

3.6.2.3 Problematische Erkenntnisgewinnung

Im Zusammenhang mit der Prüfung der PAK habe ich die Erkenntnisgewinnung der Verfassungsschutzbehörde aus Festnahmelisten und Halterabfragen problematisiert. Gem. § 14 BbgVerfSchG übermittelt die Polizei Informationen "von sich aus" (Abs. 2) oder "auf Ersuchen" (Abs. 3) an die Verfassungsschutzbehörde. Zu solchen Informationen gehören u. a. die sog. "Festnahmelisten".

Auf diesen Listen werden alle vorläufig Festgenommenen registriert. Das Polizeirecht befugt die Polizei, im Rahmen der Gefahrenabwehr eine Person festzunehmen, wenn eine Platzverweisung anders nicht durchzusetzen ist. Von diesem Instrument wird bei gewalttätigen Auseinandersetzungen während oder im Anschluß an Demonstrationen häufig Gebrauch gemacht. In der Mehrheit handelt es sich bei den vorläufig Festgenommenen um Personen, die keiner Ordnungswidrigkeit oder Straftat verdächtigt werden. Festnahme und Personalienfeststellung sowie die Registrierung in den Festnahmelisten erfolgt lediglich aufgrund der Tatsache, daß die Betroffenen vor Ort waren. Andere Sachverhalte, wie z. B. ein bestimmter Tatvorwurf oder ein Tatverdacht, sind den Festnahmelisten in der Regel nicht zu entnehmen.

Diese Übermittlung der Festnahmelisten an die Verfassungsschutzbehörde wirft datenschutzrechtliche Probleme auf. Wenn die Verfassungsschutzbehörde die Festnahmelisten zur Grundlage einer eigenen Informationsverarbeitung über die Betroffenen gem. § 8 BbgVerfSchG nimmt, besteht die Gefahr, daß damit nicht Informationen über eine verfassungsschutzrelevante Bestrebung zur Aufgabenerfüllung gem. § 3 Abs. 1 Nr. 1 BbgVerfSchG gesammelt und ausgewertet werden, sondern das mehr oder minder breite Spektrum kritischer und seine Kritik aktiv äußernder Bürger. Erst durch weitere Aufklärungsarbeit ist diejenige Gruppe von Demonstrationsteilnehmern, die nicht nur einen gesellschaftlichen Mißstand anprangern will, sondern auch andere - evtl. verfassungsschutzrelevante - Ziele verfolgt, von denjenigen Personen zu trennen, die "nur" von ihrem Grundrecht auf Demontrations- und Versammlungsfreiheit Gebrauch machen. Letztere fallen nicht mehr in den Aufgabenbereich der Verfassungsschutzbehörde. Hier sei wiederum auf § 3 Abs. 1 Satz 2 BbgVerfSchG verwiesen, der für ein Tätigwerden der Verfassungsschutzbehörde das Vorliegen tatsächlicher Anhaltspunkte voraussetzt. Grundsätzlich habe ich bezweifelt, daß Festnahmelisten dieser gesetzlichen Vorschrift genügen. Wird die Verfassungsschutzbehörde dennoch im Einzelfall auf der Grundlage der Festnahmelisten tätig, so ist dies nur hinzunehmen, wenn innerhalb einer kurzen Überprüfungsfrist tatsächliche Anhaltspunkte für einen verfassungsschutzrelevanten Sachverhalt gefunden werden.

Erkenntnisse aus Halterabfragen gelangen auf verschiedenen Wegen zur Verfassungsschutzbehörde. Zum einen befugt § 14 Abs. 3 BbgVerfSchG die Behörde selbst zu Halterabfragen. Gem. § 15 BbgVerfSchG darf sie unter bestimmten Voraussetzungen aber auch in amtlich geführte Register, wie z. B. Fahrzeugregister, einsehen. Datenlieferant kann aber auch die Polizei sein. Hat sie bei einschlägigen Anlässen durch eine Abfrage die Fahrzeughalter festgestellt, gibt sie diese auf der Rechtsgrundlage des § 14 Abs. 2 oder 3 BbgVerfSchG an den Verfassungsschutz weiter.

Dessen ungeachtet ist die Halterabfrage eine datenschutzrechtlich problematische Erkenntnisquelle. Da bei einer Halterabfrage nur zweifelsfrei feststeht, daß ein auf diesen Halter zugelassenes Fahrzeug an einem bestimmten Ort abgestellt war und damit noch nicht erwiesen ist, ob der Halter tatsächlich bei dem fraglichen verfassungsschutzrelevanten

Ereignis war, kann diese Information von der Verfassungsschutzbehörde allenfalls dann gesammelt werden, wenn schon andere Erkenntnisse über den Halter vorliegen.

§ 3 Abs. 1 Satz 2 BbgVerfSchG knüpft ein Tätigwerden der Behörde an das Vorliegen tatsächlicher Anhaltspunkte. Diese Voraussetzung muß bei jedem Tätigwerden - also auch bei einzelnen Schritten der Informationsverarbeitung - vorliegen. Ergibt schon die Prüfung der Veranstaltung keine tatsächlichen Anhaltspunkte für eine Handlung, die ein Schutzgut des Verfassungsschutzgesetzes verletzt, muß nach meiner Auffassung die Speicherung von personenbezogenen Daten im Zusammenhang mit dem Ereignis unterbleiben, selbst wenn über einen dabei festgestellten Halter bereits Erkenntnisse beim Verfassungsschutz vorliegen.

Meiner Auffassung hat sich die Verfassungsschutzbehörde nicht angeschlossen. Es besteht jedoch Einvernehmen darüber, daß grundsätzlich Erkenntnisse aus Halterabfragen für sich allein nicht zur Aufnahme in die PAK führen. Nur in eng definierten Ausnahmefällen wird von dem Grundsatz abgewichen. Datenschutzrechtlich hinnehmbar ist die Informationserhebung mittels Halterabfrage nur, wenn die daraus gewonnenen Erkenntnisse mit kurzen Speicherungsfristen registriert werden.

3.6.2.4 Unterstützungsunterschriften für eine Partei anläßlich der Wahl zum Europaparlament am 12.05.1994

Bei der Prüfung der PAK fand ich auf mehreren Karteikarten den Eintrag, daß die Betroffenen Unterstützungsunterschriften für eine bestimmte Partei anläßlich der Europawahl am 12.05.1994 geleistet hatten. Dies habe ich gegenüber dem Ministerium des Innern als schweren Verstoß gegen das Wahlgeheimnis beanstandet.

Zum Hintergrund: Parteien oder Wählergemeinschaften, die in der abgelaufenen Wahlperiode nicht in der zur Wahl anstehenden Volksvertretung (auf Europa-, Bundes- oder Landesebene) vertreten waren bzw. die erstmalig zu einer Wahl zugelassen werden wollen, benötigen dafür ein gesetzlich festgelegtes Quorum der Wahlberechtigten in den einzelnen Wahlbezirken. Dazu legen sie öffentlich Listen aus, in die sich diejenigen Wahlbürger mit Name, Anschrift und Unterschrift eintragen, die die Zulassung zur Wahl unterstützen. Die Partei bzw. Wählergemeinschaft leitet diese Listen an den Wahlleiter weiter, der einen Abgleich mit den Wählerlisten veranlaßt. Dadurch wird sichergestellt, daß bei der Ermittlung des erforderlichen Quorums nur solche Unterschriften gezählt werden, die von Wählern des Wahlkreises geleistet worden sind. Das Verfahren ist in den Wahlgesetzen bzw. den Wahlordnungen geregelt.

Rechtsgrundlage für die Europawahl ist das Europawahlgesetz (EuWG)[73] bzw. die Europawahlordnung[74]. § 82 Abs. 3 der - auf der Grundlage des § 25 Abs. 2 EuWG erlassenen - Europawahlordnung legt abschließend fest, zu welchen Zwecken Auskunft aus den Listen bzw. Formblättern der Unterstützungsunterschriften erteilt werden darf. Danach ist sie nur zur Durchführung der Wahl oder eines Wahlprüfungsverfahrens oder zur Aufklärung des Verdachts einer Wahlstraftat zulässig. Zwecke, die der Aufgabenerfüllung der Verfassungsschutzbehörde dienen, fallen somit nicht darunter. § 83 Abs. 3 Europawahlordnung bestimmt, daß diese Listen sechs Monate nach der Wahl zu vernichten sind. Damit kann das EuWG nicht als Rechtsgrundlage für die Übermittlung von Formblättern mit Unterstützungsunterschriften bzw. von Angaben daraus an die Verfassungsschutzbehörde herangezogen werden.

Ist aber bereits die Übermittlung von Informationen aus den Wahlunterlagen an die

---

[73]

[74] vom 12. März 1994, BGBl. I S. 423
vom 10. Mai 1994, BGBl. I S. 957

Verfassungsschutzbehörde unrechtmäßig, so ist es zwangsläufig auch die Aufbewahrung durch die Verfassungsschutzbehörde. Als spezialgesetzliche Norm geht das EuWG dem Verfassungsschutzgesetz vor, so daß weder § 14 BbgVerfSchG als Übermittlungsgrundlage, noch § 8 BbgVerfSchG als Speicherungs-, Veränderungs- und Nutzungsregelung in Betracht kommen. Bei den Informationen aus den Unterstützungslisten, die im übrigen nicht von einer Wahlbehörde stammten, handelte es sich um unrechtmäßige Daten, die die Verfassungsschutzbehörde nicht in die PAK einstellen durfte. Sie hätte sie vielmehr sofort nach Erhalt vernichten müssen.

Ungeachtet seiner weiten Befugnisse ist der Verfassungsschutz nicht außerhalb Art. 20 Abs. 3 GG gestellt, der die vollziehende Gewalt an Gesetz und Recht bindet. Eine Ausformung dieses Verfassungsgrundsatzes findet sich in § 6 Abs. 1 BbgVerfSchG.

Die Auffassung der Verfassungsschutzbehörde, daß nicht die Abgabe der Unterstützungsunterschrift durch die Betroffenen Zweck der Speicherung gewesen sei, sondern die daraus und aus anderen Erkenntnissen abgeleitete Unterstützung einer verfassungsschutzrelevanten Partei oder Wählergemeinschaft, und daß die Speicherung daher zulässig sei, vermag ich nicht zu teilen. Das Wahlgeheimnis genießt als eine der drei Säulen demokratischer Wahlen einen so hohen Stellenwert, daß in die Verfassungsgarantie seiner Unverletzlichkeit nur unter den o. g. Voraussetzungen eingegriffen werden darf. Soweit ein einzelner Wähler verfassungsfeindliche Ziele verfolgt, kann ihm unter bestimmten Voraussetzungen das Wahlrecht aberkannt werden. Sein Wahlgeheimnis bleibt im übrigen jedoch gewahrt.

Ich sehe daher in dem vorliegenden Fall einen schwerwiegenden Verstoß gegen das im Grundgesetz an verschiedenen Stellen (Art. 28 Abs. 1 sowie Art. 38 Abs. 1 GG) garantierten Wahlgeheimnisses, das natürlich auch für Europawahlen gilt, da es zum Wesensgehalt demokratischer Grundsätze gehört, zu deren Verwirklichung in einem vereinten Europa sich die Bundesrepublik Deutschland in Art. 23 Abs. 1 GG verpflichtet hat. Angesichts so vielfältiger Grundgesetzgarantien vermag ich mich der Auffassung der brandenburgischen Verfassungsschutzbehörde nicht anzuschließen, daß es sich hier nicht um einen Verstoß gegen das Grundgesetz handle, weil der von mir angeführte Art. 38 Abs. 1 GG "nur" das Wahlgeheimnis bei Bundestagswahlen gewährleiste.

Trotz der unterschiedlichen Rechtsauffassung hat die brandenburgische Verfassungsschutzbehörde die Eintragungen gelöscht bzw. die Karteikarten sowie den dazugehörigen Aktenrückhalt vernichtet und die Zusicherung gegeben, solche oder ähnliche Informationen in Zukunft nicht mehr zu verarbeiten.

3.6.3 Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg (G 10 AG Bbg)

Das Ministerium des Innern (MI) hat mir einen weiteren Entwurf zu dem o. g. Gesetz, der im großen und ganzen mit dem ersten Entwurf identisch ist, zugeleitet. Meine Änderungsvorschläge sind mit einer Ausnahme in dem neuen Entwurf nicht aufgegriffen worden[75]. Nur im Zusammenhang mit der Unterrichtung der G 10-Kommission ist eine Regelung vorgesehen, die im Vergleich zum Vorentwurf eine datenschutzrechtliche Verbesserung darstellt.

Ursprünglich war vorgesehen, daß das Ministerium des Innern die G 10-Kommission erst innerhalb von drei Monaten, nach dem die Überwachungsmaßnahme beendet worden ist, unterrichtet, ob der Betroffene über die gegen ihn durchgeführte Überwachungsmaßnahme

75 s. 2. Tätigkeitsbericht unter 3.5.5, S. 59

informiert werden soll oder nicht. Im neuen Entwurf ist nunmehr geregelt, daß der Sachverhalt bei der auf die Einstellung der Maßnahme folgenden Sitzung der G 10-Kommission dargelegt wird, spätestens jedoch innerhalb von drei Monaten, gerechnet vom Zeitpunkt der Beendigung.

Für die Betroffenen ist diese verbesserte Regelung nicht unerheblich, da die G 10-Kommission entscheidet, ob er von der gegen ihn ergangenen Überwachungsmaßnahme erfährt. Ungeachtet evtl. noch bestehender Bedenken, ist das Ministerium des Innern nämlich verpflichtet, den Beschluß der G10-Kommission auszuführen und den Betroffenen zu unterrichten.

Bereits in meiner ersten Stellungnahme habe ich die Auffassung vertreten, daß sich meine Kontrollkompetenz auch auf die durch die Eingriffe in das Brief-, Post- und Fernmeldegeheimnis erhobenen Daten erstreckt, da sie Verfassungsrang (Art. 74 Verfassung des Landes Brandenburg) hat. Ich habe vorgeschlagen, dies auch im vorliegenden Gesetz klarzustellen. In ihrer Stellungnahme der Landesregierung zu meinem 2. Tätigkeitsbericht hat die Landesregierung[76] diese Auffassung mit Verweis auf § 25 Abs. 4 BbgVerfSchG zurückgewiesen. Dem kann ich nicht folgen.

Die Überwachung des Post- und Fernmeldeverkehrs ist ein tiefer Eingriff in das Persönlichkeitsrecht der Betroffenen, bei dem unvermeidlich besonders sensible Informationen aus dem engsten Persönlichkeitsbereich nicht nur über die Zielperson, sondern auch über eine Vielzahl von Unbeteiligten anfallen. Als verdeckte Maßnahme, von der - wenn überhaupt - die Betroffenen erst nach Abschluß der gegen sie durchgeführten Überwachungsmaßnahmen informiert werden, sind besondere Schutzvorkehrungen des Rechts auf informationelle Selbstbestimmung der Betroffenen erforderlich. Insbesondere gilt dies für denjenigen Personenkreis, der wegen eines fortdauernden überwiegenden Allgemeininteresses nicht über die gegen sie ergangenen Maßnahmen informiert wird, so daß ihm auch nachträglich der Rechtsweg nicht offensteht. Nicht zuletzt für solche Fälle treffen die Ausführungen des Bundesverfassungsgerichts zu, daß "wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten ... und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen (ist), die Beteiligung unabhängiger Datenschutzbeauftragten von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" ist[77]. Die Auffassung, daß auch der G 10-Bereich der Kontrolle der Datenschutzbeauftragten unterliegt, wird durch den Beschluß des Bundesverfassungsgerichts vom 20. Juni 1984[78] bestätigt. Hier werden ausdrücklich auch die Datenschutzbeauftragten benannt, deren Kontrollrechte den Grundrechtseingriff einer Überwachungsmaßnahme nach G 10 verfassungsrechtlich hinnehmbar machen.

§ 25 Abs. 4 BbgVerfSchG schließt die aus der Brandenburgischen Verfassung sowie § 23 Abs. 1 Bbg DSG hergeleiteten Kontrollbefugnisse für Maßnahmen nach G 10 nicht aus. § 25 BbgVerfSchG regelt vielmehr die Kontrollrechte der parlamentarischen Kontrollkommission und legt in Abs. 4 fest, daß ihr kein Kontrollrecht über den G 10-Bereich zusteht. Der Systematik des § 25 BbgVerfSchG ist nicht zu entnehmen, daß der Gesetzgeber die Ausgrenzung des G 10-Bereiches aus den Kontrollrechten der parlamentarischen Kontrollkommission auch auf die Kontrollrechte des Brandenburgischen Datenschutzbeauftragten erstrecken wollte.

---

[76]

[77] LT-Drs. 2/169

[78] BVerfGE 65, 1 (46)
BVerfGE 67, 157 (185)

Soweit meine Aufgaben in der in Rede stehenden Bestimmung überhaupt Erwähnung finden, wird dadurch im Gegenteil die Ausdehnung meiner Kontrollbefugnisse auf die Verfassungsschutzbehörde bestärkt: § 25 Abs. 5 BbgVerfSchG legt nämlich fest, daß die parlamentarische Kontrollkommission den Landesbeauftragten ersuchen kann, Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachzugehen.

Im Hinblick auf die jüngste Vergangenheit und die Erfahrungen der brandenburgischen Bürger mit verdeckten Überwachungsmaßnahmen stünde es dem Brandenburgischen Gesetzgeber gut an, bei den Regelungen zur Überwachung des Brief-, Post- und Fernmeldegeheimnisses die Kontrolle der damit verbundenen Daten durch den Datenschutzbeauftragten ausdrücklich vorzusehen.

3.7 Landesaufnahmegesetz

Seit einem Jahr befindet sich der Entwurf eines Landesaufnahmegesetzes in der Ressortabstimmung, der - einschließlich der damit verbundenen Verarbeitung personenbezogener Daten - das Verfahren der Aufnahme und vorläufigen Unterbringung von Spätaussiedlern und Ausländern, die im Rahmen humanitärer Hilfsaktionen aufgenommen werden, endlich auf eine gesetzliche Grundlage stellen soll. Während die in dem Entwurf vorgesehene Regelung zur Datenverarbeitung bereits im vergangenen Jahr vom MI mit mir abgestimmt wurde, verzögern nunmehr neu vorgebrachte Einwendungen des Ministeriums für Arbeit, Soziales, Gesundheit und Frauen zu den Kostenregelungen des Entwurfs das Gesetzgebungsverfahren. Aus datenschutzrechtlicher Sicht ist jedoch eine gesetzliche Aufgabenbestimmung als Voraussetzung jeglicher Befugnis zur Datenverarbeitung dringend zu fordern. Deshalb sollte die Landesregierung die Frage prüfen, ob die abschließende Regelung der Kostenfrage nicht ggf. auch einer Rechtsverordnung vorbehalten und so das Gesetzgebungsverfahren zügig zum Abschluß gebracht werden kann.

3.8 Verwaltungsvorschriften zum Ausländergesetz

Die §§ 75 bis 77 Ausländergesetz (AuslG)[79] enthalten grundlegende bereichsspezifische Regelungen zur Verarbeitung personenbezogener Daten in Verfahren nach dem Ausländergesetz; die Konkretisierung der entsprechenden Befugnisse hat der Gesetzgeber dabei dem Bundesminister des Innern nach Maßgabe von § 104 AuslG überlassen. Dieser vermochte jedoch auch im Februar 1995 noch immer keinen Zeitpunkt abzusehen, zu dem mit dem Inkrafttreten bundeseinheitlicher Verwaltungsvorschriften gerechnet werden kann.

Festzustellen ist, daß der Datenschutzstandard für Ausländer praktisch in allen Bereichen deutlich hinter dem für deutsche Staatsbürger erreichten Niveau zurückbleibt. Dies kann im Hinblick darauf, daß das Grundrecht auf informationelle Selbstbestimmung für jedermann gilt, nicht hingenommen werden. Erforderlich ist es vielmehr, auch für Ausländer eine größtmögliche Transparenz der mit der Durchführung ausländerrechtlicher Bestimmungen verbundenen Datenverarbeitung zu erreichen.

Um das fortbestehende gesetzliche Regelungsdefizit bei der Ausführung des Ausländergesetzes wenigstens in gewissem Umfang auszugleichen, habe ich dem Ministerium des Innern vorgeschlagen, aufgrund der Untätigkeit des Bundes eigenverantwortlich vorläufig geltende Verwaltungsvorschriften in Kraft zu setzen, wie dies

---

79 vom 9. Juli 1990, BGBl. I S. 1354, zul. geänd. durch Gesetz vom 28. Oktober 1994, BGBl. I S. 3186

in den Ländern Berlin und Hessen bereits geschehen ist. Nachdem das Ministerium dies zunächst nicht für erforderlich gehalten hatte, hat es mir nunmehr auf einen erneuten Vorstoß meinerseits hin mitgeteilt, daß es meinen Vorschlag zur Zeit durchaus aufgeschlossen prüfe.

3.9 Statistik

3.9.1 Grundsätze des Datenschutzes bei statistischen Erhebungen

In der Vergangenheit bin ich mehrfach von Bürgern darauf angesprochen worden, ob sich denn Erhebungen für die amtliche Statistik mit Auskunftspflicht überhaupt mit dem Datenschutz vereinbaren ließen. Besonders die Befragungen nach dem Mikrozensusgesetz[80] und der Gebäude- und Wohnungszählung 1995 nach dem Wohnungsstatistikgesetz[81] haben Irritationen hervorgerufen. Die zahlreichen Anfragen geben Anlaß zu einigen grundsätzlichen Hinweisen.

Nach Maßgabe der Ausführungen des Bundesverfassungsgerichts im sog. Volkszählungsurteil[82] umfaßt das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz garantierte allgemeine Persönlichkeitsrecht die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Aber eben nur grundsätzlich und nicht schrankenlos. Dies bedeutet: der einzelne muß Einschränkungen seines Rechts auf informationelle Selbstbestimmungsrecht im überwiegenden Allgemeininteresse hinnehmen. Dazu zählen grundsätzlich auch das öffentliche Informations- und staatliche Planungsinteresse, denen die Durchführung von amtlichen Statistiken dient.

An die gesetzlichen Bestimmungen, auf deren Grundlage der informationellen Selbstbestimmung des einzelnen Schranken gesetzt werden können, hat das Bundesverfassungsgericht jedoch eine Reihe von Anforderungen gestellt, aus denen sich für den Bereich der Statistik folgendes ergibt:

- Die Einschränkungen müssen normenklar sein, d. h., der Zweck einer Statistik muß eindeutig definiert und verständlich sein.

- Der Grundsatz der Verhältnismäßigkeit muß gewahrt bleiben, d. h. die zu erhebenden Angaben müssen für den angestrebten Zweck geeignet und erforderlich sein.

- Der Gesetzgeber muß organisatorische und verfahrensrechtliche Vorkehrungen treffen, die der Gefahr der Verletzung des Persönlichkeitsrechts entgegenwirken. Dazu gehören schriftliche Aufklärungs- und Belehrungspflichten, die der Gesetzgeber dem Auskunftpflichtigen schuldig ist[83]. Dazu gehört auch die Abtrennung der sog. Hilfsmerkmale wie z. B. Name, Vorname, Anschrift usw., die eine Erhebungsstelle oder das Landesamt für Datenverarbeitung und Statistik für Kontrollzwecke kurzzeitig benötigt, von den eigentlichen statistischen Angaben und die möglichst frühzeitige Löschung der

---

80 Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt vom 10. Juni 1985, BGBl. I S. 955, i. d. Fassung vom 17. Dezember 1990, BGBl. I
81 S. 2837

82 vom 18. März 1993, BGBl. I S. 337

83 BVerfGE 65, 1 (1)

BVerfGE 65, 1 (59)

Hilfsmerkmale. Erhebungsbeauftragte, die bei einer statistischen Zählung eingesetzt werden, müssen vertrauenswürdig und auf das Statistikgeheimnis verpflichtet sein. Und der statistische Fragebogen, den der Bürger beantworten soll, muß mit dem jeweiligen konkreten Statistikgesetz übereinstimmen.

- Weitere Schutzmaßnahmen sind die Aktivitäten unabhängiger Kontrollinstanzen (Datenschutzbeauftragte)[84] und der Grundsatz der Trennung von Statistik und Verwaltungsvollzug[85].

Statistische Erhebungen müssen, auch wenn sie während der Durchführung der Erhebung zunächst noch personenbezogene Daten erfassen (was nicht immer der Fall sein muß), im Verlaufe der weiteren Datenverarbeitung stets zu anonymen Daten führen, "so daß im Ergebnis die Erstellung von "Bildern" mit Persönlichkeitsbezug auch in der Form von Teilbildern unzulässig ist"[86]. Insofern sind statistische Erhebungen und Erhebungen von personenbezogenen Daten für den Verwaltungsvollzug zwei verschiedene Dinge. Für die Verwaltung ist gerade die Personenbeziehbarkeit unabdingbar. Für die Statistik gelten dagegen Statistikgeheimnis, Gebot der Anonymisierung, Verbot der Reanonymisierung und Nachteilsverbot. Personenbezogene Daten sind nur "Hilfsmerkmale", die möglichst frühzeitig zu löschen sind[87].

Im Bundesstatistikgesetz (BStatG)[88], dem "Grundgesetz" der amtlichen Statistik, wird in § 1 die Notwendigkeit amtlicher statistischer Erhebungen wie folgt begründet: "Durch die Ergebnisse der Bundesstatistik werden gesellschaftliche, wirtschaftliche und ökologische Zusammenhänge für Bund, Länder einschließlich Gemeinden und Gemeindeverbände, Gesellschaft, Wissenschaft und Forschung aufgeschlüsselt. Die Bundesstatistik ist Voraussetzung für eine am Sozialstaatsprinzip ausgerichtete Politik".

Das Bundesverfassungsgericht[89] führt dazu aus, daß für die Funktionsfähigkeit der amtlichen Statistik ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig sei. Dieses Ziel könne aber nur erreicht werden, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner für statistische Zwecke erhobenen Daten geschaffen werde, ohne die seine Bereitschaft, wahrheitsgemäße Angaben zu machen, nicht herzustellen sei. Eine Staatspraxis, die sich nicht um die Bildung eines solchen Vertrauens bemühe, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Mißtrauen entstünde: "Kann damit nur durch eine Abschottung der Statistik die Staatsaufgabe "Planung" gewährleistet werden, ist das Prinzip der Geheimhaltung und möglichst frühen Anonymisierung der Daten nicht nur zum Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für die Statistik selbst konstitutiv"[90].

Der Bundesgesetzgeber hat in § 26 BStatG bestimmt, daß Statistikstellen nur dann

---

84

85 BVerfGE 65, 1 (60)

86 BVerfGE 65, 1 (62)

87 BVerfGE 65, 1 (53 f.)

88 s. auch BVerfGE 65, 1 (62)

89 vom 22. Januar 1987, BGBl. I S. 462 und 565, i. d. Fassung vom 17. Dezember 1990, BGBl. I S. 2837

90 BVerfGE 65, 1 (50)

BVerfGE 65, 1 (51)

Bundesstatistiken durchführen dürfen, "wenn bei der beauftragten Stelle die Trennung der mit der Durchführung statistischer Aufgaben befaßten Organisationseinheit von den anderen Aufgabenbereichen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist". D. h., es besteht ein striktes Trennungsgebot von Statistik und Verwaltungsvollzug ("informationelle Gewaltenteilung"[91]). Durch diese Abschottung wird auch vermieden, daß der Bürger durch wahrheitsgemäße Angaben bei statistischen Erhebungen Nachteile hat.

Neben der amtlichen Statistik mit Auskunftspflicht, bei der übrigens je nach der konkreten Statistik Einzelfragen auch freiwillig beantwortet werden können, gibt es andere Statistiken, die ausschließlich auf der Basis von Freiwilligkeit erstellt werden. Hier hat der Bürger die volle Möglichkeit, sein Recht auf informationelle Selbstbestimmung ohne Einschränkung auszuüben; er bleibt selbst Herr seiner personenbezogenen Daten: entweder gibt er sie preis oder nicht. Allerdings ist auch hier jede öffentliche Verwaltung gut beraten, sich bezüglich der Datenerhebung - insbesondere was Zweckbindung und Verhältnismäßigkeit anbelangt - den Grundsätzen der amtlichen Statistik verpflichtet zu fühlen. Alle übrigen Maßnahmen zum Schutz des Statistikgeheimnisses gelten ohnehin. Hier macht auch das Bundesstatistikgesetz in § 17 (Unterrichtung des Betroffenen) keinen Unterschied zwischen statistischen Erhebungen mit oder ohne Auskunftspflicht. Ufern Statistiken etwa auf kommunaler Ebene in bezug auf Häufigkeit und Datenumfang aus, entsteht die Gefahr, daß beim Bürger die Akzeptanz ganz schwindet, sich statistischen Erhebungen zu stellen. Damit wäre dann nicht nur die Repräsentativität der kommunalen Erhebung auf freiwilliger Basis, sondern möglicherweise überhaupt die amtliche Statistik mit Auskunftspflicht gefährdet.

Das Bundesverfassungsgericht erachtet es für wichtig, daß sich der Gesetzgeber vor künftigen Entscheidungen zu statistischen Erhebungen mit der jeweils aktuellen statistischen und sozialwissenschaftlichen Methodendiskussion auseinandersetzt[92]. Als Tendenz ist dabei eine geringere Belastung des Bürgers bezüglich seines Rechtes auf informationelle Selbstbestimmung vorgegeben. Dies ist ein wichtiger Gesichtspunkt, weil nämlich prinzipiell "Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist"[93].

Das Recht des einzelnen auf informationelle Selbstbestimmung und die staatliche Schutzverpflichtung hat der Landesverfassungsgeber ausdrücklich in die Verfassung des Landes Brandenburg[94] übernommen. Bis zum Inkrafttreten eines Brandenburgischen Statistikgesetzes (s. unter 3.9.2) gelten für die Durchführung von Landes- und Kommunalstatistiken das Bundesstatistikgesetz und das Brandenburgische Datenschutzgesetz.

Die Praxis unterscheidet zwischen Primär- und Sekundärstatistik. Während eine Primärstatistik stets die Datenerhebung bei Auskunftspflichtigen ausschließlich zum Zweck der Erstellung von Statistiken voraussetzt, erfordert eine Sekundärstatistik keine eigene Datenerhebung, sondern geht vielmehr von bereits vorhandenen Datenbeständen aus, die zusätzlich noch statistisch ausgewertet werden.

3.9.2 Entwurf eines Brandenburgischen Statistikgesetzes

91

92 BVerfGE 65, 1 (69)

93 BVerfGE 65, 1 (55)

94 BVerfGE 65, 1 (43)
vom 20. August 1992, GVBl. I S. 298

Der bereits in meinem 2. Tätigkeitsbericht[95] erwähnte Entwurf eines Brandenburgischen Statistikgesetzes wurde zwischenzeitlich mehrfach überarbeitet, befindet sich jedoch noch immer in der Ressortabstimmung. Das Ministerium des Innern ist allerdings zuversichtlich, daß diese aus datenschutzrechtlicher Sicht besonders bedeutsame Gesetzesvorlage nunmehr nach der parlamentarischen Sommerpause in den Landtag eingebracht werden kann. Zu den datenschutzrechtlich relevanten Regelungen der bisherigen Entwürfe hat es auf der Grundlage meiner ausführlichen Stellungnahmen konstruktive und auch für die Arbeit meiner Behörde fruchtbare Gespräche mit dem Innenministerium gegeben. Ich gehe davon aus, daß deren Ergebnisse in der abschließenden Fassung der Gesetzesvorlage angemessen berücksichtigt sein werden. Anlaß zur Besorgnis hat mir insbesondere die Heftigkeit des Widerspruchs gegeben, auf den die Regelungen zur Abschottung der Statistik, die nicht kostenfrei realisiert werden kann, bei den an der Abstimmung beteiligten Vertretern der Kommunen gestoßen sind. Demgegenüber ist zu erinnern, daß die strikte Trennung der Statistik vom Verwaltungsvollzug nach Maßgabe der oben dargestellten verfassungsrechtlichen Anforderungen (s. unter 3.9.1) nicht zur Disposition des Gesetzgebers steht. Da mir die aktuelle Fassung des Gesetzentwurfs noch nicht vorliegt und die Abstimmung mit dem Ministerium des Innern noch nicht abgeschlossen ist, wird hier im übrigen nicht näher auf die einzelnen Regelungen des Entwurfs eingegangen.

3.9.3 Wohnungsstatistik 1995

Nach Maßgabe des Wohnungsstatistikgesetzes[96] wird mit Stichtag 30. September 1995 in den neuen Bundesländern und dem ehemaligen Ostberlin eine flächendeckende Gebäude- und Wohnungszählung als Bundesstatistik durchgeführt, wie sie in ähnlicher Form bereits 1987 nach Maßgabe des Volkszählungsgesetzes 1987[97] in den alten Bundesländern erfolgte. Im wesentlichen geht es um die statistische Erhebung der Eigentumsformen an den Wohngebäuden, die Anzahl der Wohnungen, deren technische Ausstattung, Nutzung, Größe, eventuelle Belegungsbindung und Förderung durch den sozialen Wohnungsbau, das Alter der Wohngebäude und den Bauzustand. Auskunftspflichtig sind nach § 9 Wohnungsstatistikgesetz die Eigentümer und Verwalter oder Erbbauberechtigten, Verfügungs- oder Nutzungsberechtigten. Die Auskünfte können nach § 10 mündlich gegenüber einem Erhebungsbeauftragten oder schriftlich auf den Erhebungsbögen gegeben werden, die dann entweder dem Erhebungsbeauftragten verschlossen übergeben werden oder andernfalls innerhalb einer Woche der Erhebungsstelle zuzustellen sind.

An der Erstellung der Brandenburgischen Verordnung zur Durchführung der Gebäude- und Wohnungszählung 1995[98] hat meine Behörde beratend teilgenommen, ebenso an der Erstellung von Verwaltungsvorschriften zur Erhebungsstellenanleitung durch das Landesamt für Datenverarbeitung und Statistik. Ferner wurden Mitarbeiter meiner Behörde regelmäßig zu den Beratungen des Landesamtes mit den verantwortlichen Mitarbeitern der Landkreise und kreisfreien Städte zur Vorbereitung der Gebäude- und Wohnungszählung hinzugezogen.

Meine Hinweise zur datenschutzgemäßen Ausgestaltung der Erhebung zur Gebäude- und Wohnungszählung 1995 in rechtlicher und technisch-organisatorischer Hinsicht wurden sowohl vom Ministerium des Innern als auch vom Landesamt für Datenverarbeitung und Statistik berücksichtigt. Insbesondere habe ich klare Regelungen gefordert zur

---

95

96 s. dort unter 3.9.3, S. 81 ff.

97 vom 18. März 1993, BGBl. I S. 337

98 vom 8. November 1985, BGBl. I S. 2078
vom 29. Dezember 1994, GVBl. II 1995, S. 97

- räumlichen, organisatorischen und personellen Trennung der Erhebungsstellen von der Verwaltung,

- Verpflichtung der Mitarbeiter in den Erhebungsstellen und der Erhebungsbeauftragten auf das Statistikgeheimnis,

- Abschottung der Datenverarbeitung in den Erhebungsstellen vom Datennetz der Verwaltung (siehe auch unter 3.9.8).

Nach § 11 Wohnungsstatistikgesetz besteht ferner die Möglichkeit, daß die Statistikstellen der Landkreise und kreisfreien Städte für ihren Zuständigkeitsbereich Einzelangaben aus der Wohnungsstatistik vom Landesamt für Datenverarbeitung und Statistik oder vom Statistischen Bundesamt erhalten können (Rückmeldungen). Diese Einzelangaben sind zwar nicht personenbezogen, aber wegen der Angabe zu Straße und Haus-Nummer personenbeziehbar. Sie sollen zur Bildung kleinräumiger Gliederungssysteme (Blockseiten) dienlich sein. Allerdings hat der Gesetzgeber ganz klar festgelegt, daß diese Daten nur für statistische Zwecke verwendet werden dürfen. Eine Verwendung für den Verwaltungsvollzug, etwa zur konkreten Feststellung und Bekämpfung von Wohnungsleerstand, wäre grob rechtswidrig und ist gem. § 22 Bundesstatistikgesetz[99] mit Freiheitsstrafe oder Geldstrafe belegt.

Darüber hinaus hat der Gesetzgeber unter Hinweis auf § 16 Abs. 5 Bundesstatistikgesetz bestimmte Bedingungen an diejenigen kommunalen Statistikstellen gestellt, die Wert auf eine Übermittlung solcher Einzelangaben legen. Danach muß zunächst durch Landesgesetz sichergestellt sein, daß die Statistikstellen von anderen kommunalen Verwaltungsstellen getrennt sind. Da das Land Brandenburg z. Zt. noch kein Landesstatistikgesetz besitzt, gilt ersatzweise § 32 Brandenburgisches Datenschutzgesetz[100]. In Abs. 2 heißt es, daß die Statistikstellen organisatorisch und räumlich von den anderen Verwaltungsstellen getrennt sein müssen, gegen den Zutritt unbefugter Personen hinreichend zu schützen und mit eigenem Personal auszustatten sind, das die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet, schriftlich auf das Statistikgeheimnis verpflichtet wurde und während der Tätigkeit in der Statistikstelle nicht mit andern Aufgaben des Verwaltungsvollzuges betraut ist.

3.9.4 Wahlstatistik

Anläßlich der Europawahl am 12. Juni 1994 ist an mich das Problem der repräsentativen Wahlstatistik herangetragen worden. Nach den Wahlgesetzen und Wahlverordnungen des Bundes und der Länder können in repräsentativen Stichproben-Wahlbezirken Wahlscheine ausgegeben werden, die nach Geschlecht und 5 Altersgruppen unterschieden sind. Ist ein Stichproben-Wahlbezirk klein (etwa 300 bis 400 Wahlberechtigte), die Wahlbeteiligung nur gering (50 % und weniger) und wird die Briefwahlmöglichkeit stark genutzt, besteht die Gefahr, daß sich bei der Stimmenauszählung und der Auswertung eine Personenbeziehbarkeit ergibt, durch die das Wahlgeheimnis beeinträchtigt würde. Die prozentuale Aufteilung der insgesamt 10 Gruppen nach Alter, Männern und Frauen ist nämlich demographisch nicht gleichmäßig 10 %, sondern schwankt derzeit zwischen 4 und 18 % pro Gruppe. Im Land Brandenburg als Flächenstaat kommt erschwerend hinzu, daß 83 % der Gemeinden weniger als 1000 Wahlberechtigte haben. Bei der Europawahl 1994 lagen beispielsweise von 126 Stichproben-Wahlbezirken 37 bei 300 - 399 Wahlberechtigten und weitere 14 bei 400 - 499 Wahlberechtigten. Im Sommer und Herbst des vergangenen Jahres habe ich deshalb mit dem brandenburgischen Landeswahlleiter zu dieser Problematik eine Reihe von Gesprächen

---

99 vom 22. Januar 1987, BGBl. I S. 462 und 565, i. d. Fassung

100 vom 17. Dezember 1990, BGBl. I S. 2837

vom 20. Januar 1992, GVBl. I S. 2

geführt, die sehr konstruktiv waren. Im Ergebnis hat der Landeswahlleiter die Wahlstatistik zur brandenburgischen Landtagswahl am 11. September 1994 ausgesetzt; eine Maßnahme, die ich ausdrücklich begrüßt habe.

Die Rechtslage bezüglich der Wahlstatistik ist in Bund und Ländern z. T. unterschiedlich. So bestimmt beispielsweise § 49 Abs. 5 der Landeswahlordnung Berlin[101], daß nur solche Stimmbezirke ausgewählt werden dürfen, in denen je Gruppe mindestens 20 Wahlberechtigte im Wählerverzeichnis eingetragen sind. Nach § 7 Nr. 1 der Bundeswahlordnung[102] gilt das Wahlgeheimnis bei einem Briefwahlvorstand als gesichert, wenn auf ihn mindestens 50 Wahlbriefe entfallen.

Inzwischen haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 49. Konferenz in einer Entschließung zum Datenschutz bei Wahlen (s. Anlage 17) übereinstimmend empfohlen, daß die Wahlstatistik nur in solchen Wahlbezirken durchgeführt werden sollte, "in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt". Die Festlegung dieses Kriteriums läge danach bei den Wahlleitern von Bund und Ländern. Für Wahlen auf Landesebene sind in Brandenburg die rechtlichen Voraussetzungen dafür gegeben, weil nach dem Brandenburgischen Landeswahlgesetz[103] und dem Brandenburgischen Kommunalwahlgesetz[104] und den entsprechenden Wahlverordnungen die Auswahlbezirke ohnehin vom Landeswahlleiter bestimmt werden.

3.9.5 Agrarstatistik

Die Agrarstatistik ist z. Zt. die umfangreichste amtliche Statistik, die in den Landkreisen Brandenburgs durchgeführt wird. In § 95 Abs. 1 Agrarstatistikgesetz[105] werden die Landesregierungen ermächtigt, "durch Rechtsverordnung die erforderlichen Regelungen zur Bestimmung der Erhebungsstellen, zur Sicherung des Statistikgeheimnisses durch Organisation und Verfahren" und zu den im Gesetz festgelegten Zwecken zu treffen. Die Brandenburgische Verordnung über die Durchführung des Agrarstatistikgesetzes (AgrStatG-DVO)[106], an deren Abfassung ich nicht beteiligt war, regelt in § 3 Abs. 1 die Abschottung der Statistikstellen von der übrigen Verwaltung. Allerdings entspricht die Formulierung - "Soweit eben möglich, sind die Erhebungsstellen für die Dauer der Bearbeitung von Einzelaufgaben räumlich und organisatorisch von den anderen Verwaltungsstellen zu trennen" - nicht den verfassungsrechtlichen Anforderungen des Bundesverfassungsgerichts im sog. Volkszählungsurteil[107]. Bei der Abschottung der Statistik von der Verwaltung gibt es keinen Ermessensspielraum. Dasselbe regelt § 26 Abs. 1 Bundesstatistikgesetz[108], der die Ermächtigung zur Durchführung von Bundesstatistiken nur einräumt, wenn die Statistikstelle von den anderen Aufgabenbereichen getrennt ist, und zwar ohne Einschränkung. Zudem ist

---

101

102 vom 14. Januar 1992, GVBl. S. 6

103 i. d. Fassung vom 8. März 1994, BGBl. I S. 495

104 vom 2. März 1994, GVBl. I S. 38, geänd. durch SWG vom 7. Juli 1994, GVBl. I S. 294

105 vom 22. April 1994, GVBl. I S. 110

106 vom 23. September 1992, BGBl. I S. 1633

107 vom 19. April 1991, GVBl., S. 34

108 BVerfGE 65, 1 (49)

vom 22. Januar 1987, BGBl. I S. 462 und 565, i. d. Fassung vom 17. Dezember 1990, BGBl. I S. 2837

die o. g. Formulierung in § 3 Abs. 1 der AgrStatG-DVO auch aus anderen Gründen unglücklich. Bei dem Begriff "Einzelaufgaben" kann es sich nur um statistische "Einzelangaben" handeln. Das Ministerium des Innern hat in dieser Sache Abhilfe entweder durch Änderung der DVO, zumindestens aber durch ein richtigstellendes Rundschreiben an die Landkreise und kreisfreien Städte zugesagt.

3.9.6 Sozialhilfestatistik

3.9.6.1 Neue Antragsbögen

Bei der seit 01.01.1994 als Bundesstatistik durchgeführten Sozialhilfestatistik gem. §§ 127 ff. Bundessozialhilfegesetz[109] handelt es sich um eine sog. Sekundärstatistik (s. unter 3.9.1), für die nur solche Daten genutzt werden dürfen, die im Rahmen des Verwaltungsvollzuges rechtmäßig erhoben wurden. Auskunftspflichtig sind die Träger der Sozialhilfe, zu statistischen Zwecken werden anonymisierte Daten der Sozialhilfeempfänger verwendet. Bis Ende 1993 wurden bei der Antragstellung zur Sozialhilfe folgende Angaben nicht erfragt: differenzierter Ausländerstatus (EG-Ausländer, Asylberechtigte, Bürgerkriegsflüchtling, sonstige Ausländer), höchster allgemeinbildender Schulabschluß, höchster Berufsausbildungsabschluß, besondere soziale Situation bei der Hilfegewährung. Für die Hilfegewährung konnte also auf diese Daten bis dahin verzichtet werden. Das bedeutet, daß diese Daten für die Antragstellung nicht erforderlich sind.

Seit 1994 verwendet das Land Brandenburg einen neuen Antragsbogen zur Sozialhilfegewährung, in dem die o. g. vier zusätzlichen Erhebungsmerkmale bereits vorgedruckt sind. Da diese Daten aber nur für die Statistik benötigt werden, kommt es zu einer unzulässigen Vermischung von Sekundärstatistik und Primärstatistik. Primärstatistische Erhebungen müssen ohnehin von der Verwaltung getrennt durchgeführt werden. Außerdem dürfen wegen fehlender Rechtsgrundlage die vier zusätzlichen Angaben nur auf freiwilliger Basis erhoben werden; eine verweigerte Mitteilung dieser Daten darf keine Androhung oder Durchführung von Maßnahmen wegen Verletzung von Mitwirkungspflichten gem. § 66 SGB I[110] zur Folge haben.

Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hält die neu abgefragten personenbezogenen Daten der Sozialhilfe-Antragsteller ohne nähere Begründung für leistungs- bzw. entscheidungsrelevant. Da es sich im übrigen um eine Bundesstatistik handele, hätte das Land keine Möglichkeit, abweichende Regelungen zu treffen. Dies sei eine Angelegenheit der zuständigen Bundesbehörden; datenschutzrechtliche Überlegungen sollten dementsprechend auch mit dem Bundesbeauftragten für den Datenschutz geklärt werden. Im Gegensatz dazu hat trotzdem z. B. das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen auf die Empfehlung des dortigen Landesbeauftragten für den Datenschutz reagiert und per Erlaß die Bezirksregierungen und örtlichen Träger der Sozialhilfe darauf hingewiesen, daß eine Datenerhebung nur zum Zweck der Sozialhilfestatistik durch die Vorschriften des Bundessozialhilfegesetzes nicht gedeckt sei[111].

3.9.6.2 Weitergehende Vorstellungen des Verbandes Deutscher Städtestatistiker

---

109 vom 30. Juni 1961 i. d. Fassung vom 10. Januar 1991, zul. geänd. 21. Dezember 1993, BGBl. I S. 2374

110 vom 11. Dezember 1975, zul. geänd. 27. Dezember 1993, BGBl. I S. 2378

111 12. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen, S. 95

Da die Kommunen die Hauptlast der Sozialhilfe zu tragen haben, wächst bei ihnen offensichtlich das Interesse, weit mehr statistische Daten über Sozialhilfeempfänger zu erhalten, als die derzeitige amtliche Statistik liefert. Mir liegt ein Konzept des Verbandes Deutscher Städtestatistiker vor, nach dem auf freiwilliger Basis weitere zusätzliche Merkmalsgruppen erhoben werden sollen, wie z. B. kleinräumige-stadtregionale Merkmale zur Feststellung von Armutsverdichtungen und besonderen Problemlagen (mit Straßenschlüssel und Haus-Nummer), Art der besuchten Schulform, Nationaltätsmerkmale zur Analyse subkultureller/multikultureller Armutsmilieus, Ergänzung von Wohnungsangaben zur Wohnungsqualität und Belegungsdichte, differenzierte Angaben zur zuletzt ausgeübten Berufstätigkeit. Begründet wird die Notwendigkeit dieser zusätzlichen Erhebungen mit der Verbesserung der Informationsgrundlagen für kommunale Sozialberichterstattungen, Sozialplanungen und Sozialpolitiken.

Bei Erhebungen solcher Art ist deren eindeutige Zweckbestimmung nicht erkennbar, es sei denn, man unterstellt von vornherein eine bewußte Ansteuerung der Aufhebung der Trennung von Statistik und Verwaltungsvollzug. Die Gefahr der sozialen Abstempelung ist bei kleinräumigen Erhebungen der oben beschriebenen Art wegen der relativ leichten Deanonymisierung erheblich. Da auch die Sicherstellung der Vergleichbarkeit der Merkmalsdefinitionen mit amtlichen Massenerhebungen und sozialwissenschaftlich etablierten Umfrage-Instrumenten angestrebt wird, ist "eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger", die "auch in der Anonymität statistischer Erhebungen unzulässig" ist[112], nicht mehr ausschließbar. Aus diesen Gründen sowie wegen der unter 3.9.1 dargestellten Prinzipien statistischer Erhebungen ist das Konzept des Verbandes abzulehnen.

3.9.7 Geschäftsstatistiken

Gelegentlich haben mich öffentliche Stellen des Landes um Stellungnahme gebeten, ob sie Daten, die in ihrer Zuständigkeit angefallen sind, zu statistischen Zwecken an öffentliche und nicht-öffentliche Stellen in und außerhalb des Landes Brandenburg weitergeben dürfen.

Dazu ist festzustellen, daß § 31 Bbg DSG die öffentlichen Stellen des Landes befugt, personenbezogene Daten zur Erstellung von Statistiken weiterzuverarbeiten, soweit diese Daten bei der rechtmäßigen Aufgabenerfüllung in ihrer Zuständigkeit angefallen sind. Falls solche Statistiken, die üblicherweise als Geschäftsstatistiken bezeichnet werden, veröffentlicht werden sollen, dürfen sie keinen Bezug auf eine bestimmte Person mehr zulassen. Sobald diese Anonymisierung tatsächlich vorhanden ist, unterliegen derartige statistische Ergebnisse nicht mehr dem Brandenburgischen Datenschutzgesetz und damit der Kontrolle des Landesbeauftragten für den Datenschutz, weil dieses nur für die Verarbeitung personenbezogener Daten gilt. Veröffentlichung und Weitergabe solcher Statistiken sind der öffentlichen Stelle dann also freigestellt.

Allerdings weise ich ausdrücklich darauf hin, daß der Gesetzgeber die Anforderungen an die Anonymisierung von Geschäftsstatistiken außerordentlich hoch gesteckt hat. Er geht dabei über die in § 3 Abs. 3 Bbg DSG bestimmte Definition erheblich hinaus. Hier gilt: "Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können". Damit ist die sog. faktische Anonymisierung beschrieben. Für Geschäftsstatistiken gilt dagegen die absolute Anonymisierung, weil dabei die Möglichkeit einer Deanonymisierung prinzipiell

---

112 BVerfGE 65, 1 (53)

ausgeschlossen werden muß. Dies hat auch seinen guten Grund. Einmal fehlt für die einzelne konkrete Geschäftsstatistik die gesetzliche Grundlage. Zum andern besteht bei Geschäftsstatistiken öffentlicher Stellen häufig wegen des kleinräumigen Bezugs, der meist relativ geringen Anzahl der Betroffenen und der u. U. sehr sensiblen Daten eine große Gefahr der Deanonymisierung. Man stelle sich nur vor, ein Sozialamt würde in einer kleinen Stadt etwa eine Geschäftsstatistik über suchtabhängige Sozialhilfeempfänger veröffentlichen. Die soziale Abstempelung wäre nicht nur ungesetzlich und verfassungswidrig, sondern würde den Betroffenen auch in seinem sozialen Umfeld stigmatisieren.

Geschäftsstatistiken sind von ihrer Art her Sekundärstatistiken, weil bei ihrer Erstellung nur auf schon vorhandene Datenbestände zurückgegriffen wird und keine (primär-)statistischen Daten bei den Betroffenen erhoben werden.

Der Entwurf des Brandenburgischen Landesstatistikgesetzes[113] faßt den Begriff der Geschäftsstatistik enger. In § 9 Abs. 1 heißt es: "Geschäftsstatistiken bedürfen ... keiner Anordnung durch Rechtsvorschrift, wenn sie ausschließlich der Erfüllung der Aufgaben der öffentlichen Stelle ... oder der Erfüllung der Aufgaben der jeweils übergeordneten öffentlichen Stelle dienen". Das heißt, daß die Zulässigkeit der Anfertigung von Geschäftsstatistiken eindeutig an die Aufgabenstellung der öffentlichen Stelle gebunden ist. Einen Rechtsanspruch auf die Erstellung von solchen Statistiken hat neben der öffentlichen Stelle selbst nur die jeweils übergeordnete Stelle, sofern dies im Rahmen ihrer Aufgabenstellung liegt. Andere öffentliche und nicht-öffentliche Stellen haben diesen Rechtsanspruch nicht. Jedoch steht es im Belieben der öffentlichen Stelle, bereits vorhandene Geschäftsstatistiken, sofern sie nur rechtmäßig erstellt wurden und dem absoluten Anonymisierungsgebot genügen, weiterzugeben und zu veröffentlichen. Der Hinweis auf die Handhabung der Geschäftsstatistiken nach dem im Entwurf befindlichen Landesstatistikgesetz ist insofern von einiger Bedeutung, weil mit dessen Inkrafttreten § 31 Bbg DSG außer Kraft gesetzt wird.

3.9.8 Durchsetzung des Trennungsgebotes bei kommunalen Statistikstellen des Landes

Ich habe es für notwendig gehalten, die Statistikstellen der Landkreisverwaltungen und der kreisfreien Städte zu kontrollieren, die nicht mit den Erhebungen zur Gebäude- und Wohnungszählung 1995 befaßt sind. Mein grundsätzliches Interesse lag dabei auf der räumlichen, personellen und organisatorischen Abschottung der Statistikstelle von der übrigen Verwaltung, wie sie vom Bundesverfassungsgericht und Gesetzgeber gefordert wird[114]. Bei allen bisher besuchten Verwaltungen hatte ich leider Anlaß, Mängel in Bezug auf die Abschottung gem. § 25 Abs. 1 Bbg DSG zu beanstanden.

In der Mehrzahl der Fälle war die personelle Trennung nicht eingehalten. Zwar wurde z. B. die Kommunalstatistik in der Statistikstelle abgewickelt, nicht jedoch die amtliche Agrarstatistik, die in den Landwirtschaftsämtern bearbeitet wurde, wenn auch meist von denselben Mitarbeitern. Dies ist freilich ein schwerwiegender Verstoß gegen die Abschottung der Statistik von der Verwaltung. Dabei bedürfte es keines großen Aufwands, diese Mitarbeiter in die Statistikstelle umzusetzen.

Die organisatorische Trennung von Statistik und Verwaltung scheint das größte Problem darzustellen. Sie war in keinem Fall vorhanden, da die Statistikstellen derzeit meist dem Hauptamt unterstellt sind. Einige der zuständigen Stellen vertreten die Meinung, daß die Einzelstellung der Statistikstelle einer "Verschlankung" der Verwaltung entgegenstünde.

113

114 Brandenburgisches Statistikgesetz (Entwurf August 1994) s. unter 3.9.1

Diesem Argument kann ich mich nicht anschließen. Abgesehen davon, daß die Rechtslage eine klare Abschottung der Statistik zwingend notwendig macht, sind die Verwaltungskörper so groß, daß eine separierte Stellung der Statistikstelle innerhalb der Verwaltung kein Problem darstellen kann. Ich habe deshalb empfohlen, die Statistikstellen dem Landrat bzw. Oberbürgermeister direkt zu unterstellen. Dies sollte auch so im Geschäftsverteilungsplan und Behördenorganigramm nachvollziehbar dokumentiert werden. Ebenso müssen per Dienstanweisung Zuständigkeitsregelungen für Statistiken und Umfragen und in einer besonderen Dienstanweisung die Arbeit der Statistikstelle beschrieben werden. Es ist überlegenswert, ob für die Dienstaufsicht über den Leiter der Statistikstelle eine vom Landrat/Oberbürgermeister delegierte Anbindung an den Leiter eines anderen Amtes sinnvoll ist. Eine fachaufsichtliche Anbindung der Statistikstelle kann an das Rechnungsprüfungsamt erfolgen. Es dürfte klar sein, daß die Verpflichtung des Leiters und der Mitarbeiter der Statistikstelle auf das Statistikgeheimnis auch ihre Stellung gegenüber allen anderen Mitarbeitern der Verwaltung einschließlich der Dienst- und Fachvorgesetzten bestimmt. Das bedeutet auch, daß Mitarbeiter der sonstigen Verwaltung die Statistikstelle grundsätzlich nicht betreten dürfen.

Ein weiteres Problem stellte die Abschottung der ADV der Statistikstelle vom übrigen Datennetz der Verwaltung dar, die in der Mehrzahl der Fälle nicht eingehalten war. Dazu ist grundsätzlich folgendes zu sagen: Es ist durchaus zulässig, wenn die Statistikstelle zum Zweck der Erstellung von Kommunalstatistiken als Sekundärstatistik auf Datenbestände der Verwaltung zugreift, insbesondere wenn diese schon anonymisiert vorliegen oder durch das Zugriffsverfahren der direkte Personenbezug ausgeschlossen wird und dem im einzelnen keine Rechtsvorschriften entgegenstehen. In dieser Hinsicht gibt es gegen die Einbeziehung der Statistik in das allgemeine Datennetz der Verwaltung keine datenschutzrechtlichen Bedenken. Völlig anders stellt sich jedoch die Sache dar, wenn die Statistikstelle selbst personenbezogene Daten zum Zweck einer amtlichen Statistik oder einer Kommunalstatistik erhebt, also primärstatistisch arbeitet, was eine ihrer ureigensten Aufgaben ist. In diesem Fall muß die ADV der Statistikstelle von der ADV der übrigen Verwaltung völlig abgeschottet sein. Dies kann derzeit nicht durch die Zugriffsrechtevergabe innerhalb der Netzverwaltungssysteme allein völlig sichergestellt werden, zumal bei Datensicherungsmaßnahmen die Daten von Statistik und Verwaltung vermischt würden. Auch die Arbeit auf der lokalen Festplatte der PC in der Statistik ist derzeit nicht ausreichend abzuschotten. Dies kann nur durch spezielle Methoden erreicht werden. Zum einen kann man für diese Fälle eigene PC in der Statistikstelle einsetzen, die auch untereinander - jedoch nicht mit dem Verwaltungsnetz - vernetzt werden können. Allerdings muß die Statistik dann selbst für Datensicherungsmaßnahmen (Backup) sorgen. Eine andere Möglichkeit besteht darin, daß die personenbezogenen oder -beziehbaren statistischen Daten mit speziellen kryptographischen Methoden, die allerdings gewissen Ansprüchen genügen müssen[115], mittels Sicherheitssoftware und evtl. auch Zusatzhardware verschlüsselt werden. So verschlüsselt, könnten sie dann durchaus im üblichen Verwaltungsnetz abgelegt werden. Voraussetzung ist dafür aber, daß die konkreten Schlüssel nur dem Personal der Statistik zur Verfügung stehen, und zwar paßwortgebunden. Eine Einsicht Unbefugter wäre dann ausgeschlossen.

Nur z. T. war der korrekte Postlauf eingehalten. Notwendig ist es nämlich, daß alle Post, die erkennbar der Statistikstelle zugeordnet werden kann, diese auch ungeöffnet erreicht. Das setzt schon bei der Poststelle eigene Postfächer für die Statistik voraus.

Ferner wurde bei meinen Kontrollen festgestellt, daß die Statistikstellen häufig auch Aufgaben zur Durchführung von Wahlen wahrnehmen. Diese Kopplung ist insofern problematisch, als dabei auch Verwaltungshandeln erforderlich werden kann. Für diesen Fall

115 s. unter 1.3.5

müßte durch Dienstanweisung geregelt werden, daß das statistische Personal befristet von der Aufgabe "Statistik" entbunden und für die Aufgabe "Wahlen" freigestellt wird, um die Trennung von Statistik und Verwaltung abzusichern.

Die zuständigen Stellen haben zugesagt, die in den Prüfberichten aufgezeigten Mängel zu beheben. An den dazu erforderlichen Verfahrensregelungen werde ich mich beteiligen. Ungeachtet dessen werde ich weiterhin Kontrollen vor Ort vornehmen.

Bei den Erhebungen zu der Gebäude- und Wohnungszählung 1995 sehe ich für die Abschottung der temporären Erhebungsstellen von der sonstigen Verwaltung derzeit keine Probleme, da überall separate Erhebungsstellen eingerichtet wurden und das Verfahren durch Rechts- und Verwaltungsvorschriften abgesichert ist.

3.10 Zweites SED-Unrechtsbereinigungsgesetz

Der Vollzug des Zweiten SED-Unrechtsbereinigungsgesetzes (2. SED-UnBerG)[116] macht eine umfangreiche Verarbeitung personenbezogener Angaben der Antragsteller als Voraussetzung der Leistungsbewilligung erforderlich. Diese Angaben erhebt die Verwaltung bei den Betroffenen mit Hilfe mehrseitiger und inhaltlich im wesentlichen bundeseinheitlicher Antragsformulare. Meine Empfehlungen zur Aufklärung der Antragsteller über die Rechtsgrundlagen sowie über Art und Umfang der Datenverarbeitung gemäß §§ 4 Abs. 2, 12 Abs. 3 Bbg DSG hat das Ministerium des Innern bei der Gestaltung der Formulare berücksichtigt.

4 Justiz

4.1 Gesetze und Rechtsverordnungen

4.1.1 Entwurf Gesetz über das Versorgungswerk der Rechtsanwälte im Land Brandenburg (Brandenburgisches Rechtsanwaltsversorgungsgesetz - BbgRAVG)

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Referentenentwurf eines Brandenburgischen Rechtsanwaltsversorgungsgesetzes Stellung zu nehmen. Mit diesem Entwurf sollen die Mitglieder der Rechtsanwaltskammer eine berufsständische Alters-, Invaliditäts- und Hinterbliebenenversorgung erhalten. Vorgesehen ist die Einrichtung eines Versorgungswerks der Rechtsanwälte (z. Zt. sind ca. 800 Rechtsanwälte in Brandenburg zugelassen) als eine der Rechtsaufsicht des Ministeriums der Justiz (MdJ) unterstehende rechtsfähige Körperschaft des öffentlichen Rechts. Es sollen lediglich die wesentlichen Organisationsstrukturen, die Mitgliedschaftsvoraussetzungen, die Beitrags- und Leistungsgrundsätze gesetzlich geregelt werden, weitere Einzelheiten dagegen einer Satzung vorbehalten bleiben.

Die Regelung der Mitwirkungspflichten der Mitglieder in § 16 des Entwurfs, wonach diese sowie ihre Hinterbliebenen verpflichtet sind, dem Versorgungswerk alle für die Mitgliedschaft, die Beitragspflicht und den Leistungsanspruch bedeutsamen Auskünfte zu erteilen und die dafür erforderlichen Nachweise vorzulegen, erschien mir zu unbestimmt. Der Umfang der zulässigen Datenerhebung sollte sich normenklar aus dem Gesetz selbst ergeben, d. h. die in Frage kommenden Datenarten für eine zulässige Datenerhebung müssen näher konkretisiert werden. Darüber hinaus wies ich darauf hin, daß die im Rahmen der

---

116 vom 23. Juni 1994, BGBl. I S. 1311

Feststellung der Rechte und Pflichten - insbesondere die zur Berechnung des Beitrages bestehende Auskunftspflicht - sowie die Vorlage von Unterlagen von der Erforderlichkeit der Datenerhebung abhängig gemacht werden müssen. Ferner müssen die Interessenlage der auskunftspflichtigen Mitglieder und der Grundsatz der Verhältnismäßigkeit der Datenerhebung durch eine Begrenzung der Mitwirkungspflichten im Gesetzestext berücksichtigt werden.

Nach Mitteilung des MdJ wird dieser Entwurf überarbeitet und mir nach einer erneuten Ressortabstimmung zugeleitet. Falls es erforderlich sein sollte, werde ich dazu erneut Stellung nehmen.

4.1.2 Schuldnerverzeichnis

Gerichte führen als Erkenntnisquelle über die Kreditwürdigkeit im Geschäftsverkehr Verzeichnisse über die Personen ("Schuldnerverzeichnis"), die nach einem Zwangsvollstreckungsverfahren eine eidesstattliche Versicherung über ihr Restvermögen abgegeben haben oder gegen die eine Haftanordnung zur Abgabe derselben ergangen ist. Auf Antrag hatte gem. § 915 Abs. 3 Zivilprozeßordnung (ZPO) a. F. jedermann das Recht auf Auskunftserteilung über Eintragungen im Schuldnerverzeichnis. Ein solcher Eintrag im Schuldnerverzeichnis wurde entweder nach Ablauf bestimmter Fristen oder bei Nachweis der Befriedigung des Gläubigers durch den Schuldner vorzeitig gelöscht.

Nach jahrelangen Beratungen sind mit dem Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis[117] ab 1. Januar 1995 neue Vorschriften in die Zivilprozeßordnung aufgenommen worden, die durch Novellierung des § 915 ZPO und Einfügung des §§ 915 a bis h ZPO unter Berücksichtigung der neueren Entwicklungen beim Recht auf informationelle Selbstbestimmung die Regelungen über das Schuldnerverzeichnis auf eine deutlich verbesserte Grundlage stellt. Darüber hinaus wurde durch die Verordnung über das Schuldnerverzeichnis (SchuVVO)[118], die aus dem Jahre 1955 stammende allgemeine Verwaltungsvorschrift abgelöst. Ich hatte nach Abforderung des Entwurfs beim MdJ Gelegenheit, dazu schriftlich Stellung zu nehmen. Das Ministerium selbst hatte keine Veranlassung gesehen, mich zu beteiligen, da es sich bei der Führung des Schuldnerverzeichnisses seiner Auffassung nach nicht um eine Verwaltungsaufgabe i. S. v. § 2 Abs. 1 Satz 2 Bbg DSG, sondern um eine gerichtliche Aufgabe gem § 915 ZPO handele. Dieser Ansicht kann ich mich nicht anschließen, da zumindest die Gewährung von Einsichts- und Auskunftsrechten Verwaltungsaufgaben sind. Um so erfreulicher war es dann für mich, daß sich das Ministerium die Mehrzahl meiner Änderungsvorschläge in seiner Stellungnahme gegenüber dem Bundesjustizministerium zu eigen gemacht hat, die schließlich Eingang in das Gesetz fanden.

Die neuen Vorschriften enthalten beispielsweise im § 915 Abs. 2 ZPO eine Aufzählung der Zwecke, zu denen personenbezogene Daten aus dem Schuldnerverzeichnis verwendet werden dürfen. Auskunftssuchende müssen den konkreten Zweck der Auskunft angeben. Anders als bisher erfolgt eine Löschung im Schuldnerverzeichnis automatisch nach drei Jahren ohne Stellung eines besonderen Antrages. Das Gesetz regelt das Bewilligungsverfahren zum Bezug von Abdrucken und Listen aus dem Schuldnerverzeichnis detailliert. Die Bedingungen für die Einrichtung automatisierter Abrufverfahren sind ausführlich geregelt, so sind u. a. Protokollpflichten eingeführt worden. Bei Bekanntgabe von Tatsachen, die erkennen lassen, daß abgerufene Daten zweckwidrig verwendet oder in unzulässiger Weise weitergegeben wurden, ist die Einschaltung der für die Einhaltung datenschutzrechtlicher Bestimmungen zuständige Aufsichtsbehörde vorgesehen.

117

118 vom 15. Juli 1994, BGBl. I S. 1566
vom 15. Dezember 1994, BGBl. I S. 3822

4.1.3 Geldwäschegesetz

Am 29.11.1993 ist das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (sog. Geldwäschegesetz - GWG)[119] in Kraft getreten. Unter Geldwäsche versteht man die Verschleierung der illegalen Herkunft von Geld oder anderen Vermögensgegenständen. Dieses Gesetz soll der effektiven Verfolgung der Geldwäsche und damit der Bekämpfung der organisierten Kriminalität in diesem Bereich dienen. Kredit- und Finanzierungsinstitute, die Deutsche Bundespost wie auch Gewerbetreibende, Vermögensverwalter und Spielbanken müssen gem. § 9 Abs. 1 GWG den Einzahler von Beträgen von über 20.000,- DM identifizieren. Das betrifft auch Rechtsanwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte. Neben der Identität des Einzahlers sind auch Name und Anschrift desjenigen festzustellen, für dessen Rechnung der Einzahler handelt. Die erhobene Information unterliegt einer Aufzeichnungs- und Aufbewahrungspflicht. Für Kreditinstitute und Spielbanken besteht darüber hinaus gem. § 11 Abs. 1 GWG in Verdachtsfällen eine Anzeigepflicht gegenüber den zuständigen Strafverfolgungsbehörden.

Im Land Brandenburg ist die gem. § 11 Abs. 1 GWG zuständige Stelle zur Entgegennahme von Anzeigen das LKA[120], das die ergangenen Meldungen über Finanztransaktionen bei der Generalstaatsanwaltschaft in einem allgemeinen Register für Geldwäscheangelegenheiten führt und in das folgende Daten eingestellt werden: Tag des Eingangs, Name des Einzahlers, anzeigendes Institut, Tagebuchnummer des Landeskriminalamtes sowie Tag der Erledigung. Nach Auskunft des MdJ gibt es z. Zt. keine Überlegungen, die in den Verdachtsanzeigen der Kreditinstitute enthaltenen Mitteilungen in einer automatisierten Datei zu speichern.

Zu begrüßen ist, daß die Anzeigen nach § 11 GWG nicht - wie in anderen Bundesländern üblich - als normale Anzeige nach der Strafprozeßordnung behandelt und mit einem Justizaktenzeichen (Js.-.....) versehen werden. Die Folge wäre, daß auch Daten unbescholtener Bürger auf längere Zeit bei der Staatsanwaltschaft gespeichert würden und in den verschiedenen Informationssystemen der Justiz auf örtlicher, Landes- und Bundesebene auf Jahre dem Zugriff anderer Stellen ausgesetzt wären. Besonders problematisch ist eine solche Datenspeicherung unbescholtener Bürger in Datensätzen von Personen, denen schwerwiegende Vorwürfe wegen der Teilhabe an der organisierten Kriminalität gemacht werden.

Anläßlich des Inkrafttretens des GWG hat der Ostdeutsche Sparkassen- und Giroverband das vom Deutschen Sparkassenverlag aufgelegte Informationsblatt zur umfassenden Aufklärung der Sparkassenkunden in allen Sparkassen bekannt gegeben und ausgehändigt. Dies benennt in seiner Erstauflage fälschlicherweise den maßgeblichen Bareinzahlungsbetrag, der zur Aufzeichnungspflicht führe, mit 25.000.- DM statt gem. § 2 Abs. 1 GWG mit 20.000.- DM. Leider fehlt in diesem Informationsblatt auch ein sachdienlicher Hinweis auf die Vorschriften des § 9 Abs. 1 GWG (Anfertigung von Kopien der vorgelegten Ausweispapiere) sowie des § 9 Abs. 3 GWG (sechsjährige Aufbewahrung der Aufzeichnungen). Der Verband hat mir zugesichert, dies bei einer Neuauflage zu berücksichtigen.

4.1.4 Entwurf einer Errichtungsanordnung für ein bundesweites staatanwaltschaftliches Informationssystem (Bundes-SISY)

119

120 vom 25. Oktober 1993, BGBl. I S. 1770

Gemeinsamer Runderlaß des Ministeriums der Justiz und des Ministerium des Innern über die "Bestimmung der nach § 11 Abs. 1 Satz 1 GWG zuständigen Stelle zur Entgegennahme von Anzeigen" vom 25. Januar 1994, ABl. S. 203

Noch ehe das zur Einrichtung des Bundes-SISY ermächtigende Verbrechensbekämpfungsgesetz in seiner endgültigen Fassung vorlag, geschweige denn verabschiedet oder in Kraft getreten war, hat die Bundesregierung im Mai 1994 den Entwurf einer Errichtungsanordnung gem. § 476 Abs. 5 StPO(E) für das staatsanwaltschaftliche Verfahrensregister vorgelegt. In dieses beim Bundeszentralregister geführten Informationssystem sollen alle staatsanwaltschaftlichen Vorgänge aufgenommen werden, auf die - unabhängig von der Schwere und Bedeutung der Straftat - bundesweit durch Staatsanwaltschaften und Polizei zugegriffen werden kann. Gegen diese Regelung hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits auf ihrer 47. Sitzung ausgesprochen und schwere datenschutzrechtliche Bedenken angemeldet, weil durch den undifferenzierten Zugriff der Verfassungsgrundsatz der Verhältnismäßigkeit nicht gewahrt wird[121].

In meiner Stellungnahme zu der Errichtungsanordnung habe ich ausgeführt, daß der Entwurf einerseits die Anforderungen, die in Art. 4 Nr. 12 Verbrechensbekämpfungsgesetz zu § 476 Abs. 5 aufgeführt sind, nicht erfüllt, andererseits jedoch Regelungen enthält, die über den gesetzlich festgelegten Rahmen hinausgehen. Zu letzterem gehören insbesondere die Festlegungen in den Punkten 6 und 7 des Entwurfs, die neben den Staatsanwaltschaften auch die Finanzbehörden in steuerstrafrechtlichen Angelegenheiten an dem Datenaustausch mit dem Register beteiligen. Dafür fehlt eine ausreichende, normenklare Ermächtigung im Verbre-chensbekämpfungsgesetz.

Obwohl § 476 Abs. 5 StPO festlegt, daß die Errichtungsanordnung nähere Einzelheiten über die zum Betrieb der Datei erforderlichen technischen und organisatorischen Maßnahmen enthalten muß, sind solche dem Entwurf - bis auf einige allgemeine Absichtserklärungen - nicht zu entnehmen.

Kritisiert habe ich u. a. auch die Arten der im staatsanwaltschaftlichen Verfahrensregister zu verarbeitenden personenbezogenen Daten. In § 474 Abs. 2 Ziff. 1 StPO ist vorgeschrieben, daß über die Personendaten der Beschuldigten hinausgehende andere zur Identifizierung geeignete Merkmale nur gespeichert werden dürfen, soweit es zur Identifizierung erforderlich ist. Solche Merkmale könnten die in Pkt. 5.1 des Entwurfs aufgeführten abweichenden Personendaten, besonderen körperlichen Merkmale sowie unveränderlichen Kennzeichen sein. Sie dürfen jedoch im Verfahrensregister nur dann gespeichert werden, wenn eine eindeutige Identifizierung ohne diese Angaben nicht möglich ist. Diese Klarstellung sollte in die Errichtungsanordnung aufgenommen werden. Im Gegensatz zum polizeilichen Informationssystem INPOL, das ebenfalls ein Datenfeld für besondere körperliche Merkmale und unveränderliche Kennzeichen zur Identifizierung von Personen enthält, wird das staatsanwaltschaftliche Verfahrensregister nicht zum Zweck der Personenidentifizierung geführt. Es dient vielmehr, wie in Pkt. 2 der Errichtungsanordnung ausgeführt, der Registrierung aller im Bundesgebiet anhängigen Ermittlungs- und Strafverfahren.

Das MdJ hat zugesagt, mich weiterhin über den Verfahrensstand zu informieren und an dem Erlaß der Errichtungsanordnung zu einem länderübergreifenden staatsanwaltschaftlichen Verfahrensregister zu beteiligen.

4.2 Gerichte

4.2.1 Vorlage von Listen zur Sozialauswahl an das Arbeitsgericht

---

121 s. 2. Tätigkeitsbericht, Anlage 17 sowie unter 4.2., S. 86 ff.

In dem Rechtsstreit einer gekündigten Erzieherin gegen ihre frühere Arbeitgeberin, eine kreisfreie Stadt, hatte das prozeßführende Rechtsamt dem Arbeitsgericht gemäß § 1 Abs. 3 Satz 1, 2. Halbsatz Kündigungsschutzgesetz (KSchG)[122] die Listen der Verwaltung zur Sozialauswahl mit Angaben zu Namen, Alter, Familienverhältnisse von ca. 200 Erzieherinnen vorgelegt. Der Prozeßvertreter der Klägerin, ein Rechtsschutzsekretär einer Gewerkschaft, hatte daraufhin von ihm gefertigte Kopien dieser Listen an seine Mandantschaft verteilt, die überwiegend aus gekündigten Erzieherinnen bestand. Auf diese Weise hatten die Listen unter den Erzieherinnen in den Kitas der Stadt rege Verbreitung gefunden.

Die Verpflichtung der Verwaltung zur Offenbarung der Personal- und ggf. sogar Sozial- und Gesundheitsdaten einer Vielzahl ihrer Beschäftigten und Dritter im Kündigungsschutzprozeß halte ich aus datenschutzrechtlicher Sicht für ausgesprochen problematisch. Innerhalb des Prozeßverhältnisses scheint sie mir zwar letztlich unvermeidbar zu sein, weil sich der verfassungsrechtliche Rechtsschutzanspruch des Klägers im Kündigungsschutzprozeß anders nicht wirksam verwirklichen lassen dürfte. Ich halte es jedoch entsprechend den Vorgaben des Bundesverfassungsgerichts im sog. Volkszählungsurteil[123] um so mehr für geboten, in jedem Einzelfall die Möglichkeit wirksamer verfahrensrechtlicher Schutzvorkehrungen gegen eine Zweckentfremdung und mißbräuchliche Verwendung der Daten zu prüfen. So wäre beispielsweise zu erwägen, ob es zum Nachweis nach § 1 Abs. 3 Satz 1, 2. Halbsatz KSchG nicht völlig genügt hätte, dem Arbeitnehmer die Listen lediglich zur Einsichtnahme vorzulegen mit der Möglichkeit, sich ggf. Notizen zu machen. Ferner könnte das Gericht gem. §§ 171 b und 172 Nr. 3 Gerichtsverfassungsgesetz (GVG)[124] ggf. die Öffentlichkeit von der Verhandlung ausschließen und es dann gem. § 174 Abs. 3 Satz 1 GVG den anwesenden Personen zur Pflicht machen, die in dem Prozeß mit der Vorlage der Listen zur Sozialauswahl offenbarten personenbezogenen Daten geheim zu halten. Die Bedeutung des Grundrechts auf informationelle Selbstbestimmung stellt die Gerichte nicht frei, von Verfassungs wegen zu prüfen, ob von dieser verfahrensrechtlichen Möglichkeit zum Grundrechtsschutz Gebrauch zu machen ist. Darauf sollten sie von den beklagten Verwaltungen jeweils ausdrücklich hingewiesen werden.

Der Präsident des Landesarbeitsgerichts hat sich erfreulicherweise dazu bereit gefunden, das Schreiben, in dem ich ihm meine Überlegungen zu der Problematik dargestellt hatte, den Richterinnen und Richtern der Arbeitsgerichte und des Landesarbeitsgerichts informationshalber zur Kenntnis zu geben.

4.2.2 Hinterlassenschaften von betrieblichen Konfliktkommissionen - datenschutzrechtlich unbefriedigend gelöst

Mit der Verabschiedung des Gesetzes über die gesellschaftlichen Gerichte der DDR (GGG)[125] nahmen 1982 betriebliche Konfliktkommissionen ihre Tätigkeit auf. Sie sollten einerseits rein statistisch die Zahl der ordentlichen gerichtlichen Verfahren auf ein Minimum beschränken und andererseits gem. § 3 GGG vor Ort "gesellschaftliche Aktivitäten zur Durchsetzung der sozialistischen Gesetzlichkeit" und "Sicherheit in den Kombinaten, Betrieben, Städten und Gemeinden" fördern. Angeleitet durch den FDGB und diesem gegenüber

---

[122] i. d. Fassung vom 25. August 1969, BGBl. I S. 1317, zul. geänd. durch Gesetz vom 26. Februar 1993. BGBl. I S. 278

[123] BVefGE 65, 1 (46)

[124] i. d. Fassung vom 9. Mai 1975, BGBl. I S. 1077, zul. geänd. durch Gesetz vom 24. Juni 1994, BGBl. I S. 1374

[125] vom 25. März 1982, DDR-GBl. 1982 Teil I Nr. 13, S. 269

rechenschaftspflichtig, waren die Konfliktkommissionen gesellschaftliche Organe zur "Erziehung und Selbsterziehung der Werktätigen", die über die Einhaltung der Gebote der sozialistischen Moral, private Streitfälle (z. B. bei Unterhaltsverpflichtungen) und geringfügige Straftaten von Betriebsangehörigen entschieden. Somit erhielten die 237.821 Mitglieder der insgesamt 27.831 Konfliktkommissionen[126] ein detailliertes Bild des privaten Lebensbereichs der vorgeladenen Arbeitskollegen.

Während im GGG selbst keine formalen Vorschriften zur Arbeitsweise der betrieblichen Kommissionen zu finden waren, enthielt die im gleichen Jahr vom Staatsrat der DDR verabschiedete Konfliktkommissionsordnung (KKO)[127] Festlegungen zur Beschlußfassung betrieblicher Konfliktkommissionen (§ 5 Abs. 3), für die Aufbewahrung ihrer Unterlagen und Schreibarbeiten (§ 63) sowie über die zweijährige Aufbewahrung und anschließende Abgabe dieser Dokumente an das zuständige Kreisgericht (§ 66 Abs. 1 - 3).

Das datenschutzrechtliche Problem hat sich im Zusammenhang mit der allgemeinen Hektik der Wende unbemerkt eingeschlichen. Denn das noch am 13.09.1990 verabschiedete Schiedsstellengesetz (SchG)[128], das durch den Einigungsvertrag[129] in Kraft geblieben ist, hat die betrieblichen Konfliktkommissionen als auch die Schiedskommissionen mit Wirkung vom 03.10.1990 aufgehoben und darüber hinaus die Abgabe aller bei ihnen anhängigen Verfahren an die Kreisgerichte verfügt. Eine spezielle Regelung für die in den zwei zurückliegenden Jahren bei den betrieblichen Konfliktkommissionen abgeschlossenen Verfahren ist jedoch nicht getroffen worden.

Nachdem alle diesbezüglichen Versuche auf Bundesebene fehlgeschlagen sind, eine Rechtsgrundlage für die Ablieferung solcher Vorgänge zu schaffen, haben die neuen Bundesländer dann eigene Schritte unternommen. So hat Ende 1991 das MdJ Brandenburg den noch bestehenden DDR-Bezirksgerichten Cottbus, Frankfurt (Oder) und Potsdam empfohlen, in analoger Anwendung der Regelung des Einigungsvertrags (Zuständigkeitsübergang bei Inkrafttreten von Bundesrecht im Beitrittsgebiet)[130] die Rückforderung von Unterlagen der ehemaligen betrieblichen Konfliktkommissionen an die zuständigen Kreisgerichte zu veranlassen. Dagegen hat Berlin als einziges Land die ansonsten nach wie vor bestehende Gesetzeslücke 1993 dadurch geschlossen, in dem die Novellierung des Landesarchivgesetzes genutzt wurde und dabei mit § 5 Archivgesetz des Landes Berlin (ArchGB)[131] ein Passus aufgenommen worden ist, der die Zuständigkeit für personenbezogene Daten aus ehemaligen Einrichtungen der DDR regelt. Danach sind ehemalige Mitglieder betrieblicher Konfliktkommissionen und nicht-öffentliche Stellen zur Herausgabe derartiger Unterlagen an das Landesarchiv verpflichtet. Darüber hinaus ist in § 5 Abs. 2 ArchGB die strikte Trennung zwischen nicht-öffentlichem und öffentlichem Datenschutz aufgehoben worden. Der Berliner Datenschutzbeauftragte ist über derartige Aktenherausgaben zu informieren, und gleichzeitig räumt ihm das Gesetz bei Vorliegen von hinreichenden Anhaltspunkten für eine Verletzung der Herausgabepflicht auch eine

---

126 H.-J. Heusinger: Rechtssicherheit - garantiert für jeden, Berlin: Staatsverlag der DDR, 1985, S. 72 ff.

127 vom 12. März 1982, DDR-GBl. 1982 Teil I Nr. 13, S. 274

128 vom 13. September 1990, DDR-GBl. 1990 Teil I Nr. 61, S. 1527

129 vom 31. August 1990, BGBl. II S. 889 in Anl. II, Kap. III, Sachgeb. A, Abschn. I, Ziff. 3

130 vom 31. August 1990, BGBl. II S. 889 in Anl. I Kap. III Sachgeb. A Abschn. III Nr. 28 Maßgabe k

131 vom 29. November 1993, GVBl. Berlin S. 56

Kontrollbefugnis gegenüber nicht-öffentlichen Stellen nach § 28 BlnDSG[132] ein.

Ungeachtet dieser geglückten rechtlichen Regelung sind jedoch in Berlin wie in Brandenburg und in den anderen neuen Bundesländern nur sehr wenige Akten der betrieblichen Konfliktkommissionen sichergestellt worden. Meine Umfrage bei den hiesigen Amtsgerichten hat dies bestätigt. Darüber hinaus ist ein verschwindend kleiner Bestand in den Treuhanddepots und im Brandenburgischen Landeshauptarchiv "gelandet". Bisher sind mir Mißbrauchsfälle nicht bekannt geworden. Ich appelliere jedoch an diejenigen Personen, die noch im Besitz solcher Akten sind, diese nunmehr endgültig bei den Gerichten abzugeben.

4.2.3 Namenskartei ehemaliger DDR-Bezirks- und Kreisstaatsanwaltschaften

Nach Mitteilung des MdJ werden bei den derzeitigen vier Staatsanwaltschaften in Brandenburg die Namenskarteikarten der ehemaligen DDR-Bezirks- und Kreisstaatsanwaltschaften aufbewahrt, um sie evtl. für Rehabilitierungsverfahren vorzuhalten. Grundlage für die Aufbewahrung dieses Schriftgutes ist Abschn. I. 2 der Allgemeinen Verfügung des Ministers der Justiz und für Bundes- und Europaangelegenheiten[133], wonach das angesprochene Schriftgut bis auf weiteres nicht vernichtet werden darf. In Anbetracht der Vielzahl noch nicht rechtskräftig abgeschlossener Rehabilitierungsverfahren und der vom Bundestag bis zum 31. Dezember 1995 verlängerten Antragsfrist würde die Vernichtung des angesprochenen Schriftgutes nach Auffassung des Generalstaatsanwaltes zu einem unwiederbringlichen Beweismittelverlust führen, zumal die Namensverzeichnisse und Karteikarten der DDR in Ermangelung von Verfahrensakten und Urteilen oftmals einzige Grundlage für die Rehabilitierung und Entschädigung der Betroffenen sind. Nach Ablauf o. g. Frist muß über die weitere Vorgehensweise mit der Namenskartei entschieden werden.

4.2.4 Herausgabe von Grundbuchdaten an Dritte

In mehreren Fällen hatte ich mich mit den Voraussetzungen des Einsichtsrechts in das Grundbuch zu beschäftigen. Nach § 12 Abs. 1 Grundbuchordnung[134] ist demjenigen die Einsicht in das Grundbuch zu gestatten, der ein berechtigtes Interesse dargelegt hat. Ein berechtigtes Interesse hat jeder, dem ein Recht am Grundstück oder ein Grundstücksrecht zusteht, unabhängig davon, ob er als Berechtigter eingetragen worden ist oder nicht. Darüber hinaus kann auch ein tatsächliches - z. B. ein wirtschaftliches - Interesse genügen.

Ein Petent war von einer fremden Person als Käufer einer Eigentumswohnung angeschrieben worden. Meine Anfrage beim zuständigen Amtsgericht ergab, daß dieses auf Antrag die Anschriftenliste sämtlicher Wohnungseigentümer und damit Miteigentümer an den Käufer der Eigentumswohnung herausgegeben hatte, obwohl dies eine Verletzung grundbuchrechtlicher Vorschriften darstellt. Nach § 45 Abs. 3 Satz 2 Grundbuchverfügung[135] ist die Erteilung eines abgekürzten Auszugs aus dem Inhalt des Grundbuchs nicht zulässig. Diese Rechtsauffassung wurde auch von der Direktorin des Amtsgerichtes geteilt und der Vorfall zum Anlaß genommen, die betroffenen Beschäftigten nachhaltig auf die Bedeutung

---

[132] i. d. Fassung vom 17. Dezember 1990, GVBl. 1991, S. 16, 54, zul. geänd. durch Nr. 70 der Anlage zu § 1 Abs. 1 des Ge-

[133] setzes vom 17. Oktober 1994, GVBl. S. 428

[134] vom 25. Juni 1992, JMBl. 1992, S. 90

[135] i. d. Fassung vom 26. Mai 1994, BGBl. I S. 1114

Allgemeine Verfügung über die Einrichtung und Führung des Grundbuches vom 8. August 1935

einer besonders sorgfältigen Prüfung des berechtigten und rechtlichen Interesses vor Gewährung von Einsicht in die Grundbücher und Grundakten zu sensibilisieren.

4.3 Strafvollzug

4.3.1 Datenschutzrechtliche Prüfungen in Justizvollzugsanstalten

Erstmalig habe ich im Berichtszeitraum eine datenschutzrechtliche Prüfung zweier Justizvollzugsanstalten (JVA) vorgenommen. Dabei wollte ich mir einen ersten Überblick über die Datenverarbeitung im Strafvollzug im Land Brandenburg verschaffen und feststellen, wie unter den dort vorliegenden Besonderheiten die Bestimmungen des Bbg DSG eingehalten werden. Ein Recht auf informationelle Selbstbestimmung besitzt auch der Strafgefangene, das ihm nur im Rahmen einer gesetzlichen Regelung eingeschränkt werden darf. Dieser Tatsache hat der Datenschutzbeauftragte Geltung zu verschaffen.

Für die Kontrollbesuche wurden die größte JVA im Land Brandenburg mit ca. 550 Gefangenen und einer separaten Krankenabteilung sowie eine kleinere JVA mit ca. 120 Gefangenen (auch Frauen) ausgewählt.

In der größeren JVA befindet sich seit kurzem ein Rechnernetz, bestehend aus einem Server-Rechner und sechs PC im Probebetrieb. Das genutzte Programmsystem BASIS wurde über das MdJ beschafft. Dabei soll es sich um eine bundeseinheitliche Lösung handeln, mit der angeblich lediglich alle im Justizvollzug bereits üblichen Formulare und Mitteilungen, die vorher manuell erstellt und ausgefüllt wurden, mit gleichem Inhalt und in gleicher Form durch Rechnerausdrucke ersetzt werden. Dafür werden die erforderlichen Stammdaten der Gefangenen im Server-Rechner gespeichert. Während meines Besuches wurde in der JVA gerade die Stammdatenerfassung vorgenommen.

Für das Programmsystem existierten keinerlei Dokumentations- oder Bedienungsunterlagen. Lediglich eine Mitarbeiterin war beim Projektentwickler kurz in die Bedienung des Systems eingewiesen worden. Kompetente Gesprächspartner, die über das Softwaresystem aussagefähig waren, standen meinen Mitarbeitern nicht zur Verfügung. Eine genauere Prüfung des DV-Systems erschien mir unter den gegebenen Bedingungen nicht sinnvoll und wurde auf einen späteren Zeitpunkt verschoben. Meine Mitarbeiter konzentrierten sich daher auf die Besichtigung der JVA, die Datenverarbeitung in der Justizvollzugsgeschäftsstelle und im Krankenbereich sowie auf die Führung der Gefangenenpersonalakten.

Aus der Vielzahl der festgestellten Mängel sind nachstehend die problematischsten herausgehoben, zu denen ich meine Forderungen und Empfehlungen an das MdJ herangetragen habe:

- So habe ich empfohlen, für die in den JVA tätigen Sozialarbeiter und Psychologen die Führung von Sonderakten, die getrennt von der Gefangenenpersonalakte aufbewahrt werden, zuzulassen. Damit soll verhindert werden, daß die vertraulichen Informationen, die Gefangene den Sozialarbeitern oder Psychologen im Verlauf eines Gespräches anvertrauen, dem Zugriff anderer Bediensteter unterliegen, die diese Informationen für ihre Aufgabenerfüllung nicht benötigen. Das MdJ lehnte dies zunächst ab, da das Verfahren angeblich den Grundsätzen der Personalaktenführung widerspräche. Gleichwohl ist es aber bereit, die Angelegenheit auf Länderebene zur Diskussion zu stellen, da eine getrennte Aktenführung bundeseinheitlich zu regeln wäre. Ich hoffe, daß dies bald gelingt, denn das gegenwärtig praktizierte Verfahren, wonach alle Informationen der Sozialarbeiter und Psychologen in den Gefangenenpersonalakten vermerkt werden, stellt nicht nur eine Verletzung des informationellen Selbstbestimmungsrechtes der Gefangenen dar, sondern bringt auch Sozialarbeiter und Psychologen in Bedrängnis, die ebenso wie Ärzte einer besonderen Schweigepflicht unterliegen.

- Hinweisen mußte ich darauf, daß der Gefangene nur zu solchen Datenangaben verpflichtet ist, die für den Strafvollzug benötigt werden, und alle darüber hinausgehenden Informationen bei ihm allenfalls auf freiwilliger Basis erhoben werden dürfen. Aus der Gefangenensituation heraus ist der Begriff der Freiwilligkeit aber nur erfüllt, wenn bei Betroffenen nicht der Eindruck entstehen kann, daß ihnen im Verweigerungsfall Nachteile entstehen könnten. Darauf ist der Gefangene bei der Datenerhebung ausdrücklich hinzuweisen. Bei einigen Informationen (Kinderanzahl, erlernter Beruf, zuletzt ausgeübte Tätigkeit, Anschrift nächster Angehöriger, Tatbeteiligte usw.) bestehen noch unterschiedliche Auffassungen zwischen dem MdJ und mir darüber, ob diese Daten wirklich für die Durchführung des Strafvollzuges erforderlich sind.

- Meiner Forderung, den Gefangenen ein Einsichtsrecht in die Gefangenenpersonalakte zu gewähren, will das MdJ bislang noch nicht folgen. Jedoch stellt das Akteneinsichtsrecht einen wesentlichen Bestandteil des informationellen Selbstbestimmungsrechts dar, das allenfalls durch eine materiell-rechtliche Grundlage eingeschränkt werden könnte (s. oben). Eine solche Rechtsgrundlage ist nicht erkennbar.

- Auf meinen Hinweis, daß bei Gefangenen, die seit DDR-Zeiten einsitzen, unzulässigerweise noch immer die alten Gefangenenpersonalakten unbereinigt vorliegen und genutzt werden, hat das MdJ bisher noch keine Stellungnahme abgegeben. Hierfür muß kurzfristig eine Lösung angestrebt werden, die den Erfordernissen der §§ 35 - 37 Bbg DSG gerecht wird.

- Mit der Einführung einer automatisierten Datenverarbeitung im Justizvollzug müssen gleichzeitig auch alle im Bbg DSG geforderten Maßnahmen eingeleitet werden. Das betrifft besonders die Dateibeschreibung gem. § 8 Bbg DSG, die technisch-organisatorischen Maßnahmen gem. § 10 Bbg DSG (s. hierzu auch unter 1.3.1) und die Meldungen zum Dateienregister gem. § 24 Bbg DSG. Das MdJ hat mir signalisiert, daß diese Versäumnisse demnächst behoben werden sollen.

- Durch geeignete Sicherheitsvorkehrungen muß gewährleistet werden, daß Gefangene in keinem Fall Zugang zu Datenverarbeitungsanlagen oder zu Unterlagen mit personenbezogenen Daten erhalten. Als besonders kritisch sehe ich dabei den Einsatz von Gefangenen für Reinigungsarbeiten in Kernbereichen der Datenverarbeitung an. Das MdJ teilt meine Bedenken in dieser Frage leider nicht und verweist im übrigen auf die finanziellen Belastungen, die durch den Einsatz vertraglich verpflichteter Reinigungsfirmen auftreten. Keinesfalls bin ich bereit, Reinigungsarbeiten durch Gefangene in den Kernbereichen der Datenverarbeitung wegen der Gefahr unerlaubter Datenoffenbarung an Dritte hinzunehmen. Kostengründe können grundgesetzlich geschützten Persönlichkeitsrechten nicht entgegengehalten werden.

- Die gegenwärtig gültige Vollzugsgeschäftsordnung (VGO)[136] ist überholt und trägt modernen Möglichkeiten der Datenverarbeitung im Strafvollzug nicht ausreichend Rechnung. Im übrigen hat die 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im September 1994 in Potsdam fehlende bereichsspezifische Regelungen bei der Justiz in einer Entschließung (s. Anlage 4) kritisiert. Dazu gehören auch Regelungen über die Datenerhebung, -verarbeitung und -nutzung im Strafvollzug. Ich erwarte, daß das MdJ auf Bundesebene darauf Einfluß nimmt, daß das bestehende Defizit abgebaut wird.

- Meine Forderung, bis dahin zunächst durch eine Dienstanweisung für den Datenschutz den Umgang mit dem Recht auf informationelle Selbstbestimmung der Gefangenen im

136 i. d. Fassung vom 1. Januar 1977 (Stand: April 1982), durch AV des MdJ vom 2. März 1991 in Kraft gesetzt

Justizvollzugsbereich zu regeln, stößt beim MdJ auf Unverständnis. Nach eigenen Angaben besteht dort "Unklarheit über den Inhalt einer solchen Dienstanweisung". Ich bin gern bereit, entsprechende Hilfestellung zu geben.

Über die Umsetzung meiner Empfehlungen und Forderungen bin ich noch mit dem MdJ im Gespräch. Über konkrete Ergebnisse werde ich zu gegebener Zeit berichten.

4.3.2 Anfertigung von Lichtbildern bei Strafgefangenen

Derzeit wird in mehreren Bundesländern die Praxis der Anfertigung von Lichtbildern bei Gefangenen hinsichtlich der Rechtmäßigkeit und der aus sachlichen Gründen zwingenden Erforderlichkeit diskutiert. Auf Befragung teilte mir das MdJ mit, daß in den Justizvollzugsanstalten Brandenburgs ausnahmslos von allen Gefangenen Lichtbilder angefertigt werden, damit diese jederzeit eindeutig identifiziert werden können.

Auch wenn das MdJ dazu berechtigte Gründe (Verwechslungen, Nichtidentifizierbarkeit im Fluchtfall) anführen kann, muß im Einzelfall aufgrund der Sachlage über die Anfertigung von Lichtbildern entschieden werden. Denn gem. § 86 Abs. 1 Strafvollzugsgesetz (StVollzG)[137] hat der Gesetzgeber in das Ermessen der Vollzugsbehörde gestellt, ob und wenn ja in welchen Fällen diese Lichtbilder anfertigen wollen. Damit gelten die allgemeinen Rechtsregeln über die ermessensfehlerfreie Entscheidung im Einzelfall oder in vergleichbar gleichgelagerten Fällen. Diesem Rechtsgedanken trägt auch die selbst vorgenommene Ermessensbindung in der von den Landesjustizverwaltungen vereinbarten Vollzugsgeschäftsordnung (VGO) Rechnung. Dort wird in Nr. 23 Abs. 2 lediglich festgelegt, daß nur von Strafgefangenen mit einer Vollzugsdauer von einem und mehr Jahren Lichtbilder anzufertigen sind.

Diese Feststellung habe ich gegenüber dem MdJ mit der Bitte verbunden, daß die Betroffenen darauf hinzuweisen sind, daß sie gem. § 86 Abs. 3 StVollzG sowie Nr. 23 Abs. 4 VGO bei Entlassung aus dem Strafvollzug die Vernichtung der erkennnungsdienstlichen Unterlagen verlangen oder diese - wie in Schleswig-Holstein - auf Wunsch ausgehändigt bekommen können.

5 Bildung, Jugend und Sport

5.1 Verwaltungsvorschriften und Verordnungen im Schulbereich

Im Berichtszeitraum hatte ich Gelegenheit, zu einigen Rechtsverordnungen und Verwaltungsvorschriften des Ministeriums für Bildung, Jugend und Sport (MBJS) Stellung zu nehmen. Mit ihrer Verabschiedung wird die bereits im 2. Tätigkeitsbericht[138] von mir kritisierte Verlagerung spezialgesetzlicher Regelungen auf Rechtsverordnungen anstelle von materiell-rechtlichen Regelungen fortgesetzt.

5.1.1 Verwaltungsvorschriften Schulakten (VV-Schulakten)[139]

Darüber hat eine grundsätzliche Erörterung mit dem MBJS stattgefunden, die ein im wesentlichen zufriedenstellendes Ergebnis erbrachte.

---

137 vom 16. März 1976, BGBl. I S. 581, ber. S. 2088 und 1977 I S. 436

138 s. unter 1.3, S. 18 ff.

139 vom 17. November 1994, ABl. MBJS 1994, S. 884

In Nr. 2 Abs. 2 der VV-Schulakten war u. a. vorgesehen, daß Klassen- und Notenbücher 10 Jahre an den Schulen verbleiben. Unter Hinzuziehung des Grundsatzes der Erforderlichkeit ist für diese Akten eine wesentlich kürzere Aufbewahrungszeit, und zwar von zwei bis drei Jahren, ausreichend. Auf meine Anregung hin hat das Ministerium diese lange Aufbewahrungsfrist auf drei Jahre nach Abschluß des jeweiligen Schuljahres verkürzt.

Die von mir nachgefragte Differenzierung einerseits hinsichtlich des zeitlichen Verbleibs der Schülerkarteikarten sowie der Klassenarbeiten und Klausuren, die - soweit es sich z. B. nicht um Abiturarbeiten handelt -, grundsätzlich ebenfalls den Schülern ausgehändigt werden, und andererseits hinsichtlich der Klassen- und Notenbücher ergibt sich nach Mitteilung des Ministeriums aus der möglichen Beweissicherungsfunktion der einzelnen Akten. Schülerkarteikarten stellen lediglich einen Auszug aus der Schülerakte dar und sollen bei besonderen Vorkommnissen die Möglichkeit eröffnen, die Eltern schnell erreichen zu können. Ihr Zweck ist somit beim Abgang der Schüler aus der jeweiligen Schule erfüllt. Daher kann ihre Vernichtung bereits nach einem Jahr erfolgen. Klassenarbeiten bzw. Klausuren sind beim Zustandekommen von Zeugnisnoten und der sich daran anschließenden Entscheidung über eine Versetzung gemäß den einschlägigen Verordnungen für die einzelnen Bildungsgänge von herausgehobener Bedeutung. Daher können sie erst nach Ende des Schuljahres herausgegeben werden. Meinem Vorschlag, auf jeden Fall einen Zusatz in Nr. 2 Abs. 3 VV-Schulakten über den Verbleib von Schülerkarteikarten sowie Klassenarbeiten und Klausuren für ein Jahr an den Schulen, sofern letztere nicht herausgegeben werden, aufzunehmen, ist das Ministerium nicht gefolgt. Jedoch konnte ich das Ministerium bewegen, nicht nur die Aufbewahrungsfrist für Schülerakten, sondern auch für die übrigen Akten vorzusehen und in der Verwaltungsvorschrift zu regeln. Somit ist meinem Wunsch nach Festlegung des Beginns der Aufbewahrungsfrist sowie der Bestimmung des Aufbewahrungsortes der Akten entsprochen worden.

Die 10jährige Aufbewahrungsfrist für das Protokoll über die Vernichtung von Akten ist auf meine Anregung hin ebenfalls gestrichen worden. Die meinerseits mehrfach angemahnte Protokollierung der Vernichtung von Klassenarbeiten und Klausuren ist nun auch festgeschrieben worden.

Weiterhin habe ich gefordert, daß sich das Einsichtsrecht des in Nr. 6 Abs. 4 VV-Schulakten genannten Personenkreises an dem Grundsatz der Erforderlichkeit zu orientieren hat, d. h., daß diese Personen nur insoweit Einsicht nehmen, als dies zur Erfüllung ihrer dienstlichen Aufgaben erforderlich ist. Meinem Wunsch wurde mit der Einfügung "... im Rahmen der Erfüllung ihrer dienstlichen Aufgaben ..." Rechnung getragen. Dies gilt insbesondere für Widerspruchsverfahren und Ablehnungen zur Aufnahme an eine bestimmte Schule. In diesem Zusammenhang muß die Schulaufsichtsbehörde Einblick in die Schülerakte nehmen können.

Bisher nimmt Nr. 7 der VV-Schulakten lediglich auf schulformspezifische Zusatzdaten in die Schülerakte Bezug, ohne sie im einzelnen aufzuzählen. Das Ministerium sicherte mir zu, daß zur Transparenz dieser Zusatzdaten eine konkrete Aufstellung erfolgen wird. Da die einzelnen Bildungsgänge sich noch im Aufbau befinden, ist eine abschließende Aussage über alle Daten, die für die Schullaufbahn notwendig sind, noch nicht möglich. Sobald diese abgeschlossen ist, wird es eine Ergänzung der VV-Schulakten geben.

Hinsichtlich des Umgangs mit Schülerakten bestimmt Nr. 9 Abs. 1 Satz 2 VV-Schulakten nun, daß die Schulleitung für die einheitliche Führung der Schülerakten zu sorgen hat und in Zweifelsfällen entscheidet, ob eine Eintragung in die Schülerakte erfolgt oder Unterlagen zur Schülerakte genommen werden. Da ein Einsichts- und Auskunftsrecht bereits in Nr. 9 der VV-Datenschutz/Statistik enthalten ist, wird eine von mir geforderte Regelung als unnötige Doppelung angesehen.

5.1.2 Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg (AufnV)[140]

Zum Erlaß dieser Verordnung war das MBJS gem. § 36 Abs. 3 Erstes Schulreformgesetz (1. SRG)[141] ermächtigt. Sie regelt die Voraussetzungen, unter denen die Aufnahme in eine Schule mit dem gewünschten Bildungsgang in der Sekundarstufe I oder der Gymnasialen Oberstufe unter Berücksichtigung der begrenzten Aufnahmekapazitäten geschehen soll.

In § 4 Satz 1 des Verordnungsentwurfes sollen die Eltern "gehalten" sein, "der Schulleitung zur Überprüfung eines Rechtsanspruchs auf Aufnahme in eine weiterführende Schule die erforderlichen Angaben zu machen". Zur Normenklarheit habe ich vorgeschlagen, entweder einen abschließenden Katalog der notwendigen Angaben aufzunehmen oder einen Verweis auf die konkreten Vorschriften des jeweiligen Aufnahmeverfahrens. Das Ministerium hat sich für letzteres entschieden.

Das Anmeldeverfahren für den weiteren Bildungsgang in der Sekundarstufe I legt fest, daß die Kopien des Grundschulgutachtens und des Halbjahreszeugnisses allen Unterlagen beizulegen sind, wobei an keiner Stelle der Aufbewahrungsort und die Aufbewahrungsdauer festgeschrieben wurde. Da die Hinzuziehung der VV-Schulakten[142] keinen Aufschluß über diesen Umstand gab, sollte hier eine Ergänzung erfolgen.

Zur Eignungsfeststellung nach § 8 Abs. 3 Satz 1 AufnV sieht der Entwurf vor, daß die Schulleitungen mit den Eltern und Schülern Gespräche führen, die zu protokollieren sind. Auch hier fehlt eine Konkretisierung hinsichtlich des Aufbewahrungsortes und der Dauer. Soweit die Protokolle für die Aufgabenerfüllung nicht mehr erforderlich sind, habe ich deren unverzügliche Vernichtung gefordert.

Die inzwischen in Kraft getretene Verordnung enthält nun in § 1 Abs. 3 AufnV erfreulicherweise die Festlegung über eine einjährige Aufbewahrungsfrist sowohl von Anmeldeunterlagen, Gesprächsprotokollen und Aufnahmeentscheidungsunterlagen. Die Aussonderung und Vernichtung erfolgt nach den Verwaltungsvorschriften über Akten an Schulen in öffentlicher Trägerschaft in der jeweils geltenden Fassung.

5.1.3 Entwurf: Nichtschülerprüfungsverordnung (PO-Nsch)

Durch das Ablegen einer Nichtschülerprüfung nach der PO-Nsch können schulische Abschlüsse der Sekundarstufe I, der schulische Teil der Fachhochschulreife, die allgemeine Hochschulreife und berufsqualifizierende Abschlüsse auch ohne Besuch einer öffentlichen Schule erworben werden. In meiner Stellungnahme hierzu habe ich angeregt, darin enthaltene Einzelbestimmungen im Sinne einer Normenklarheit zu präzisieren, so sollte z. B. der Umfang der Verschwiegenheitsverpflichtung gem. § 5 Abs. 5 PO-Nsch in der Weise klargestellt werden, daß eine solche Pflicht "über alle Prüfungsvorgänge" besteht.

Diese Anregung beabsichtigt das Ministerium zu berücksichtigen. Darüber hinaus hatte ich um Klärung gebeten, inwieweit es erforderlich ist, die Namen der Zuhörenden in den anzufertigenden Prüfungsniederschriften festzuhalten und warum nicht auch die Teilnahme von landesbediensteten Lehrkräften sowie Lehramtsanwärtern die Zustimmung durch den Prüfling erfordert.

140

141 vom 23. Dezember 1994, GVBl. II 1995, S. 66

142 i. d. Fassung 1. Juli 1992, GVBl. S. 258, zul. geänd. 13. Juli 1994, GVBl. I S. 384

vom 17. November 1994, ABl. MBJS 1994, S. 884

Das Ministerium hält die Angabe der Namen der Zuhörenden in den Prüfungsniederschriften für erforderlich, um ggf. überprüfen zu können, wer unberechtigterweise Prüfungsthemen oder Informationen über Prüflinge weitergegeben und damit gegen die Verschwiegenheitsverpflichtung verstoßen hat. Die erweiterte Zustimmung des Prüflings über Zuhörende wäre nicht erforderlich, da die Nichtschülerprüfung zu den Tätigkeitspflichten von landesbediensteten Lehrkräften bzw. zur Ausbildung von Lehramtsanwärtern gehört. Dem ist nicht zu widersprechen.

5.1.4 Entwurf: Verwaltungsvorschriften über die Durchführung von Hausunterricht (VV-Hausunterricht)

Diese Verwaltungsvorschriften sollen den Anspruch auf Hausunterricht für Kinder und Jugendliche regeln, die wegen einer akuten bzw. chronischen Erkrankung über längere Zeit nicht bzw. nur regelmäßig eingeschränkt eine Schule besuchen können oder für die ein Schulweg und die physische Mindestanforderung während des Unterrichts unzumutbar belastend wäre. Das staatliche Schulamt ordnet Hausunterricht auf Grundlage eines ärztlichen und im Zweifelsfall eines amtsärztlichen Gutachtens an, für dessen Aufbewahrung datenschutzgerechte Regelungen festzulegen sind, zumal nach Nr. 7 der VV-Schulakten[143] die Gutachten bisher nicht als Bestandteile der Schülerakten aufgeführt sind.

Ich habe ihre separate Aufbewahrung angeregt, darüber hinaus sollte den Erziehungsberechtigten oder dem volljährigen Schüler die Möglichkeit eingeräumt werden, auf Antrag hin überprüfen zu lassen, ob das in der Schulakte abgelegte ärztliche Gutachten spätestens 10 Jahre nach Abmeldung vom Schulbesuch überhaupt noch benötigt wird.

Wenn eine andere als die bisher besuchte Schule mit der Durchführung des Hausunterrichts beauftragt ist, wird gem. Nr. 3 Abs. 10 der VV-Schulakten über die betreuten Schüler eine Akte angelegt, die nach Beendigung des Hausunterrichts an die bisherige Schule gesandt und der Schülerakte beigelegt wird. Hier müßte ebenfalls eine Überprüfungsmöglichkeit hinsichtlich der Aufbewahrungsdauer und der getrennten Aufbewahrung des ärztlichen Gutachtens bestehen.

5.1.5 Rundschreiben: Übergang aus der Jahrgangsstufe 6 der Primarstufe in die Jahrgangsstufe 7 einer Schule der Sekundarstufe 1 (§ 11 AO-GS vom 21. Juni 1991)[144] - Stand: 05.12.1994 sowie zum Entwurf der "Verordnung zur Änderung der Ausbildungsordnung der Grundschule im Land Brandenburg" - Stand: 02.12.1994

Nach § 9 i. V. m. § 11 Brandenburgische Ausbildungsordnung der Grundschule (AO-GS) sind die Eltern der Schüler der Klasse 6 im ersten Schulhalbjahr in einer Klassenelternversammlung über die Angebote, die Voraussetzungen und die Ziele der weiterführenden Schulen sowie über die örtlichen Gegebenheiten zu informieren. Für dieses Verfahren der Elternberatung sowie der Erstellung der Grundschulgutachten und Bildungsgangempfehlungen sind im Vorgriff auf eine Änderungsverordnung zu § 11 Abs. 2 und 4 der AO-GS Regelungen in dem o. g. Rundschreiben aufgestellt worden.

Hinsichtlich der individuellen Beratung legt das Rundschreiben u. a. fest, daß über das Beratungsgespräch ein Protokoll zu fertigen ist. Ich habe bemängelt, daß nicht ersichtlich ist, wo und wielange dieses Protokoll aufbewahrt werden soll und hierzu Änderungen des § 11 Abs. 2 AO-GS angeregt.

143

144 vom 17. November 1994, ABl. MBJS, S. 884

vom 21. Juni 1991, GVBl., S. 324, geänd. durch 1. ÄndVO vom 20. Mai 1994, GVBl. II S. 486

Das MBJS hat das als Nr. 87/94[145] gekennzeichnete Rundschreiben zwischenzeitlich bekanntgegeben und meine Änderungsvorschläge zur Aufbewahrung und Vernichtung der Protokolle folgendermaßen berücksichtigt. Für die Protokolle über das individuelle Beratungsgespräch, über den Beschluß der Klassenkonferenz zum Grundschulgutachten und der Empfehlung für einen weiterführenden Bildungsgang sowie über die von den Eltern gegen das Gutachten vorgetragenen Bedenken ist eine einjährige Aufbewahrungsfrist durch die Schulleitung der Grundschule festgelegt worden. Nach Ablauf dieser Frist erfolgt die Aussonderung und Vernichtung dieser Gutachten nach der Verwaltungsvorschrift über Akten an Schulen in öffentlicher Trägerschaft in der jeweils geltenden Fassung.

5.1.6 Förderausschußverfahren

Das MBJS beabsichtigte, eine Broschüre über die "Feststellung des sonderpädagogischen Förderbedarfs - Förderausschußverfahren" herauszugeben, und bat mich hierzu um Stellungnahme. Das dort beschriebene Verfahren beruht auf den Bestimmungen der "Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf (SopV)"[146], an deren Abfassung ich jedoch nicht beteiligt worden bin.

Diese Veröffentlichung hat keinen rechtsverbindlichen Charakter. Sie kann auch eine Verwaltungsvorschrift ersetzen. Dennoch sollen laut Vorwort "verbindliche Vorgaben zu Vorbereitung und Durchführung des Verfahrens" gegeben werden. Die Verbindlichkeit betrifft auch die im "Anhang beigefügten Vorlagen für Schülerunterlagen". Dazu zählt u. a. der Antrag zum Verfahren, in dem eine Einverständniserklärung der Eltern aufgenommen worden ist. Dies wäre somit praktisch eine bereichsspezifische datenschutzrechtliche Regelung, die jedoch nach dem Volkszählungsurteil des Bundesverfassungsgerichts[147] einem Gesetz vorbehalten ist. Bisher ist es sowohl im 1. Schulreformgesetz als auch in der Sop-V versäumt worden, einen angemessenen datenschutzrechtlichen Standard zu erreichen. Diese Vorgehensweise ist völlig unakzeptabel.

Unabhängig davon habe ich u. a. auf verschiedene Punkte hingewiesen. Vor allem ist die im Antrag enthaltene Einverständniserklärung der Erziehungsberechtigten pauschal abgefaßt. Darin ist vorgesehen, daß für die Zusammenarbeit im Förderausschuß die Psychologen, Lehrer, Sonderpädagogen und der Arzt von der Schweigepflicht entbunden werden. Außerdem sollen damit die Eltern ihre Zustimmung geben, daß im Rahmen dieses Verfahrens die erforderlichen Unterlagen von dem genannten Personenkreis eingesehen werden dürfen. Da zu Beginn der Beratung des Förderausschusses noch gar nicht absehbar ist, welche schweigepflichtigen Personen zu welchen Teilen des schulischen und außerschulischen Umfeldes des Kindes befragt werden müssen, können die Eltern wirksam i. S. v. § 4 Abs. 2 SopV nur hinsichtlich des festgelegten Schülerkreises des Förderausschusses gem. § 3 Abs. 4 in der Weise ihre schriftliche Einwilligung erklären, daß das jeweilige Gutachten oder die Information in den Förderausschuß eingeht.

Darüber hinaus sollte unbedingt den Erziehungsberechtigten die Möglichkeit eingeräumt werden, auf Antrag prüfen zu lassen, ob in der Schülerakte festgehaltene Informationen noch benötigt werden. Denn jeder spätere Klassenlehrer wird das Fördergutachten lesen und seine Schlüsse daraus ziehen können. Diese können einerseits im Interesse des behinderten Schülers liegen, andererseits dokumentieren sie auch auf Dauer seine Stigmatisierung.

Das MBJS hat mir telefonisch zugesagt, daß es meine Anregungen aufnehmen wird.

145

146 ABl. des MBJS vom 8. Februar 1995, S. 54 ff.

147 vom 30. November 1992, ABl. MBJS 1993, S. 529
BVerfGE 65, 1

5.1.7 Einsichtnahme in Akten während eines Schülerpraktikums

Während eines Schülerpraktikums in der öffentlichen Verwaltung hatte ein Schüler Zugang zu sehr sensiblen personenbezogenen Daten über die Eltern eines Mitschülers und hat diese ihm gegenüber offenbart. Das gab mir Anlaß, beim zuständigen Ministerium nachzufragen, inwieweit Schüler überhaupt auf datenschutzrechtliche Belange in Zusammenhang mit Akten hingewiesen werden. Dazu gibt es ein Mitteilungsblatt des MBJS mit dem Titel "Merkblatt für Betriebe zur Durchführung von Schülerpraktika", wonach den Schülern im Sinne der allgemeinen Bildungs- und Erziehungsziele des Ersten Schulreformgesetzes für das Land Brandenburg Gelegenheit gegeben werden soll, "...einen Einblick in die Berufs- und Arbeitswelt einschl. ihrer sozialen Strukturen zu erhalten, um die im Unterricht erworbenen Erkenntnisse und Einsichten durch eigenen Erfahrungs- und Erlebnisbezug vertiefen zu können ...".

Ich habe vorgeschlagen, das Merkblatt um die Verpflichtung dahingehend zu ergänzen, daß die Verwaltung dafür Sorge tragen soll, daß die erforderlichen technischen und organisatorischen Maßnahmen zur Durchsetzung datenschutzrechtlicher Erfordernisse vor Beginn der Praktika zu sichern sind. Dies hat das Ministerium unterdessen umgesetzt und mir darüber hinaus zugesichert, die Verwaltungsvorschrift "Schülerbetriebspraktika"[148] in diesem Sinne eindeutig abzufassen.

148 vom 22. Mai 1993 ABl. MBJS, S. 404, geänd. durch Verwaltungsvorschriften vom 25. Februar 1993, ABl. MBJS, S. 131

5.2 Lehrer und Schüler nicht ohne Sorgen

5.2.1 Einsatz privater PC zu Hause durch die Lehrer

Lehrer, Schulräte und auch das MBJS hat im Berichtszeitraum die Frage bewegt, ob gegen die Verarbeitung von Schülerdaten (Name, Anschrift, Geburtsort, Geburtsdatum und Bewertungen der Schüler) auf eigenem PC zu Hause datenschutzrechtliche Bedenken bestehen. Da bisher keine spezialgesetzlichen Vorschriften im Schulwesen existieren und sich der einzelne Lehrer durch den Einsatz eines privaten Rechners meiner Kontrollmöglichkeit entzieht, habe ich eine solche Datenverarbeitung als datenschutzrechtlich unzulässig bewertet. Nach § 26 Brandenburgisches Datenschutzgesetz habe ich nur ein ungehindertes Zugangsrecht zu den Räumen öffentlicher Stellen, in denen Daten verarbeitet werden. Das erstreckt sich jedoch nicht auf Privaträume, weil nach Art. 13 Grundgesetz die Unverletzlichkeit der Wohnung entgegensteht.

Bei Beibehaltung dieser augenblicklichen Rechtslage - das haben inzwischen die Erfahrungen aus anderen Bundesländer gezeigt - werden die Lehrer in die Illegalität getrieben. Denn da die zunehmende Technisierung auch vor der Lehrerschaft der hiesigen Schulen nicht haltmacht, gibt es bereits jetzt eine Reihe von technischen Möglichkeiten, u. a. schulverwaltende Tätigkeiten, die Gestaltung des Kurssystems in der gymnasialen Oberstufe sowie das Ausfüllen der Zeugnisse zeitsparend am PC zu erledigen. Dafür dürfen aber derzeit gem. Nr. 3 Abs. 1 der Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und statistische Erhebungen (VV Datenschutz/Statistik)[149] nur in der Schule stehende Datenverarbeitungsgeräte eingesetzt werden. Dies wird sich auf Dauer nicht aufrechterhalten lassen.

Das Ministerium bat mich daher um Stellungnahme, ob eine der hessischen Regelung angelehnte Vorschrift über den Einsatz von privaten PC meine Zustimmung finden würde. Diese sieht vor, daß auf Antrag der Schulleiter in begründeten Fällen gestatten kann, daß Lehrer Daten von Schülern auf Datenverarbeitungsgeräten außerhalb der Schule verarbeiten können. Dies setzt aber eine Einverständniserklärung des einzelnen Lehrers mit einer Kontrolle durch den Landesbeauftragten für den Datenschutz voraus.

Ich halte dies ins Auge gefaßte Verfahren für überlegenswert und habe meine Zustimmung davon abhängig gemacht, daß die Schule auch bei Benutzung eines privaten PC der jeweiligen Lehrkraft zu Hause dennoch speichernde Stelle i. S. v. § 8 Abs. 1 Bbg DSG bleibt. Die Angelegenheit werde ich unter besonderer Beachtung der damit zusammenhängenden und in Art. 13 Grundgesetz garantierten Unverletzlichkeit der Wohnung weiterverfolgen und zu gegebener Zeit darüber berichten.

5.2.2 Weitergabe von Notenlisten an Sekretärinnen und Schulleiter

Ist die Eintragung von Einzelnoten zum Zwecke der Weitergabe an die Eltern durch andere als den Fachlehrer zulässig? Mit dieser Frage habe ich mich im Rahmen einer Eingabe beschäftigt. Darin wurde mir die Gepflogenheit berichtet, daß die Notenhefte im Sekretariat liegen, damit die Sekretärin Zugriff zu diesen Heften hat, um bei telefonischen Anfragen der Eltern Auskünfte erteilen zu können.

Diese Vorgehensweise war nicht hinnehmbar. Sie entsprach im übrigen nicht einmal der einschlägigen Verwaltungsvorschrift über Akten an Schulen (VV-Schulakten)[150] in

---

149

150 vom 26. November 1993, ABl., S. 1730; ABl. MBJS 1994, S. 85
vom 17. November 1994, ABl. MBJS 1994, S. 884

öffentlicher Trägerschaft, die in Nr. 6 Abs. 4 Satz 1 bestimmt, daß die Notenbücher außerhalb der Unterrichtsräume unter Verschluß zu halten sind. Es werden diejenigen Personen abschließend aufgeführt, die im Rahmen der Erfüllung ihrer dienstlichen Aufgaben darin Einsicht nehmen dürfen; Sekretärinnen gehören nicht dazu, so daß diese auch nicht befugt sind, Auskunft über den Leistungsstand zu geben.

Des weiteren stellte sich die Frage, ob die Schulleitung zur routinemäßigen Kontrolle regelmäßig die Notenhefte einsehen darf. Hierzu habe ich festgestellt, daß es nach § 45 Abs. 3 Satz 4 1. SRG zu den vorrangigen Aufgaben der Schulleiter gehört, in Zusammenarbeit mit Lehrern, Eltern und Schülern auf gute Unterrichts- und Arbeitsbedingungen hinzuwirken. § 45 Abs. 5 Satz 3 1. SRG regelt, daß in die Unterrichts- und Erziehungsarbeit von Lehrern nur dann eingegriffen werden darf, wenn gegen geltende Vorschriften, Anordnungen der Schulaufsichtsbehörden oder Beschlüsse von Mitwirkungsorganen verstoßen wird oder wenn eine geordnete Unterrichts- und Erziehungsarbeit nicht gewährleistet ist. Das in der VV-Schulakten vorgesehene Einsichtsrecht der Schulleiter im Rahmen der Erfüllung ihrer dienstlichen Aufgaben schließt ein unabhängig von einer Beschwerde bestehendes Einsichtsrecht in die Notenhefte nicht ein. Diese Einsichtnahme durch die Schulleitung kann auch nicht mit der Begründung einer rechtzeitigen Steuerung und Korrektur zur Verhinderung von Ausfällen bei den Schülern gerechtfertigt werden.

5.2.3 Alte Zöpfe bei Einschulungsuntersuchungen

Vom Deutschen Kinderschutzbund erreichte mich eine Meldung, daß bei der Einschulungsuntersuchung von Kindern während der gesamten - auch ärztlichen Untersuchung - neben dem Arzt und ggf. medizinischem Hilfspersonal auch der Schulleiter und die künftige Klassenlehrerin des Kindes anwesend waren. Der leitende Schularzt bestätigte diese Verfahrensweise und verwies auf eine jahrelang entsprechende Praxis, die "sich bewährt habe".

Die gleichzeitige Anwesenheit eines Lehrers sowie des Schulleiters bei der schulärztlichen Einschulungsuntersuchung verstößt gegen das Erste Schulreformgesetz für das Land Brandenburg (1. SRG)[151] und darüber hinaus auch gegen die Ausbildungsordnung für die Grundschule (AO-GS)[152]. Insbesondere wird dabei ein Straftatbestand (Verstoß gegen die ärztliche Schweigepflicht) gem. § 203 StGB erfüllt.

Der zukünftige Klassenlehrer eines zu untersuchenden Schulkindes hat keinen Anspruch auf Übermittlung und damit Kenntnisnahme des Schuluntersuchungsergebnisses, da er weder als Lehrer an der Entscheidung der Schulaufnahme nach § 3 Abs. 3 der AO-GS beteiligt ist, noch ihm das Ergebnis des schulärztlichen Gutachtens vorgelegt werden darf. Dementsprechend ist auch dessen Anwesenheit bei der Einschulungsuntersuchung zu untersagen. Auch die Teilnahme des Schulleiters war aus meiner Sicht nicht korrekt. Der Schulleiter hat die schulärztliche Untersuchung abzuwarten und nur auf der Grundlage des Ergebnisses des schulärztlichen Gutachtens seine Entscheidung hinsichtlich der Einschulung zu fällen.

Die zuständigen Stellen, an die ich mich wegen der Eingabe gewandt hatte, bestätigten mir, daß in Zukunft während der Einschulungsuntersuchungen aus datenschutzrechtlichen Gründen die Anwesenheit der künftigen Schulleiter bzw. Klassenlehrer nicht mehr gestattet werde. Um dies landesweit durchzusetzen, hat das Ministerium die notwendigen Maßnahmen gegenüber allen Amtsärzten der Landkreise und kreisfreien Städte eingeleitet.

---

151 vom 1. Juli 1992, GVBl. I S. 258, zul. geänd. 13. Juli 1995, GVBl. I , S. 384

152 vom 21. Juni 1991, GVBl. I S. 324

5.2.4 Schadensersatz oder Zeugnis - der Datenschutz hilft

Einer Schülerin war der für einen Wandertag ausgeliehene Schulvolleyball beim Spielen durch ein Auto plattgefahren worden. Aus angeblichen Datenschutzgründen erhielt sie daraufhin von ihrem Klassenlehrer kein Zeugnis.

Die Bearbeitung der Eingabe gestaltete sich wegen der unzulänglichen Zuarbeit der zuständigen Stellen zeitraubend. Die Einlassung der zuständigen Stellen entsprach nicht den Unterstützungspflichten gem. § 26 Bbg DSG. So nannte mir das MBJS eine Schule, die nicht existierte. Mit meiner telefonischen Nachfrage bei dem Leiter des zuständigen Schulamtes hatte ich ebenfalls wenig Erfolg, da dort meine Anfrage zu diesem Vorfall als "unverständliche Einmischung" gewertet wurde. Daraufhin habe ich mich an die mir unterdessen bekannt gewordene Schule gewandt und diese aufgeklärt.

Aus dem allgemeinen Auskunftsrecht nach § 18 Abs. 1 Bbg DSG läßt sich auch ein unmittelbarer Anspruch auf konkrete Auskunft über Benotungen auf Antrag ableiten. Der Auskunftsanspruch umfaßt alle zur Person des Betroffenen gespeicherten personenbezogenen Daten, zu denen auch die Zeugnisnoten der Schülerin gehören, und schließt grundsätzlich auch das Recht auf Abschriften ein. Nach § 18 Abs. 4 Bbg DSG bleibt es dem pflichtgemäßen Ermessen der speichernden Stelle überlassen, die Auskunftserteilung durch Übersendung einer Abschrift oder eines Speicherauszuges zu ermöglichen.

Die Rechtslage habe ich dem Schulleiter mitgeteilt. Erst danach kam Bewegung in die Angelegenheit. Die Schülerin erhielt ihr Zeugnis. Des weiteren beauftragte das Schulamt die beiden Klassenlehrer, ein klärendes Gespräch mit den Eltern des Schulkindes u. a. über den Schadensersatz zu führen. Der Vorfall wurde zum Anlaß genommen, das Lehrerkollegium über den Umgang mit personenbezogenen Daten zu belehren.

6 Wissenschaft, Forschung und Kultur

6.1 Behindert Datenschutz die Forschung?

Die Frage, ob Datenschutz die Forschung behindere, wird häufig von Wissenschaftlern bejaht, teilweise wird nicht einmal davor zurückgeschreckt, medienwirksam zu behaupten, Datenschutz torpediere die Forschung. Dabei geht es im Kern - wie bei allen anderen datenschutzrechtlichen Problemfeldern auch - nur darum, einen Interessenausgleich mittels "praktischer Konkordanz" zwischen zwei konkurrierenden Grundrechten herzustellen. Wenn also eine Reihe von Wissenschaftsgebieten bzw. deren Forscher in Übereinstimmung mit dem Grundrecht Freiheit der Forschung nach Art. 5 Abs. 3 Grundgesetz (GG) den einzelnen Menschen als konkretes Objekt ihrer Forschung benötigen, dann müssen diese auch respektieren, daß sie mit ihren vielfältigen Datenwünschen in das Recht auf informationelle Selbstbestimmung - abgeleitet vom Allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i. V. m. Art 1 Abs. 1 GG - unmittelbar eingreifen. Ein bloßes Objekt-Sein kann hier nicht erwartet werden, denn ein solches Verständnis würde kraß im Widerspruch zum aktiv zu gebrauchenden Recht auf informationelle Selbstbestimmung stehen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, es sei denn, ein überwiegendes Allgemeininteresse schränkt dieses Recht auf der Grundlage eines Gesetzes ein.

Für die Eingriffe in das Recht auf informationelle Selbstbestimmung haben der Bundes- und Landesgesetzgeber in den allgemeinen Datenschutzgesetzen Forschungsklauseln (§ 30 BDSG bzw. § 28 Bbg DSG) vorgesehen. Darüber hinaus enthalten wegen der spezifischen Art der Daten einige Spezialgesetze (z. B. Sozialdaten - § 75 SGB X, Meldedaten - § 32 Abs. 3 BbgMeldeG, Archivdaten - § 9 BbgArchivG) eigene Forschungsregelungen. Schließlich sind

verschiedene Gesetze auf datenvorhaltende öffentliche Stellen (z. B. statistische Ämter - Statistikgesetze, Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik - Stasi-Unterlagen-Gesetz, Meldebehörden - Landesmeldegesetz) ausgerichtet.

Damit ist für den Wissenschaftler der Weg zu den von ihm begehrten Daten weitgehend vorgeschrieben. Für die angesprochene Zielvorstellung ("praktische Konkordanz") hat der Verantwortliche für ein Forschungsprojekt in der Vorbereitungsphase dafür methodisch die Frage der Erforderlichkeit des Grundrechtseingriffs und dessen Intensität zu prüfen. Ersteres ist zu verneinen, wenn mit "milderen Mitteln" - beispielsweise ohne Verwendung von personenbezogenen Daten - der angestrebte wissenschaftliche Zweck ebenfalls erreicht wird. Sollte nach Inbetrachtziehung anderer Alternativen in diesen Fällen trotzdem auf einen Grundrechtseingriff nicht verzichtet werden, dann wäre (auch wenn die Einwilligung der Probanden vorliegt) diese Vorgehensweise unverhältnismäßig und insoweit ebenfalls nicht verfasssungskonform. Wenn die Verwendung von personenbezogenen Daten jedoch bejaht werden muß, dann ist zu prüfen, ob

- die für die Erfassung vorgesehenen Daten geeignet sind, den Zweck des speziellen Projektes zu fördern,

- unter mehreren geeigneten Methoden diejenige ausgewählt wurde, mit der die geringste Beeinträchtigung des Betroffenen verbunden ist und

- die mit der ausgewählten Maßnahme verbundene Beeinträchtigung in einem angemessenen Verhältnis zum Untersuchungszweck steht.

Grundsätzlich kann die Forschung nur in Zusammenarbeit mit den Betroffenen und nicht an ihnen vorbei betrieben werden. Im Idealfall gelingt es dem Forscher, ein "Arbeitsbündnis" mit den Betroffenen zu schließen, deren Daten er für seine Zwecke nutzen will. Voraussetzung ist die Kenntnis über ein inzwischen erprobtes Methodenarsenal.

6.1.1 Anonymisierung bei Forschungsvorhaben

Im Gegensatz zu personenbezogenen Daten, die gem. § 3 Abs. 1 Bbg DSG Einzelangaben über persönliche und sächliche Verhältnisse einer bestimmten oder zumindest einer bestimmbaren natürlichen Person (Betroffener) darstellen, sind anonyme Daten Einzelangaben, die keinen Personenbezug ermöglichen. Wird durch ein Verfahren sichergestellt, daß dieser qualitative Umschlag - Verlust des Personenbezugs - erreicht wird, endet gleichzeitig das grundrechtlich geschützte Recht des einzelnen, "über die Preisgabe und Verwendung seiner persönlichen Daten" zu entscheiden[153], und damit ist die Konkurrenzsituation zwischen den Grundrechten Freiheit in der Forschung und Recht auf informationelle Selbstbestimmung aufgelöst.

In der Praxis gibt es allerdings fließende Übergänge zwischen den personenbezogenen Daten einer bestimmten bzw. bestimmbaren Person und anonymisierten Daten; ihre Abgrenzung bereitet Schwierigkeiten. So handelt es sich nur um "formal anonymisierte Daten", wenn lediglich der Name und ggf. die Adresse vom sonstigen Datensatz abgetrennt werden. Die Person kann dann weiterhin anhand der vorliegenden Einzelangaben identifiziert werden oder dies gelingt Dritten durch vorhandenes Zusatzwissen, mittels technischer Möglichkeiten der Datenverarbeitung, aufgrund der zur Verfügung stehenden Zeit oder durch Kombination dieser drei Möglichkeiten.

---

153 BVerfGE 65,1 (43)

Es sei dahingestellt, wann Daten tatsächlich anonym im Sinne von "absolut anonym" - also nicht mehr personenbeziehbar - sind. Um das Problem jedoch überhaupt handhaben zu können, spricht man von "faktisch anonymisierten Daten", wenn eine Person nur mit einem völlig unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitsaufwand reidentifiziert werden kann[154]. Von dieser Definition für Anonymisierung gehen sowohl § 3 Abs. 7 BDSG als auch § 3 Abs. 3 Bbg DSG aus.

Bei Forschungsvorhaben, in denen zunächst auf personenbezogene Daten zugegriffen werden soll, sind die für eine faktische Anonymisierung notwendigen Schritte gem. § 28 Abs. 3 Bbg DSG immer so früh wie möglich einzuleiten. Hierzu bieten sich eine Reihe unterschiedlicher Verfahren an:

- formales Anonymisieren von Datensätzen,
- Überführen der Datensätze auf eine höhere Abstraktionsebene,
- Einstreuen von Zufallsfehlern,
- Zerlegen von Datensätzen in separate Merkmalsbereiche,
- Ziehen von Unterstichproben sowie
- Nutzen von Schlüsseln und Codierungen.

Darüber hinaus läßt sich zusätzlich durch technische und organisatorische Maßnahmen die Wahrscheinlichkeit einer Deanonymisierung von Daten reduzieren. Dabei ist an das Trennungs- und Löschungsgebot, ein strafbewährtes Reidentifizierungs- und Übermittlungsverbot und eine Aufzeichnungspflicht bei Zugriffen auf Datenbestände zu denken.

6.1.2 Daten mit Doppelbezug

Insbesondere bei medizinischen Forschungsvorhaben werden im Zusammenhang mit Interviews oder Fragebogenerhebungen beim Betroffenen häufig Daten erhoben, die auch als personenbezogene Daten Dritter (des Partners, der Eltern usw.) anzusehen sind. Da aufgrund des Rechts auf informationelle Selbstbestimmung personenbezogene Daten grundsätzlich beim Betroffenen und mit dessen Kenntnis zu erheben sind (s. u. a. § 12 Abs. 2 Bbg DSG, § 13 Abs. 2 BDSG), stellt sich deshalb hier die Frage, ob und unter welchen Voraussetzungen diese Erhebung von Daten auch von Dritten hinnehmbar wäre.

Auf keinen Fall darf die Anonymität Dritter schon durch die Anlage des jeweiligen Forschungsvorhabens in Frage gestellt werden. Um dies im konkreten Einzelfall auszuschließen, scheint mir die Prüfung anhand folgender zwei Kriterien hilfreich zu sein:

- Welchen Grad der Anonymisierung weisen die erhobenen Daten auf, so daß ihre Deanonymisierung ausgeschlossen werden kann (s. unter 6.1.1)?

- Läßt sich allein schon durch den Charakter der erhobenen Daten (z. B. Verwandtschaftsgrad) ein Personenbezug herstellen (s. unter 6.2.5)?

Falls insoweit die Daten mit Doppelbezug als nicht ausreichend anonymisiert anzusehen sind, dürfte es unumgänglich sein, daß der Forscher über den Betroffenen die Einwilligung Dritter einholen muß.

6.1.3 Datentreuhänder

Bei der Datentreuhandschaft handelt es sich um ein erst Ende der 80er Jahre speziell bei

---

154 BVerfGE 65,1 (49)

epidemiologischen Untersuchungen eingesetztes Verfahren. Dabei übernimmt der Datentreuhänder die Rolle eines vertrauenswürdigen Dritten (Vermittlers) zwischen der datenspeichernden Stelle, dem betroffenen Personenkreis und der wissenschaftlichen Institution ein. Insofern kann dadurch der Schutz der personenbezogenen Daten gewährleistet und gleichzeitig der Datenbedarf der Forschung mit Hilfe von anonymisierten Daten gedeckt werden.

Dies setzt voraus, daß Datentreuhänder - entweder als eigenständige private oder staatliche Einrichtung - gegenüber Dritten, wie Statistikstellen, abgeschottet werden und die bei ihnen gespeicherten Daten darüber hinaus durch Beschlagnahmeverbot sowie Zeugnisverweigerungsrecht gegen den Zugriff der Strafverfolgungsbehörden geschützt sind. Hierfür fehlen bislang gesonderte gesetzliche Regelungen, die in dieser Weise die Vertrauenswürdigkeit von Datentreuhändern garantieren.

Es sollte überlegt werden, den Datentreuhänder möglichst mit den nachfolgend nur grob skizzierten Funktionen

a) Anonymisierung als Voraussetzung für den Datenzugang durch die Forschung,
(Die Basisfunktion der Datentreuhänder könnte darin liegen, personenbezogene Daten von datenhaltenden Stellen entgegenzunehmen und diese nach der Anonymisierung an wissenschaftliche Institutionen zu übermitteln. Dabei ist zu beachten, daß auch die Übermittlung von Daten zu Zwecken der Anonymisierung an den Datentreuhänder ohne Einwilligung des Betroffenen eine Zweckentfremdung und damit einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, die einer gesetzlichen Regelung bedarf.)

b) Verknüpfung von Daten,
(Datentreuhänder können Daten aus verschiedenen Quellen unter Nutzung des Personenbezugs (Identifikationsdaten oder Kennummer) miteinander verknüpfen und die so neugeordneten Daten nach Maßgaben (z. B. Auswertung, Anonymisierung, Übermittlung) weiter verarbeiten. Die dadurch entstehenden komplexeren Datenbestände müssen gegen den Zugriff Dritter gesichert werden.

Der damit verbundene Grundrechtseingriff kann nur mit Einwilligung der Betroffenen oder aufgrund eines Gesetzes geschehen.

Allerdings scheint der Datentreuhänder ein milderes Mittel im Vergleich mit der direkten Übermittlung personenbezogener Daten an die wissenschaftliche Institution zu sein, weil die Daten nur bei ihm personenbezogen vorliegen. Bei Längsschnittuntersuchungen würde dies bedeuten, daß ein Identifikationsbezug beim Datentreuhänder verbleibt, so daß dieser jederzeit - nicht aber die nutzende Einrichtung - eine personenbezogene Datenzuordnung mit weiteren Daten vornehmen kann.)

c) Haltung, Bereitstellung sowie Archivierung von Daten
(Hierbei ist zwischen Bevorraten von personenbezogenen Datenbeständen als Datenbanken für laufende Forschungsvorhaben und als Archiv für spätere Forschungszwecke zu unterscheiden. In Betracht käme außerdem die Funktion der Errichtung und Betreuung von Forschungsregistern. Nur besteht für die Betroffenen kein Unterschied, ob das dafür erforderliche Gesetz eine Stelle oder einen Datentreuhänder berechtigt, letztere zu führen. Deshalb dürfte sich bei dieser Funktion die Aufgabe des Datentreuhänders im wesentlichen darauf beschränken, daß er die personenbezogenen Daten eigenständig oder nach Weisung des Auftraggebers verarbeitet und diesem lediglich die anonymisierten Ergebnisse zur Verfügung stellt.)

zu beauftragen.

6.1.4 Mortalitäts-follow-up

Abgesehen von der Auswertung der Leichenschauscheine für die Todesursachenstatistik ist bisher in Brandenburg die Frage nicht geregelt, wer darüber hinaus für welche Zwecke Einblick in den Leichenschauschein nehmen darf. Vor allem die medizinische Forschung hat ein hohes Interesse daran, zu erfahren, woran ein bestimmter Mensch gestorben ist. Hierfür kann nur der Betroffene zu Lebzeiten selbst die Einwilligung wirksam erteilen.

In dieser Hinsicht bietet das Mortalitäts-follow-up einen durchführbaren Ausweg. Die wissenschaftliche Einrichtung sendet an das Gesundheitsamt, das die Leichenschauscheine aufbewahrt, eine Liste mit den Identifikationsdaten einschließlich einer Kennummer der Personen, deren Todesursache ermittelt werden soll. Das Gesundheitsamt übermittelt der anfragenden Stelle Kopien der Leichenschauscheine, bei denen Identifikationsdaten entfernt sind und stattdessen die jeweilige Kennummer eingetragen ist.

Voraussetzung dafür ist allerdings, daß bei der anfragenden Stelle die Identifikationsdaten der Personen, deren Todesursache in Erfahrung gebracht werden soll, vor und nicht erst nach Entgegennahme der Rückmeldung des Gesundheitsamtes definitiv gelöscht werden. Denn nur so kann sichergestellt werden, daß eine Zuordnung zwischen Todesursache und Identifikationsdaten der fraglichen Personen wirklich nicht mehr möglich ist; die Rückmeldung erfolgt damit anonym.

6.1.5 Adreßmittlung

Bereits in meinem 2. Tätigkeitsbericht[155] bin ich auf dieses Verfahren als datenschutzrechtlich geeigneten Lösungsweg für Situationen eingegangen, in denen aufgrund verschiedenster Anlässe (u. a. wissenschaftlicher Vorhaben) Privatpersonen oder wissenschaftliche Institutionen an eine öffentliche Stelle (Schule, Behörde, Kammer usw.) mit der Bitte herantreten, die Privatadressen von Absolventen, Betreuten oder Mitgliedern mitzuteilen, ohne daß hierfür eine geeignete Rechtsgrundlage oder die Zustimmung der Betroffenen vorliegt (s. hierzu auch unter 10.3.1).

In solchen Fällen ist lediglich notwendig, daß der Interessent der angeschriebenen Stelle - falls diese zustimmt - vorfrankierte (nicht adressierte) Kuverts mit dem zu übersendenden Material übergibt. Dort werden die Kuverts dann aufgrund des dort vorliegenden Anschriftenmaterials adressiert und verschickt. Der Adressat entscheidet selbst durch seine Rückantwort, daß er sich mit dem Interessenten in Verbindung setzen will. Somit wird vermieden, daß die Adressen Dritten unbefugterweise zur Kenntnis gelangen und daß die Einwilligung zur Nutzung von ursprünglich zu anderen Zwecken gespeicherten Daten eingeholt werden muß.

6.2 Kohortenstudie "Gesundheit, Ernährung, Krebs"

Die Kohortenstudie "Gesundheit, Ernährung, Krebs (GEK)" war nicht das einzige medizinische Forschungsvorhaben, zu dessen Datenschutzkonzeption ich im Verlaufe des Berichtszeitraumes gebeten worden bin, Stellung zu nehmen. Vor allem um unnötige Duplizitäten zu vermeiden, wird aber auf die Darlegung weiterer Forschungsvorhaben verzichtet.

Nach Darstellung des Projektleiters stellt GEK eines der beiden deutschen Teilbeiträge im Rahmen des Programms "Europa gegen den Krebs" dar, das die Variabilität der

---

155 s. unter 5.2.4, S. 94 ff.

Ernährungsformen in Europa ausnutzt, um die Rolle der Ernährung bei der Entstehung chronischer Krankheiten (u. a. Krebs) im einzelnen zu bestimmen. Insgesamt sollen daran 400.000 Personen teilnehmen; für die Teilnahme an GEK wird versucht, 30.000 Männer und Frauen im Alter von 35 bis 64 Jahren zu gewinnen.

Nach der mir ursprünglich angezeigten Vorhabensbeschreibung sollte die Basiserhebung für die GEK-Studie anhand von umfangreichen Fragebögen, eines Interviews und der Untersuchung von biologischen Proben folgende 4 Komplexe umfassen:

- die Erfassung des Lebensmittelverzehrs und die daraus abgeleitete Energie- und Nährstoffaufnahme,
- die Erfassung weiterer Merkmale des Lebensstils, die Einfluß auf das Erkrankungsrisiko nehmen können,
- anthropometrische Messungen sowie
- die Bestimmung von (nicht näher definierten) molekularbiologischen Blut- sowie anderen biochemischen Blut- und Urinparametern.

Eine Liste über beim Probanden zu erfassende Krankheiten wurde später nachgereicht.

Dieser Rekrutierungsphase sollte sich lückenlos die Nachbeobachtungsphase - zunächst über 10 Jahre - anschließen, während der jeder Teilnehmer in einem Abstand von zwei bis vier Jahren schriftlich angesprochen wird, ob Neuerkrankungen bei ihm aufgetreten sind, und wenn ja, sollte durch Mitarbeiter an der Studie bei den mit der Erkrankung befaßten Ärzten die jeweilige Diagnose ermittelt werden. Schließlich sollte ein langfristig angelegtes Mortalitäts-follow-up (s. unter 6.1.4) in die Studie einfließen, d. h., die Leichenschauscheine der an der Studie Beteiligten sollten später hinsichtlich Todesursachen ausgewertet werden. Gegen das Forschungsvorhaben ließen sich keine grundsätzlichen datenschutzrechtlichen Bedenken erheben, da als Rechtsgrundlage hierfür eine Einwilligungserklärung der Probanden gem. § 4 Abs. 1 Buchst. b i. V. m. § 28 Bbg DSG vorgesehen war.

Es mußte allerdings eine Vielzahl von Einzelfragen mühevoll geklärt werden, über die nachfolgend nur ausgewählt berichtet wird. Nachdem dies glücklich erreicht worden war, kam zu meinem Erstaunen der Projektleiter erneut auf mich zu und hielt nunmehr eine "aktuelle Erweiterung" der Studie um eine Familienanamnese für erforderlich, um damit die hereditären Ursachen von selektiv erfaßten Erkrankungen abschätzen zu können.

6.2.1 Ansprechen von potentiellen Teilnehmern

Trotz mehrfacher Berichterstattung in den Medien über das Forschungsvorhaben beschwerten sich Bürger verärgert bei mir darüber, daß sie ein bzw. wiederholt Schreiben erhalten hätten, mit denen sie aufgefordert worden seien, sich an der GEK-Studie zu beteiligen und gleichzeitig gebeten worden seien, sich dafür möglichst an einem vorbezeichneten Termin im GEK-Studienzentrum einzufinden. Teilweise vermuteten sie darin zu Unrecht eine unberechtigte Weitergabe ihrer Daten durch das Meldeamt und baten für die Zukunft um Abhilfe.

Gegen diese Verfahrensweise war in materieller Hinsicht nichts einzuwenden. Das standardisierte Ankündigungsverfahren genügte allerdings nicht den formalen datenschutzrechtlichen Erfordernissen, da es in seinem zweiten Absatz mißverständlich abgefaßt ("Ihre Adresse wurde mit Genehmigung der zuständigen Behörde aus dem Einwohnermelderegister entnommen.") war und es ansonsten zur praktizierten Verfahrensweise keinen Hinweis auf die gesetzliche Grundlage enthielt. Woher sollen Bürger wissen, daß Forschungsinstituten mit § 28 Abs. 3 Brandenburgisches Meldegesetz

(BbgMeldeG)[156] ein Privileg eingeräumt wird, aufgrund dessen sie auf Antrag bei der zuständigen Behörde (Ministerium des Innern) die Genehmigung erhalten können, daß ihnen eine Vielzahl von Adressen nicht namentlich genannter Einwohner (sog. "Gruppenauskunft") zur Verfügung gestellt wird?

6.2.2 Einwilligungserklärung

Die mir zunächst - und im übrigen davor bereits der Ethikkommission der Landesärztekammer Brandenburg - vorgelegte Einwilligungserklärung genügte bei weitem nicht den Anforderungen, die gem. § 4 Abs. 2 i. V. m. § 12 Abs. 3 Bbg DSG daran zu knüpfen sind. Diese bedarf nicht nur der hier vorgesehenen Schriftform; darüber hinaus ist der Betroffene "in geeigneter Weise über die Bedeutung der Einwilligung ... aufzuklären und "unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung ... mit Wirkung für die Zukunft widerrufen kann".

Diese Formulierungen sind nicht zufällig und fast gleichlautend in allen Datenschutzgesetzen aufgenommen worden; der einzelne kann nämlich sein Recht auf informationelle Selbstbestimmung tatsächlich nur wahrnehmen, wenn ihm - als in der Regel absolutem Laien auf dem jeweiligen Forschungsgebiet - auch wirklich verständlich gemacht wird, worin er eigentlich einwilligt. Im vorliegenden Fall kam hinzu, daß der abgefaßte Einwilligungstext im Zusammenhang mit der vorgesehen Untersuchung der Blutprobe viel zu global von der Bestimmung "biochemischer und molekularer Faktoren" sprach. Darunter kann so gut wie alles verstanden werden. Zur Eingrenzung und näheren Definierung dessen, was vorgesehen ist, habe ich vorgeschlagen, wenigstens konkrete Beispiele zu benennen. Dem wurde durch folgenden Zusatz Rechnung getragen: "Es werden Blutwerte untersucht, die zur Klärung des Zusammenhangs von Ernährung und chronischen Erkrankungen beitragen. Dazu gehört z. B. die Bestimmung von Vitaminen und Hormonen. Bei einigen Krankheiten ist es für die Feststellung des Ernährungseinflusses wichtig, im Blut die Erbanlagen zu erkennen."

Der Hinweis auf die Möglichkeit, die zugesagte Teilnahme jederzeit widerrufen zu können, wurde wörtlich aus § 4 Abs. 2 Bbg DSG übernommen. Zur Klarstellung, was "mit Wirkung für die Zukunft" bedeutet, wurde diese Aussage jedoch dahingehend präzisiert, daß damit nur eine Löschung der personenbezogenen Daten in der Adreßdatei, nicht aber der bereits erhobenen Daten erreicht werden kann.

6.2.3 Erforderlichkeit erfaßter Daten

Da bei GEK mit Einwilligung der Betroffenen ihre personenbezogenen Daten erfaßt werden sollten, beschränkte sich hier die Prüfung der Erforderlichkeit darauf, ob die zu erhebenden Angaben für das Vorhaben benötigt werden, um den Zweck der Untersuchung zu fördern. Diesbezüglich bestand lediglich Zweifel bei der Erfassung der Adresse von Verwandten und Zwillingen. Ersteres sollte geschehen, um den Betroffenen im Fall eines Umzuges erreichen zu können. Von dieser Vorstellung nahm das Forschungsinstitut später von selbst Abstand.

Anders verhielt es sich mit der Frage an die Betroffenen, ob sie ein Zwilling sind. Hier war die Begründung, sie stände "im Zusammenhang mit zukünftigen Fragestellungen in der Ernährungsforschung, die dahin tendieren, welchen Anteil die Umwelt und welchen Anteil die genetische Komponente besitzen". Mit der Antwort "Zwilling" wäre es möglich "nachzufragen, ob nicht der andere Zwilling Studienteilnehmer werden will". Europaweit würden dafür mit Berufung auf ein internationales Expertenteam ca. 360.000 Personen gesucht.

---

156 vom 25. Juni 1992, GVBl. I S. 236

Damit war eindeutig, daß es sich hierbei lediglich um eine Bevorratung von Daten handeln würde, kein inhaltlicher Zusammenhang zur eigentlichen Fragestellung der GEK-Studie bestand und ein solches Vorgehen gegen § 12 Abs. 2 Bbg DSG verstoßen würde, wonach personenbezogene Daten grundsätzlich beim Betroffenen mit dessen Kenntnis zu erheben sind.

Auch Betroffene sollten sich nicht davor scheuen, sich die ihnen im Zusammenhang mit Forschungsprojekten gestellten Fragen und deren Zweckbestimmung eingehend erklären zu lassen. Wenn die Forschung ihre Informationserwartung insoweit sowohl gegenüber dem Träger des informationellen Selbstbestimmungsrechts als auch gegenüber meiner Behörde rechtfertigen muß, kann ich darin keine "Zensur" der Forschung sehen.

6.2.4 Behandlung von Auskunftswünschen

Die Datenschutzkonzeption der GEK-Studie sah von Anfang an vor, nach der abgeschlossenen Erstbefragung der Probanden (Interview) die erfaßten Daten nicht ständig personenbezogen vorzuhalten, sondern in zwei Dateien - und diese wiederum mit gestuften Zugriffsrechten getrennt an verschiedenen Orten - aufzubewahren. Die sog. "Adreßdatei" enthält neben dem Namen und der Anschrift für jeden Probanden eine Teilnehmernummer. In einer zweiten Datei sind unter der jeweiligen Teilnehmernummer die eigentlichen Daten einschließlich Befunde abgespeichert. Ich habe diese Verfahrensweise begrüßt, zumal dadurch der Zugriff Unbefugter auf die hier als sehr sensibel einzustufenden personenbezogenen (medizinischen) Daten erst mit wesentlich höherer krimineller Energie möglich ist. Zusätzlich habe ich angeregt, die Dokumentation der Daten in Papierform - bis auf die Einwilligungserklärung - wegen unzulässiger Doppelspeicherung umgehend zu vernichten.

Im Verlauf des ersten Studienjahres hat sich dann ein unerwartet hohes Interesse der Probanden - vor allem an ihren bestimmten Blutwerten - gezeigt, so daß Überlegungen angestellt werden mußten, wie diesen über die zu ihrer Person gespeicherten Daten gem. § 18 Abs. 1 Bbg DSG verfahrensmäßig einfach und risikolos Auskunft erteilt werden kann, ohne daß dabei nicht betroffene Personen Informationen über Dritte (andere Probanden) erhalten. Hierzu wurde mit mir folgendes Verfahren abgestimmt: Aufgrund einer schriftlichen Nachfrage des Teilnehmers findet eine Identifizierung des Absenders anhand der Adresse, des Namens und der angegebenen Teilnehmernummer statt. Hierzu wird auf die Adreßdatei zugegriffen, der Zugriff wird protokolliert. Im Fall einer Übereinstimmung von eingegebenen und gespeicherten Daten wird automatisch ein standardisiertes Antwortschreiben erstellt. In einem zweiten Schritt wird dann der entsprechende Befund aus der eigentlichen Datenbank herausgesucht und auf einem speziellen Datenblatt dokumentiert. Beides erhält der Proband zugesandt.

6.2.5 Familienanamnese

Hierzu bestand die Vorstellung, die Erkrankungen (hier: Herzinfarkt, Schlaganfall, Diabetes, Bluthochdruck und Krebserkrankungen, aufgeschlüsselt nach Organen) von Verwandten ersten Grades (Mutter, Vater, Schwester, Bruder) des Probanden zu erfassen. Ich habe dieses Ansinnen datenschutzrechtlich als völlig unakzeptabel bewertet. Die Speicherung des Verwandtschaftsverhältnisses stellt einen eindeutigen Personenbezug zu einer ganz bestimmten lebenden oder bereits verstorbenen Person her. Selbst wenn diese nicht ohne Zuhilfenahme weiterer Informationen zu identifizieren ist, ergibt sich eben daraus ein Reanonymisierungspotential für Dritte.

Aus dem herstellbaren Personenbezug folgt, daß diese Krankheitsdaten von Verwandten ersten Grades nicht nur - wie gewünscht - die Teilnehmer der Studie umfassender charakterisieren, sondern daß es sich um Angaben handelt, die datenschutzrechtlich zugleich als Daten Dritter anzusehen und dementsprechend zu bewerten sind. Ausschließlich letztere

können darüber entscheiden, ob für sie diese Daten einen schutzwürdigen Belang darstellen oder nicht.

Da es nicht ernsthaft in Betracht zu ziehen war, die Einwilligungserklärung der Verwandten aufgrund des damit verbundenen Aufwandes einzuholen, habe ich dem Projektleiter vorgeschlagen, summarisch die für die Studie interessierenden Krankheiten der Verwandten ersten Grades des Teilnehmers zu erfassen. Ich sehe mit dieser Verfahrensweise ausreichend sowohl das Recht auf informationelle Selbstbestimmung, als auch das Interesse an der Verarbeitung dieser Daten berücksichtigt. Mein Vorschlag wurde zunächst vom Projektleiter akzeptiert, aber kurz darauf fragte er bei mir nach, ob nicht doch wenigstens eine Differenzierung zwischen Erkrankungen statthaft wäre, die vor bzw. nach Erreichen des 50. Lebensjahres aufgetreten sind.

Dagegen mußte ich einwenden, daß damit - zumindest bei einigen der Betroffenen - eine Personenbeziehbarkeit nicht mehr ausgeschlossen werden könne und somit eine rechtlich nicht vertretbare Reanonymisierung vorliegen würde. So müsse es sich bei den jüngeren Teilnehmern an der Studie im Falle der Erkrankungen ihrer Verwandten ersten Grades sehr wahrscheinlich um deren Eltern bzw. in Verbindung mit geschlechtsspezifischen Tumoren um den Vater bzw. die Mutter handeln, wenn diese über der genannten Altersgrenze erkrankt waren. Ich habe deshalb dieser Vorgehensweise nicht zugestimmt.

6.3 Krankheitsregister

Aufgrund des allgemein gestiegenen Gesundheitsbewußtseins in der Bevölkerung sind Politiker zunehmend bereit - unter Hintanstellung bisheriger Kostenargumente - den Aufbau von medizinischen Forschungsregistern massiv zu fördern. Dabei wird der Eindruck erweckt, daß mit solchen Registern bereits die gesicherten Voraussetzungen für die Bekämpfung der jeweiligen Krankheiten geschaffen werden. Hier ist aber Skepsis angezeigt, weil selbst durch eine repräsentative oder Totalerfassung bei den mehrheitlich multifaktorellen Geschehen bislang nur in Ausnahmefällen der Schlüssel zur Aufdeckung von Krankheitsursachen gefunden wurde. Selbst wenn die Brauchbarkeit solcher Ergebnisse vorausgesetzt werden könnte, wären die Ergebnisse nur verwertbar, wenn der politische Wille vorhanden wäre, die erkannten Krankheitsursachen konsequent zu bekämpfen und ggf. die hierfür erforderlichen Mittel bereitzustellen.

In jedem Fall darf angesichts der bestehenden Forschungseuphorie der Eingriff in das Grundrecht auf informationelle Selbstbestimmung und die Offenbarung von Arztgeheimnissen nicht außer Acht gelassen werden, da dabei in der Regel äußerst sensible Daten erfaßt werden, die deshalb teilweise sogar den Betroffenen selbst aus ärztlicher Fürsorge vorenthalten werden.

Bei der Errichtung und Führung von epidemiologischen Krankheitsregistern ist unbedingt die Einhaltung grundsätzlicher Voraussetzungen zu fordern:

- Die Errichtung und Führung eines Krankheitsregisters bedarf eines speziellen Gesetzes. Forschungsklauseln, wie z. B. in § 28 Bbg DSG, genügen dafür nicht, da mit dem ständig anwachsenden Datenpool Forschungsvorhaben realisiert werden sollen, die thematisch und methodisch nicht eingrenzbar sind und auch nicht sein sollen.

- In Krankheitsregister dürfen - sofern keine spezialgesetzlichen Bestimmungen anderes zulassen - Daten nur einfließen, wenn Betroffene (oder deren gesetzliche Vertreter) nach Unterrichtung über die Zwecke der Registrierung und den Umfang der Verarbeitung eingewilligt haben.

- Bei statistischen Auswertungen - auch durch Wissenschaftler - ist sicherzustellen, daß eine

Identifizierung von Personen nicht möglich ist. Das gilt auch für sog. Fall-Kontroll-Studien.

Von Krankheitsregistern sind klinische Behandlungsregister zu unterscheiden. Hier ist die Datenverarbeitung durch den Behandlungsvertrag abgedeckt; dies sollte aber kein Grund sein, daß die behandelnden Ärzte ihre Patienten nicht über die Existenz solcher Register informieren.

6.3.1 Krebsregistergesetz

Entgegen der mehrheitlich von den Ländern bestrittenen Gesetzgebungskompetenz des Bundes in bezug auf ein solches Gesetz[157] ist durch einen Kompromiß im Vermittlungsausschuß des Bundestages und des Bundesrates zwischenzeitlich vom Bund ein Gesetz über Krebsregister (Krebsregistergesetz - KRG)[158] verabschiedet worden. Ich hatte zu Vorentwürfen gegenüber der Landesregierung mehrfach Stellung genommen und darüber hinaus auch wiederholt Kontakt gesucht, doch diese hat sich mit den vorgetragenen Einzelargumentationen mit dem Hinweis nicht auseinandergesetzt, sie würde das Gesetz ablehnen, weil hierzu der Bund keine Regelungskompetenz besäße.

Das Gesetz verpflichtet alle Bundesländer, bis zum 1. Januar 1999 flächendeckend bevölkerungsbezogene Krebsregister einzurichten und zu führen. Es berechtigt die behandelnden Ärzte, verpflichtet sie jedoch nicht, der Vertrauensstelle des jeweiligen Krebsregisters patientenbezogene Daten zu übermitteln. Diese Stelle prüft die gemeldeten Daten auf Schlüssigkeit und Vollständigkeit, nimmt ggf. Berichtigungen nach erfolgten Rückfragen vor, übernimmt die Identitätsdaten und die epidemiologischen Daten auf getrennte Datenträger und übermittelt einen anonymisierten epidemiologischen Datensatz an die räumlich und personell getrennte Registerstelle, wozu eine Kontrollnummer und asymmetrisch verschlüsselte Identitätsdaten gehören, die für Nachmeldungen benötigt werden. Insofern ist auch eine Reidentifikation der erfaßten Datensätze nicht ausgeschlossen und für Forschungszwecke, die einer Genehmigung von den Ländern selbst zu bestimmende Behörde bedürfen, ausdrücklich vorgesehen.

Der Arzt hat seine Patienten über ihr Widerspruchsrecht zur beabsichtigten oder bereits erfolgten Meldung zum frühestmöglichen Zeitpunkt zu unterrichten. Dies darf nur unterbleiben, solange gesundheitliche Nachteile für die Patienten zu erwarten sind. Wenn dann nachträglich durch den Betroffenen Widerspruch eingelegt wird, kann dadurch das Löschen selbst von bereits im Register gespeicherten Daten erreicht werden.

Insofern ist mit der so vorgesehenen anonymisierten Datenspeicherung von Krebspatienten ein Interessenausgleich einerseits zwischen dem Recht auf informationelle Selbstbestimmung und andererseits dem öffentlichen Interesse, derartige Daten für Forschungszwecke nutzen zu können, weitgehend gelungen. Ich bedauere jedoch, daß die Anträge Bayerns im Vermittlungsausschuß zum Zeugnisverweigerungsrecht sowie zum Beschlagnahmeverbot - wie in § 35 Abs. 3 SGB I vorgesehen -, um deren Unterstützung ich die Landesregierung noch vor der entscheidenden Sitzung des Vermittlungsausschusses ausdrücklich gebeten hatte, nicht mehr Berücksichtigung gefunden haben.

Ansonsten ist mit § 13 für die Länder eine Öffnungsklausel aufgenommen worden, Ausführungsgesetze bis spätestens 1999 zu erlassen. Das betrifft u. a. die Erhebung und Meldung epidemiologischer Daten über den vorgegebenen Rahmen hinaus, die Bestimmung der

---

157 s. hierzu in meinem 2. Tätigkeitsbericht unter 7.2.9, S. 123 ff.

158 vom 4. November 1994, BGBl. I S. 3351

zuständigen Genehmigungsbehörde und die weitere Verarbeitung und Nutzung von Daten aus vor Inkrafttreten des Gesetzes bereits bestehenden Krebsregistern (s. hierzu unter 7.3.1.2).

Darüber hinaus haben die Krebsregister der Länder einmal jährlich anonymisierte epidemiologische Daten für die "Dachdokumentation Krebs" an das in Berlin ansässige Robert-Koch-Institut zu übermitteln.

6.3.2 Fehlbildungsregister bei Neugeborenen

Weniger bekannt dürften Bemühungen - insbesondere seitens der Bundesärztekammer und einzelner Universitätsinstitute - sein, flächendeckende Fehlbildungsregister einzurichten, um die unbefriedigend geklärten Ursachen von Fehlbildungen zu erforschen. Ihre Einrichtung ist problematisch, da

- zum Erhalt valider Daten in ein solches Register jährlich die Datensätze von mindestens 4.000 Geburten eingehen müssen und

- experimentell belegt ist, daß identische Fehlbildungen durch verschiedene Ursachen ausgelöst werden können.

Weil die durch die verschiedenen Institutionen für Meldungen zu einem Fehlbildungsregister vorgesehenen Erhebungsbögen eine Reidentifikation nicht ausschließen, habe ich beim Ministerium für Arbeit, Soziales, Gesundheit und Frauen angefragt, ob sich die perinatologischen Zentren im Lande Brandenburg an diesem Vorhaben beteiligen. Nach dessen Kenntnissen ist dies augenblicklich nicht der Fall und auch nicht geplant.

6.4 Staatskirchenvertrag

Seit Anfang 1994 führt die Landesregierung Verhandlungen mit der Evangelischen Kirche von Berlin-Brandenburg über den Abschluß eines sog. Staatskirchenvertrages. Mit anderen Religionsgemeinschaften werden ebenfalls Verträge angestrebt.

Die Bereitschaft seitens der Landesregierung, mich an den Verhandlungen der drei dafür gebildeten Arbeitsgruppen (Finanzen, Schul- und Hochschulangelegenheiten, Rechtsfragen) zu beteiligen, wurde bisher unterschiedlich gesehen. Während das Ministerium der Finanzen sich von mir eine Stellungnahme zu steuerrechtlichen Fragen erbeten hat, wurde eine Beteiligung meiner Behörde von der bisher federführenden Staatskanzlei als "noch nicht für zwingend notwendig" erachtet und im übrigen darauf hingewiesen, daß bei einem nach Art. 91 Abs. 2 Brandenburgische Verfassung ratifizierungsbedürftigen Staatsvertrags eine Anhörung des Datenschutzbeauftragten nach § 7 Abs. 2 Bbg DSG nicht gegeben ist.

Daß ich diese Haltung der Landesregierung entschieden mißbillige, habe ich bereits Anfang März gegenüber dem Landtagsausschuß für Wissenschaft, Forschung und Kultur zum Ausdruck gebracht. Ich sehe darin eine Beschneidung meiner vom Gesetz unmittelbar abzuleitenden Aufgaben, bei der Schaffung von spezialgesetzlichen Datenschutzregeln mitzuwirken, zumal noch nicht abzusehen ist, ob es sich auch in diesem Fall beim Staatsvertrag zugleich um ein unmittelbar berechtigendes und verpflichtendes Gesetz handeln wird.

Im übrigen betrifft der abzuschließende Staatsvertrag datenschutzrechtlich nicht nur Fragen des Steuer- und Melderechts, die die Evangelische Kirche ganz offensichtlich nach ihrem Bedürfnis und nicht nach dem Prinzip der strikten Erforderlichkeit geregelt sehen möchte, sondern u. a. auch Fragen der Seelsorge, des Zeugnisverweigerungsrechtes von Pfarrern gegenüber der Polizei und der Sicherstellung des Datenschutzes im kirchlichen Bereich. Ich bin gespannt, ob mit dem Übergang der Zuständigkeit in das Ministerium für Wissenschaft, Forschung und Kultur (MWFK) und der von dort inzwischen zugesagten Einbeziehung sich die Angelegenheit zu einer konstruktiven Zusammenarbeit zwischen Landesregierung und meiner Behörde gestaltet.

6.5 Fragebögen zu den Feierlichkeiten anläßlich des 50. Jahrestages der Befreiung

Die Stiftung Brandenburgische Gedenkstätten bat mich, die den Einladungsschreiben an die ehemaligen Häftlinge der Konzentrationslager Ravensbrück und Sachsenhausen sowie des Zuchthauses Brandenburg beigefügten Fragebögen zu prüfen, welche Daten daraus für die Forschung und für die Archive der jeweiligen Einrichtung verwendet werden dürfen. Mit den Fragebögen wurden die zur Betreuung der Gäste notwendigen Angaben, wie z. B. Behinderungen und andere gesundheitliche Beeinträchtigungen, erhoben.

Rechtsgrundlage für die Erhebung der Daten war § 12 Bbg DSG. Danach ist die Erhebung personenbezogener Daten nur zulässig, wenn sie zur Aufgabenerfüllung und dem damit verbundenen Zweck erforderlich ist. Die Daten sind grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben, dabei ist er auch über den Verwendungszweck aufzuklären. Als Rechtsgrundlage für die Datenverarbeitung kam im vorliegenden Fall § 13 Abs. 2 Buchst. b i. V. m. § 4 Abs. 2 Bbg DSG in Betracht. Danach war die Verarbeitung personenbezogener Daten nur mit Einwilligung der Betroffenen zulässig. Mit der Beantwortung des Fragebogens sowie der Unterschrift hatten die Betroffenen der Nutzung ihrer Angaben allerdings nur insoweit zugestimmt, als diese für die Abwicklung ihres Besuches erforderlich sein würden. Da der Fragebogen keine Angaben über eine Nutzung der Daten zu wissenschaftlichen Zwecken enthielt, konnte der Betroffene dazu auch nicht schriftlich eingewilligt haben. Das

wäre jedoch erforderlich gewesen.

Die fehlende Einwilligung wird auch nicht durch den Rückgriff auf § 28 Bbg DSG als Rechtsgrundlage für die weitere Nutzung von Daten zu wissenschaftlichen Zwecken aufgefangen. Hiernach dürfen zwar öffentliche Stellen personenbezogene Daten auch ohne Einwilligung der Betroffenen für ein bestimmtes Forschungsvorhaben nutzen, wenn unter bestimmten Voraussetzungen schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse die schutzwürdigen Belange des Betroffenen erheblich überwiegt. Die Voraussetzungen für die 1. Alternative lagen hier jedoch nicht vor. Ob die Voraussetzungen für die 2. Alternative gegeben sind, war nicht nachprüfbar, da nähere Ausführungen über die wissenschaftlichen Zwecke fehlten. Mit Rücksicht auf den Personenkreis, der in seiner Vergangenheit nicht nur den Grausamkeiten des KZ-Alltags unterworfen, sondern darüber hinaus auch oft noch Opfer "wissenschaftlicher Forschung" gewesen war, habe ich im übrigen vorgeschlagen, von einer wissenschaftlichen Nutzung dieser Daten Abstand zu nehmen.

Unterdessen hat die Stiftung Brandenburgische Gedenkstätten mitgeteilt, daß den eingeladenen Zeitzeugen bei ihrer Begrüßung neben den Unterlagen über den Ablauf der Feierlichkeiten auch eine Erklärung überreicht werden soll, mittels derer sie ihr Einverständnis zu einer wissenschaftlichen Auswertung ihres Fragebogens erklären können. Gegen dieses Verfahren waren datenschutzrechtlich keine Bedenken zu erheben.

6.6 Umsetzung des Brandenburgischen Archivgesetzes

Eine Vielzahl von Eingaben und Anfragen zur Benutzung von öffentlichem Archivgut - insbesondere für die zeitgeschichtliche Forschung, zur Erstellung von Dorfchroniken u. ä. - hat deutlich gemacht, daß bei der Umsetzung des Brandenburgischen Archivgesetzes (BbgArchivG)[159] erhebliche Unsicherheiten bestehen, die zu einer insgesamt uneinheitlichen Praxis der Benutzungsbewilligung führen. Festzustellen ist, daß die Archive mit der Anwendung der gesetzlichen Bestimmungen noch nicht ausreichend vertraut sind und insbesondere eine konsequente Anspruchsprüfung nach Maßgabe des Gesetzes nicht erfolgt. Dabei ergab sich als vordringlicher Handlungsbedarf, daß Kriterien erarbeitet werden müssen, nach denen das Vorliegen der gesetzlichen Anspruchsvoraussetzungen für die Archivbenutzung von den Archiven zu prüfen ist. Dem MWFK sind dazu in § 17 Abs. 1 Nr. 1 und Abs. 2 BbgArchivG die erforderlichen Regelungsbefugnisse zur Verfügung gestellt. Unter eingehender Darlegung der aus datenschutzrechtlicher Sicht relevanten Fragestellungen und Kriterien habe ich ihm deshalb empfohlen, erläuternde Ausführungsvorschriften zu den für die Benutzung des öffentlichen Archivguts maßgeblichen Vorschriften des Brandenburgischen Archivgesetzes zu erlassen, und dazu meine Unterstützung angeboten. Nach anfänglichem Zögern hat das Ministerium meinen Vorschlag aufgegriffen und mir mitgeteilt, daß es gem. § 17 Abs. 2 BbgArchivG die Auslegung einzelner Bestimmungen des Gesetzes, insbesondere der §§ 9, 10 und 11 BbgArchivG in Ausführungsvorschriften regeln werde.

Hinweisen möchte ich an dieser Stelle auf folgendes Problem. Gem. § 11 Abs. 1 Nr. 2 BbgArchivG ist auch eine nach Maßgabe der §§ 8 bis 10 BbgArchivG an sich zulässige Benutzung des öffentlichen Archivguts dann einzuschränken oder zu versagen, wenn und soweit schutzwürdige Belange Dritter entgegenstehen. Das bedeutet, daß das Archiv prüfen muß, ob tatsächlich schutzwürdige Belange eines Dritten durch die Benutzung des Archivguts beeinträchtigt werden. Dies setzt wiederum voraus, daß vor einer Benutzungsbewilligung das jeweilige Archivgut im einzelnen daraufhin überprüft wird, ob es

159 vom 7. April 1994, GVBl. I S. 94

personenbezogene Angaben im Sinne von § 3 Abs. 1 Bbg DSG enthält, durch deren Offenbarung schutzwürdige Belange Dritter berührt sein könnten. Vielen Akten ist dies von außen nicht anzusehen; vielmehr hat die Erfahrung der Archive gelehrt, daß auch in den als "Sachakten" ausgewiesenen Archivbeständen immer wieder unvermutet Unterlagen mit z. T. ausgesprochen sensiblen personenbezogenen Angaben auftauchen können (z. B. IM-Berichte). Die gesetzliche Regelung verpflichtet deshalb das Archiv dazu, jede Akte vor einer Herausgabe an den Benutzer selbst durchzusehen.

7 Arbeit, Soziales, Gesundheit und Frauen

7.1 Soziales

7.1.1 2. SGB-Änderungsgesetz: Die wichtigsten Änderungen für die Praxis

Die längst überfällige Novellierung der Bestimmungen zum Sozialdatenschutz im Sozialgesetzbuch (SGB) I und X ist am 29.04.1994 mit der Zustimmung des Bundesrates zum Gesetz zur Änderung von Vorschriften des Sozialgesetzbuches über den Schutz der Sozialdaten sowie zur Änderung anderer Vorschriften (2. Gesetz zur Änderung des Sozialgesetzbuches - 2. SGBÄndG)[160] abgeschlossen worden. Überfällig war die Änderung deshalb, weil die §§ 79 ff. SGB X a. F. die Verbindung des bereichsspezifischen Datenschutzes zum bereits am 1. Juni 1991 novellierten Bundesdatenschutzgesetz (BDSG) herstellten. Im neuen Text sind - im Gegensatz zu der bisherigen Textfassung des SGB - nur mit wenigen Ausnahmen Verweisungen auf das BDSG zu finden. Damit ist das Gesetz für den Bürger transparenter geworden. Gleichzeitig war es ein Ziel, die bisherigen Paragraphenziffern im SGB X beizubehalten, um die Orientierung für den Benutzer zu erleichtern. Aus diesem Grunde sind die aus dem BDSG übernommenen neuen Begriffsbestimmungen in den §§ 67 bis 67 d SGB X zu finden.

Über die mit dieser Novellierung verbundenen Änderungen, insbesondere für die Sozialleistungsträger, soll im folgenden ein Überblick gegeben werden.

7.1.1.1 Sozialgeheimnis beim Leistungsträger (§ 35 SGB I)

Neu eingeführt wurde der Begriff der Sozialdaten. Nach § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die im Hinblick auf die Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden. Diesen Sozialdaten stehen nach § 35 SGB I die Betriebs- und Geschäftsgeheimnisse gleich, wobei darunter alle betriebs- oder geschäftsbezogenen Daten - auch von juristischen Personen - , die Geheimnischarakter haben, zu verstehen sind.

Bisher hatte jeder nach § 35 SGB I a. F. einen Anspruch darauf, daß Einzelangaben über seine persönlichen und sachlichen Verhältnisse von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Das Sozialgeheimnis nach § 35 SGB I n. F. schützt die Erhebung, die Verarbeitung und die Nutzung von Sozialdaten.

§ 35 SGB I n. F. stellt nun begrüßenswerterweise klar, daß das Sozialgeheimnis auch innerhalb des Leistungsträgers gewahrt werden muß, d. h., die Sozialdaten dürfen nur Befugten zugänglich gemacht oder nur an diese weitergegeben werden. Nach Beendigung der Tätigkeit haben die Beschäftigten der Sozialversicherungsträger das Sozialgeheimnis weiter zu wahren. Sozialdaten der Beschäftigten und ihrer Angehörigen sind besonders geschützt.

---

160 vom 13. Juni 1994, BGBl. I S. 1229

Auf diese Daten dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, nicht zugreifen. Außerdem dürfen Zugriffsberechtigte diese Daten nicht an diese Personengruppe weitergeben. In der Begründung wird ausgeführt, daß an Personalentscheidungen im Sinne der neuen Vorschriften Personen mitwirken, die am Entscheidungsprozeß selbst beteiligt sind, nicht aber an seiner Vorbereitung. Die Daten von Angehörigen brauchen nicht besonders ermittelt oder erfaßt werden, wenn dem Leistungsträger unbekannt ist, daß es sich um Angehörige handelt.

Der aus § 3 BDSG übernommene Begriff der Übermittlung hat darüber hinaus eine zusätzliche Bedeutung erlangt. Darunter ist jetzt auch das Bekanntgeben nicht gespeicherter Sozialdaten zu verstehen. Damit werden auch Daten geschützt, die ausschließlich im Gedächtnis festgehalten sind.

Der Begriff des Nutzens ist identisch mit dem im BDSG verwendeten Begriff. Darüber hinaus ist auch die Weitergabe innerhalb der speichernden Stelle eine Nutzung, wenn es sich bei der Weitergabe nicht um eine Verarbeitung handelt.

Die speichernde Stelle ist der Leistungsträger i. S. v. § 12 SGB I. Ist der Leistungsträger eine Gebietskörperschaft, so bilden die Organisationseinheiten eine speichernde Stelle, die eine Aufgabe nach einem besonderen Teil des Sozialgesetzbuches funktional durchführen. Durch diese Regelung wird klargestellt, daß die an einer Entscheidung notwendigerweise beteiligten Stellen innerhalb der Behördenhierarchie (z. B. Dezernent einer Gemeinde) ein Teil der speichernden Stelle sind. Außerdem wird geregelt, daß die Organisationseinheiten einer Gemeinde (wie z. B. das Rechenzentrum oder die Stadtkasse), die unterstützende Funktionen für die Erfüllung der Aufgaben der anderen Organisationseinheiten (wie z. B. Wohngeldamt, Sozialamt) ausführen, insoweit Teile der speichernden Stelle sind.

7.1.1.2 Erhebung von Sozialdaten (§ 67 a SGB X)

Die Vorschriften zur Datenerhebung waren bis zuletzt sehr umstritten. Seitens des Bundesrats stand zur Diskussion, bei Mißbrauchsverdacht die Angaben des Betroffenen an diesem vorbei zu überprüfen, wenn die Überprüfung bei ihm selbst einen unverhältnismäßigen Aufwand erfordern würde. Damit wäre aber der Erhebungsgrundsatz weitgehend ausgehöhlt worden. Letztlich sind die vom Bundesbeauftragten für den Datenschutz vorgetragenen Vorstellungen - insbesondere zu den Verfahren bei sog. Mißbrauchsfällen - im Vermittlungsausschuß des Bundestags und des Bundesrats aufgegriffen worden.

Nach § 67 a SGB X sind Sozialdaten jetzt grundsätzlich beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie innerhalb des Sozialdatenpools - das sind die im § 35 SGB I und § 69 Abs. 2 SGB X genannten Stellen - nur erhoben werden, wenn

- die speichernde Stelle zur Übermittlung der Daten an die erhebende Stelle befugt ist,
- die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und
- keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

In § 67 d Abs. 2 SGB X ist einer vielfach geäußerten Forderung der Sozialleistungsträger Rechnung getragen worden. Nach dieser Vorschrift trägt die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle. Erfolgt die Übermittlung allerdings auf Ersuchen des Empfängers, trägt dieser die Verantwortung für die Richtigkeit der Angaben in seinem Ersuchen, weil die übermittelnde Stelle diese Angaben nicht prüfen kann. Darüber hinaus muß der ersuchende Träger den "unverhältnismäßigen Aufwand" einer "Erhebung beim Betroffenen" für die ersuchte Stelle nachvollziehbar darlegen.

7.1.1.3 Sozialdaten an Strafverfolgungsbehörden (§§ 68 und 73 SGB X)

Die allgemeine Amtshilfe war in § 68 SGB X a. F. geregelt. Der Paragraph kam bisher durch die frühere Einschränkung zu in Dateien enthaltenen Daten, die sich aus § 10 Abs. 1 Satz 2 BDSG a. F. ergab, nur in wenigen Fällen zur Anwendung. Diese Einschränkung ist nunmehr ersatzlos gestrichen. Statt dessen sind die Behörden ausdrücklich genannt, die die allgemeine Amtshilfe aus dem "Sozialdatenpool" in Anspruch nehmen dürfen. Das sind die Polizeibehörden, die Staatsanwaltschaften und Gerichte, die Behörden der Gefahrenabwehr und die Justizvollzugsanstalten. Außerdem ist die Übermittlung von Daten zur Durchsetzung öffentlich-rechtlicher Ansprüche in Höhe von mindestens 1.000 DM zulässig. Über ein Auskunftsersuchen gem. § 68 SGB X n. F. entscheidet weiterhin der Leiter der ersuchenden Stelle, sein allgemeiner Stellvertreter oder ein besonders bevollmächtigter Bediensteter.

Umstritten war die Frage, ob der Aufenthaltsort mit der derzeitigen Anschrift gleichzusetzen ist. Der Bundesrat schlug deshalb zur Klarstellung in § 68 SGB X und im Rahmen der Übermittlung für den Schutz der inneren und äußeren Sicherheit gem. § 72 SGB X vor, neben der "derzeitigen Anschrift" auch noch die Worte "oder tatsächlicher Aufenthaltsort" einzufügen. Danach hätten die Sozialämter verpflichtet werden können, der Polizei und anderen Sicherheitsbehörden nicht nur wie bisher, z. B. in Fällen des Sozialleistungsbetruges, sondern auf deren Ersuchen auch im Zusammenhang mit anderen Delikten etwa mitzuteilen, daß sich eine von diesen gesuchte Person im Sozialamt aufhält. Der Vorschlag des Bundesrates, die "derzeitige Adresse" mit dem "tatsächlichen Aufenthaltsort" gleichzusetzen, hat sich nicht durchgesetzt; somit ist § 68 SGB X als Ausnahmevorschrift eng auszulegen. Damit ist den Intentionen der Datenschutzbeauftragten Rechnung getragen worden.

Bei den Vorberatungen in den Ausschüssen des Bundesrates war vergeblich angeregt worden, § 73 SGB X zu streichen. Vielmehr ist der Anwendungsbereich von § 73 SGB X erweitert worden, so daß jetzt keine Unterscheidung mehr zwischen Verbrechen und Vergehen vorgenommen wird. Die Übermittlung von Sozialdaten an Strafverfolgungsbehörden ist

zulässig, soweit sie zur Durchführung eines Ermittlungsverfahrens wegen eines Verbrechens oder wegen einer Straftat von erheblicher Bedeutung erforderlich ist. Bei der Formulierung "Straftaten von erheblicher Bedeutung" hatte der Ausschuß für Arbeit und Sozialordnung des Bundestags erklärt, daß eine sachliche Differenzierung der Erheblichkeit von Straftaten nicht allein über die Straftatbestände erfolgen kann. Vielmehr müssen auch andere Kriterien (wie z. B. die Schadenshöhe) berücksichtigt werden. Die Übermittlung von Sozialdaten wegen einer anderen Straftat ist zulässig, soweit die Übermittlung auf Namen und Vornamen sowie früher geführte Namen, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen sowie Namen und Anschriften seiner derzeitigen und früheren Arbeitgeber und die Angaben über die erbrachten oder demnächst zu erbringenden Geldleistungen beschränkt wird. Jede Übermittlung nach § 73 SGB X bedarf einer richterlichen Anordnung. Dies könnte bei Kindesmißhandlungen etc. relevant sein, da aufgrund dieser Bestimmung die Vorlage der gesamten Akte des Beschuldigten verlangt werden kann.

Aus der Sicht der Jugendhilfe kann dadurch ein schützenswertes Vertrauensverhältnis zu potentiellen Zeugen durch die richterlich erzwingbare Übermittlungspflicht gestört werden und die Arbeit der Jugendämter mit Familien, in denen eine Kindesmißhandlung oder ein sexueller Mißbrauch vorgekommen ist, schwer belasten. Aus datenschutzrechtlichen Gründen teile ich diese Auffassung, da durch diese Übermittlungspflicht die Gefahr besteht, daß bestimmte Aufgaben der Jugendämter nicht mehr erfüllt werden können.

7.1.1.4 Erfüllung sozialer Aufgaben (§ 69 SGB X)

Die Krankenkassen sind nun gem. § 69 Abs. 4 SGB X befugt, einem Arbeitgeber mitzuteilen, ob die Fortdauer einer Arbeitsunfähigkeit oder eine erneute Arbeitsunfähigkeit eines Arbeitnehmers auf derselben Krankheit beruht. Die Übermittlung von Diagnosedaten an den Arbeitgeber ist allerdings nicht zulässig.

7.1.1.5 Unterhaltspflichten und Versorgungsausgleich (§ 74 SGB X)

Eine Übermittlung von Sozialdaten bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich war bisher nur zulässig, nachdem der Auskunftspflichtige gemahnt wurde und innerhalb einer angemessenen Frist seiner Auskunftspflicht nicht nachgekommen war. Da häufig die Anschrift des Auskunftspflichtigen nicht bekannt war, konnte auch keine Mahnung erfolgen. Aus diesem Grunde dürfen gem. § 74 SGB X den Auskunftsberechtigten jetzt die Anschriften zum Zwecke der Mahnung übermittelt werden.

7.1.1.6 Zweckbindung (§ 78 SGB X)

Nach bisherigem Recht durften Sozialdaten nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie befugt übermittelt worden sind. Unbefugt übermittelte Daten unterlagen einem absoluten Verwertungsverbot. Jetzt dürfen Polizeibehörden, Staatsanwaltschaften, Gerichte und Behörden der Gefahrenabwehr Sozialdaten, die ihnen übermittelt worden sind, unabhängig vom Zweck der Übermittlung sowohl für Zwecke der Gefahrenabwehr als auch der Strafverfolgung und -vollstreckung nach § 78 Abs. 1 Satz 2 verarbeiten und nutzen.

Das vom Bundesverfassungsgericht im Volkszählungsurteil[161] ausdrücklich geforderte Zweckbindungsgebot, das auch ein Verwertungsverbot mit einschließt, wird damit unterlaufen. Informationen, die der Bürger dem Jugendamt anvertraut hat, können frei weiterverwendet werden, wenn sie von einem/einer Jugendamtsmitarbeiter/-in in strafbarer Weise gem. § 85 SGB X i. V. m. § 203 StGB weitergegeben worden sind. Insbesondere unter diesem Gesichtspunkt haben die Datenschutzbeauftragten ihre Bedenken geäußert, die auch

161 BVerfGE 65, 1

die Arbeitsgemeinschaft Jugendhilfe teilt.

7.1.1.7 Rechte der Datenschutzbeauftragten (§ 81 SGB X)

Infolge der Verweisung auf das BDSG war in der früheren Fassung des § 79 Abs. 3 SGB X unklar, welche Rechte den Datenschutzbeauftragten im Rahmen ihrer Kontrollen zustehen sollten. Eine verfassungskonforme Auslegung dieser alten Vorschrift führte zu der Maßgeblichkeit landesrechtlicher Bestimmungen. Nach § 81 Abs. 2 Satz 3 SGB X n. F. richten sich nunmehr die Aufgaben und Befugnisse der Datenschutzbeauftragten nach dem jeweiligen Landesrecht, womit eine Verbesserung der Kontrollbefugnisse der Landesdatenschutzbeauftragten einhergeht.

Nach § 81 Abs. 4 SGB X haben die Sozialversicherungsträger und ihre Verbände die §§ 36 und 37 Abs. 1 des BDSG entsprechend anzuwenden. Das bedeutet, daß sie einen Datenschutzbeauftragten zu bestellen haben. Darüber hinaus ist bei den räumlich getrennten Organisationseinheiten sicherzustellen, daß der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben unterstützt wird. Immerhin bleibt der behördliche Datenschutzbeauftragte - wenn auch mit eingeschränkten Kompetenzen - erhalten. Der ursprüngliche Entwurf sah seine vollständige Abschaffung vor.

7.1.2 Datenschutz bei gesetzlichen Sozialversicherungsträgern

7.1.2.1 Zugriffssperren bei Versicherungsdaten innerhalb der AOK

Für die 126 landesweit existierenden AOK-Geschäftsstellen wurde im Berichtszeitraum ein neues Rechenzentrum in Teltow eingeweiht. Es wird von der AOK Brandenburg als ein Musterbeispiel für eine zukunftsweisende, rationelle Problemlösung angesehen. Nunmehr kann jede Geschäftsstelle on-line auf die gespeicherten Beitrags- und Leistungsdaten von Versicherten zugreifen. Mit dieser Form der automatischen Datenverarbeitung will die AOK - wie andere Krankenkassen - der Erwartungshaltung ihrer Kunden nach "grenzenlosem Service" entsprechen. Die datenschutzrechtlich bedenkliche Konsequenz des Online-Zugriffs ist, daß eine Vielzahl von Mitarbeitern landesweit auf die Daten aller Versicherten zugreifen kann. Dies widerspricht dem Erforderlichkeitsprinzip.

Gegen meine Forderung, zumindest den Zugang zu den Versichertendaten dahingehend einzuschränken, daß die Versicherten selbst entscheiden können, ob sie diesen "grenzenlosen Service" in Anspruch nehmen wollen, wandte die AOK u. a. folgendes ein: Grundsätzlich werde der Versicherte von der AOK an seinem Wohnort betreut. Da aber häufig der Wohn- und Beschäftigungsort des Versicherten nicht identisch seien, wäre die Betreuung von nur einer Geschäftsstelle nicht sinnvoll. Bei einer Beschäftigungssituation mit ständigem Ortswechsel und hohem Ehegattenbeschäftigungsgrad müsse auch eine auftragsweise Erledigung durch Familienangehörige berücksichtigt werden. Wichtig sei auch die Betreuung der Arbeitgeber der Versicherten durch die AOK-Geschäftsstellen in deren jeweiligem Betriebsstandort. Eine ausdrücklich von den Arbeitgebern gewollte Betreuung aus einer Hand sei durch die AOK anders nicht praktizierbar.

Das in § 17 SGB I[162] enthaltene Gebot, daß die Versicherten ihre Leistungen einfach und schnell erhalten sollen, wird aber durch das Wahlrecht der Versicherten nicht eingeschränkt. Zur Durchsetzung des Selbstbestimmungsrechts des Betroffenen, den Zugriff stets entweder

---

162 vom 11. Dezember 1975, BGBl. I S. 3015, zul. geänd. durch 2. SGB-Änderungsgesetz vom 13. Juni 1994, BGBl. I S. 1229 und Agrarsozialreformgesetz 1995 vom 29. Juli 1994, BGBl. I S. 1890

nur durch eine, mehrere ausdrücklich vereinbarte oder alle Geschäftsstellen der Krankenkassen zu gestatten, müssen lediglich die dafür erforderlichen technischen Voraussetzungen i. V. m. § 78 a SGB X geschaffen werden. Ohne ein schriftliches Einverständnis des Versicherten sollte ausschließlich der Zugriff auf einen "Stammdatensatz" (Name, Geburtsdatum, Anschrift, Krankenversichertennummer sowie betreuende Geschäftsstelle des Versicherten) zulässig sein.
Die AOK Brandenburg ist nicht bereit, die Zugriffsrechte künftig auf Antrag des Versicherten - wie dies aus anderen Bundesländern bekannt ist - auf einzelne Geschäftsstellen zu beschränken. Sie will vielmehr mit der Begründung, daß dies ein Problem der gesamten AOK-Gemeinschaft sei, eine Klärung auf der Ebene des AOK-Bundesverbandes mit dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für Gesundheit abwarten. Mit Hinweis auf den Beschluß der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 (s. Anlage 15) erwarte ich die Unterstützung des Ministeriums für Arbeit, Soziales, Gesundheit und Frauen (MAGSF) entsprechend meiner datenschutzrechtlichen Bewertung.

7.1.2.2 Durchsuchungsanordnung bei der AOK

Aufgrund eines Artikels des Nachrichtenmagazins "FOCUS" über rückständige Sozialversicherungsbeiträge einer Brandenburger Firma in Millionenhöhe erwirkte die Staatsanwaltschaft Potsdam einen Durchsuchungsbeschluß bei der AOK Brandenburg u. a. wegen des Verdachts des Vorenthaltens und Veruntreuens von Arbeitsentgelt gem. § 266 a Strafgesetzbuch (StGB)[163]. Er war lediglich auf strafprozessuale Beschlagnahme- und Durchsuchungsvorschriften (§§ 33 Abs. 4, 94, 98, 103, 105, 162 Strafprozeßordnung (StPO))[164] gestützt und erstreckte sich u. a. auch auf die Beschlagnahme von Unterlagen über Beitragsrückstände. Dagegen machte die AOK erhebliche datenschutzrechtliche Bedenken geltend und bat mich um Unterstützung.

Die Durchsuchungsanordnung, mit der eine Übermittlung von Sozialdaten (hier: Arbeitgeberdaten sowie aller säumigen Beitragsschuldner) verbunden war, widersprach sowohl nach meiner Auffassung als auch der des MAGSF der Rechtslage. Eine Übermittlung von Sozialdaten kann sich nicht auf die Strafprozeßordnung stützen; sie bedarf vielmehr einer Übermittlungsbefugnis nach dem SGB X. Zur Durchführung eines Strafverfahrens wegen eines Vergehens ist zwar eine Übermittlung von Sozialdaten gem. § 73 Abs. 2 SGB X zulässig, jedoch muß eine richterliche Anordnung vorliegen. Diese lag hier gerade nicht vor. Auch schied § 69 Abs. 1 Nr. 2 SGB X als Rechtsgrundlage aus, wonach eine Übermittlung zulässig ist, soweit sie erforderlich ist für die Durchführung eines mit der Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens einschl. eines Strafverfahrens. Da sich das staatsanwaltschaftliche Ermittlungsverfahren im Stadium des Vorverfahrens befand, war die Voraussetzung "gerichtliches Verfahren" nicht erfüllt. Darüber hinaus war auch die Erforderlichkeit zu verneinen, die im Zusammenhang mit den gesetzlichen Aufgaben einer nach § 35 SGB I genannten Stelle zu beurteilen ist. Nach unserem damaligen Sachstand war nicht ersichtlich, inwiefern diese Voraussetzungen erfüllt waren; außerdem war diese von der Krankenkasse nicht bejaht worden. Demzufolge ist festzustellen, daß die AOK im vorliegenden Fall nicht verpflichtet war, Auskunft zu erteilen, Zeugnis abzulegen oder Schriftstücke, Akten, Dateien und sonstige Datenträger vorzulegen oder auszuliefern, da die Voraussetzungen für eine Offenbarung nach § 35 Abs. 3 SGB I nicht erfüllt waren (sog.

---

163 i. d. Fassung vom 10. März 1987, BGBl. I S. 945, ber. S. 1160

164 i. d. Fassung vom 7. April 1987, BGBl. I S. 1074, ber. Pkt. S. 1319

Zeugnisverweigerungsrecht und Beschlagnahmeverbot zugunsten der Sozialbehörde).

Die AOK legte beim Amtsgericht Beschwerde gegen den Durchsuchungsbeschluß ein. Da jedoch dieses Rechtsmittel keine aufschiebende Wirkung hat, mußte eine Aufstellung über fällige Forderungen an Sozialversicherungsabgaben der Staatsanwaltschaft zur Verfügung gestellt werden. Die AOK übergab der Staatsanwaltschaft einen Computerausdruck, der die rückständigen Forderungen der in ihrem Geschäftsbereich ansässigen Arbeitgeber enthielt. Eine Durchsuchung oder gar Beschlagnahme von Akten mit geschützten Arbeitnehmerdaten hatte sich somit erübrigt. Auf die Beschwerde der AOK hob das Amtsgericht den fehlerhaften Durchsuchungsbeschluß auf, erließ jedoch einen neuen Beschluß, der die AOK nunmehr auf der Grundlage des § 73 SGB X zur Offenbarung der säumigen Schuldner verpflichtete. Daraufhin einigte sich die AOK mit der Staatsanwaltschaft dahingehend, daß die eingezogenen Unterlagen wieder zurückgegeben werden und die AOK nach dem Grundsatz der Erforderlichkeit ohne Einbeziehung des neuen Beschlusses auf der Grundlage von § 69 Abs. 1 Nr. 2 SGB X der Staatsanwaltschaft entsprechend aufbereitete Unterlagen übermitteln wird.

7.1.2.3 Auskunftserteilung zum Strafverfahren gegen Unbekannt

Folgender Sachverhalt veranlaßte die AOK Brandenburg, an mich mit der Bitte um datenschutzrechtliche Prüfung heranzutreten: Im Zusammenhang mit einem Ermittlungsverfahren wurde der Sachbearbeiterin einer AOK-Geschäftsstelle von der Polizei ein Bild mit der Bitte um Identifizierung einer Person vorgelegt, weil diese eine Verbindung zwischen einem Computerbetrug und einem Versicherten vermutete. Da die Sachbearbeiterin aus datenschutzrechtlichen Gründen die Personalien des Versicherten der Polizei nicht mitteilte, bat diese zumindest um Übersendung der "kleinen Personalien" (Name, Anschrift) der auf dem Bild wiedererkannten Person und kündigte eine zeugenschaftliche Vernehmung der betreffenden Sachbearbeiterin an.

Das polizeiliche Ermittlungsersuchen ließ sich nicht auf § 68 Abs. 1 SGB X stützen. Danach ist zur Erfüllung von Aufgaben der Polizeibehörden eine Übermittlung personenbezogener Daten zulässig, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Wenn die ersuchte Stelle aufgrund vorhandener Erkenntnisse eine Beeinträchtigung der Belange nicht ausschließen kann, genügt dies, um die Offenbarung unzulässig zu machen. Da das Interesse des Betroffenen, sich einem Ermittlungsverfahren bzw. dem Zugriff der Strafverfolgungsbehörden zu entziehen, als solches nicht schutzwürdig ist und der AOK in diesem Fall keine effektiven Anhaltspunkte bzw. Informationen für die Annahme einer Beeinträchtigung des Betroffenen vorlagen, wären für eine Übermittlung nach der o. g. Vorschrift zwar die materiellen Voraussetzungen gegeben gewesen. Besteht jedoch für die ersuchende Stelle die Möglichkeit, die Angaben auf andere Weise zu beschaffen, so muß sie sich zunächst dieser anderweitigen Beschaffungsmöglichkeiten bedienen, auch wenn dies mit zusätzlichem Aufwand an Zeit und Kosten verbunden ist. Das Melderegister enthält die erforderlichen Personalien des Betroffenen und verfügt über eine Bildkartei, so daß sich das Polizeipräsidium zunächst an die Meldebehörde wenden muß. Erst wenn dieses Auskunftsersuchen sowie anderweitige Beschaffungsversuche ergebnislos geblieben wären, hätten alle erforderlichen Voraussetzungen für eine Auskunft durch die AOK vorgelegen.

Für den Fall einer richterlichen Anordnung vor der Übermittlung an das Polizeipräsidium wäre § 73 Abs. 2 i. V. m. § 72 Abs. 1 Satz 2 SGB X einschlägig gewesen. Hiernach ist eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen eines Vergehens zulässig, wobei die Übermittlung auf Angaben über Name und Vorname sowie früher geführte Namen, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen sowie Namen und Anschrift seiner derzeitigen und früheren Arbeitgeber beschränkt ist. Da hier der Richter nicht eingeschaltet war, lag auch insoweit keine Offenbarungsbefugnis vor. Soweit aber eine Offenbarung unzulässig ist, besteht nach § 35 Abs. 1 SGB I u. a. auch keine Zeugnispflicht.

Diese datenschutzrechtliche Bewertung habe ich der AOK mitgeteilt.

7.1.2.4 Auskunftsersuchen der Berufsgenossenschaften zur Aufstellung des Lohnnachweises

Zwischen dem Hauptverband der gewerblichen Berufsgenossenschaften und der AOK für das Land Brandenburg ist ein Streit darüber entstanden, ob die AOK im Rahmen der Amtshilfe gegenüber den gewerblichen Berufsgenossenschaften weiterhin zur Mitteilung der Lohnsumme zur Erstellung des Lohnnachweises verpflichtet ist. Bis Ende 1993 hat sie diese Auskunftsersuchen erfüllt, weil die Berufsgenossenschaften erst ihren Prüfdienst aufbauen mußten. Die AOK ist aber nunmehr der Auffassung, daß sie Auskünfte zum Beitragssoll der Berufsgenossenschaften ohne eingehende Darlegung der erfolglosen Ermittlungsbemühungen im Rahmen der Lohnbuchprüfung gem. § 744 Reichsversicherungsordnung (RVO) nicht mehr erteilen könne. Nach § 744 Abs. 1 RVO besteht für die Berufsgenossenschaften ein Einsichtsrecht in die Geschäftsbücher und sonstigen Unterlagen zur Prüfung der eingereichten Lohnnachweise oder um diese selbst aufzustellen. Demgegenüber hält der Hauptverband der gewerblichen Berufsgenossenschaften solche Auskünfte durch die Krankenkassen insbesondere dann für zulässig, wenn der Unternehmer den für die Umlage und Beitragsrechnung notwendigen Lohnnachweis selbst nicht einreicht und wegen der erheblichen Zahl nicht erfolgter Meldungen die Berufsgenossenschaften mit einem unverhältnismäßig großen Aufwand die Prüfung der Lohnnachweise und die Einsichtnahme in Geschäftsbücher der Unternehmer vornehmen müßte.

Die Berufsgenossenschaften sind der Auffassung, daß sie bei Kleinbetrieben ihrer Darlegungspflicht nachgekommen sind, wenn sie der AOK mitteilen, daß sie sich vergeblich bemüht haben, die notwendigen Angaben von Unternehmen selbst zu erhalten und das Unternehmen darauf hingewiesen haben, daß die Angaben im Falle der Verweigerung von der AOK erbeten werden.

Wie die AOK halte ich die Auskunftspraxis der Berufsgenossenschaft im Rahmen des § 69 Abs. 1 Nr. 1 SGB X mangels Erforderlichkeit für nicht zulässig. Das Vorliegen der Erforderlichkeit hängt von den jeweiligen Umständen des Einzelfalles ab und muß jeweils konkret nachgewiesen werden. Eine Datenübermittlung ist nur dann erforderlich, wenn die anfragende Stelle ohne die Datenverarbeitung eine Aufgabe nicht oder nicht sachgerecht (etwa nicht vollständig oder zeitgerecht) erfüllen kann. Um den Risiken genereller Pauschalanfragen durch die Berufsgenossenschaften zu begegnen, ist im Rahmen der Erforderlichkeit eine konkrete Darlegung der unternommenen Versuche, selbst an die verlangten Daten zu gelangen, zu fordern. Zur praktischen Handhabung dieser Darlegungspflicht der Berufsgenossenschaften habe ich empfohlen, genau festzulegen, welche Anforderungen die AOK an die Erforderlichkeit der jeweiligen Auskunftsersuchen stellt. So könnte jedem Ersuchen der Schriftwechsel oder zumindest das letzte an den Versicherten gesandte Mahnschreiben beigefügt werden.

7.1.2.5 Fragebogen des Gemeindeunfallversicherungsverbandes Brandenburg

Von einer Petentin wurde mir ein Antragsformular auf ergänzende Leistungen gem. § 569 a Nr. 5 Reichsversicherungsordnung (RVO) wegen der Betreuung/Beaufsichtigung ihres unfallverletzten Kindes übersandt. Es enthielt eine Fülle von Daten, die mit der Gewährung der Erstattung ihres Verdienstausfalls nicht im Zusammenhang standen.

Unter anderem sollten alle im Haushalt lebenden Kinder unter 12 Jahren bzw. behinderte und auf Hilfe angewiesene Kinder aufgeführt werden. Da es sich lediglich um die Genehmigung ergänzender Leistungen wegen Betreuung bzw. Beaufsichtigung des unfallverletzten Kindes handelte, erschien mir die Aufzählung weiterer im Haushalt lebender Kinder für die Feststellung der Geldleistungen unerheblich. Ebenso überflüssig war die Frage nach der Versorgung weiterer Kinder außerhalb des Haushalts. Schließlich war die Notwendigkeit,

nach dem Verwandtschaftsverhältnis der im Haushalt lebenden Personen für die Anspruchsberechtigung zu differenzieren, nicht ersichtlich.

Auf meine Anfrage teilte mir der Gemeindeunfallversicherungsverband mit, daß es sich um einen aus den alten Bundesländern weitestgehend übernommenen Fragebogen handele, den er offensichtlich nicht ausreichend geprüft hätte. Die von mir monierten Fragen seien für die Beurteilung eines Anspruchs auf ergänzende Leistungen tatsächlich unerheblich. Lediglich die Fragen hinsichtlich des Verwandtschaftsverhältnisses seien zwar grundsätzlich gerechtfertigt, weil die Kosten nur dann übernommen werden können, wenn nicht eine andere im Haushalt der Familie lebende oder ihr sonst nahestehende Person zur Verfügung steht. Jedoch könne auf eine Differenzierung verzichtet werden. Der Gemeindeunfallversicherungsverband hat mir zugesichert, diesen Fragebogen vollständig zurückzuziehen.

7.1.2.6 Pflegeversicherung: Pflegebedürftigkeits-Richtlinien (PflRi)

Durch die Spitzenverbände der Pflegekassen wurden aufgrund von § 17 SGB XI[165] i. V. m. § 213 SGB V[166] Richtlinien zur Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit (PflRi) beschlossen. Diese Richtlinien sind für die Pflegekassen sowie für den Medizinischen Dienst der Krankenkassen (MDK) verbindlich.

Als Anlage zur o. g. Richtlinie wird für den MDK ein bundesweit einheitlicher, fünfseitiger Gutachtenvordruck mit der Überschrift "Gutachten zur Feststellung der Pflegebedürftigkeit gem. SGB XI" vorgegeben. Der Vordruck enthält auf den ersten drei Seiten das eigentliche Gutachten. Ab der vierten Seite (Nr. 5) sollen die hieraus resultierenden Ergebnisse und Empfehlungen dokumentiert werden.

Ziff. 5.8 Satz 1 PflRi bestimmt, daß der MDK das Ergebnis seiner Prüfung der Pflegekasse in einem Gutachten mitteilt, für das das als Anlage beigefügte Formular zu verwenden ist. Die Datenschutzbeauftragten sind einstimmig der Auffassung, daß sich Inhalt und Umfang des Gutachtenformulars für den MDK nicht mehr im Rahmen einer "Ergebnismitteilung" an die Pflegekasse und damit an die Vorgaben des § 18 Abs. 5 SGB XI hält. Nach § 18 Abs. 5 SGB XI hat der MDK der Pflegekasse lediglich das Ergebnis seiner Prüfung mitzuteilen und Maßnahmen zur Rehabilitation, Art und Umfang von Pflegeleistungen sowie einen individuellen Pflegeplan zu empfehlen. Der Bundesbeauftragte für den Datenschutz hat die Spitzenverbände der Pflegekassen sowie nachrichtlich das Bundesministerium für Arbeit und Sozialordnung aufgefordert, Ziff. 5.8 der PflRi zu korrigieren. Dazu ist das Ministerium mit Hinweis auf die Begründung zu § 18 Abs. 5 SGB XI jedoch nicht bereit.

Die von der Pflegebedürftigkeits-Richtlinie behauptete Mitwirkungspflicht der Antragsteller geht über die tatsächlichen in §§ 60 ff. SGB I gesetzlich geregelten Mitwirkungspflichten von Antragstellern auf Sozialleistungen hinaus (§ 18 Abs. 3 SGB XI, Ziff. 5.3 und 5.4 PflRi). Die Mitwirkungspflicht umfaßt keinesfalls die Einwilligung, alle Auskünfte bei sämtlichen behandelnden Ärzten bzw. betreuenden Pflegepersonen einzuholen. In der Praxis ist es in den vergangenen Jahren immer wieder vorgekommen, daß in Einwilligungsformularen pauschal auf die Mitwirkungspflicht der Betroffenen hingewiesen wird und sich diese aus Angst vor finanziellen Risiken bereiterklären, wesentlich mehr personenbezogene Daten zur Verfügung zu stellen, als tatsächlich im Rahmen ihrer Mitwirkungspflicht erforderlich wären. Die Einwilligungsformulare müssen darüber hinaus die Betroffenen über den konkreten Umfang ihrer Mitwirkungspflicht angemessen informieren.

165

166 vom 1. Januar 1995, BGBl. 1994 I S. 1014
vom 20. Dezember 1988, BGBl. I S. 2477

7.1.2.7 Irreführende Werbung mit Akteneinsichtsrecht

Eine Bürgerin beschwerte sich bei mir darüber, daß ihr die AOK Einsicht über ihre dort gespeicherten Krankenhausdaten verweigere. Dies stand für sie im Widerspruch zu einer Werbeaktion in dem Schaukasten der AOK-Geschäftsstelle, dem zu entnehmen war, daß jeder seine Daten bei der Krankenkasse einsehen könne. Bei der Probe aufs Exempel sei ihr jedoch lediglich ein leeres Formular gezeigt worden.

Der behördliche Datenschutzbeauftragte bestätigte in seiner Stellungnahme: Versicherte haben Anspruch auf Auskunft über die zu ihrer Person bei der AOK Brandenburg gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und ferner über den Zweck der Speicherung. Der Auskunftsanspruch erfaßt auch alle medizinischen Daten, wobei jedoch bei Angaben über gravierende gesundheitliche Verhältnisse (z. B. Diagnosen über bösartige Krebserkrankungen, psychische Krankheiten etc.) der betreffende behandelnde Arzt zur Auskunft an den Versicherten eingeschaltet werden kann (§ 35 SGB I i. V. m. § 83 SGB X und § 9 BDSG und § 25 Abs. 2 SGB X).

Die AOK ist schließlich meiner Bitte nachgekommen, der Versicherten die gewünschten Auskünfte zu geben. Dem Recht auf Einsichtnahme in ihre Krankenhausdaten wurde in Form einer Übersicht entsprochen.

7.1.3 Kontrollbesuch bei Jugendämtern

Im Berichtszeitraum habe ich in drei Jugendämtern die Umsetzung der datenschutzrechtlichen Vorschriften gem. §§ 61 - 68 SGB VIII[167] aufgrund von Eingaben aus diesem Bereich überprüft. Erfreulicherweise konnte ich feststellen, daß die dort als vorrangig zu betrachtende Wahrung des Sozialgeheimnisses gem. § 35 SGB I durchgehend von allen Mitarbeitern/-innen der Jugendämter ernst genommen wird. Bei den kontrollierten Jugendämtern handelte es sich um organisatorisch neu strukturierte Ämter unterschiedlicher Größe. Die Behörden sind zumeist in drei Abteilungen gegliedert: Jugend (Arbeit, Kita); Sozialer Dienst (Wirtschaftliche Jugendhilfe, Hilfen zur Erziehung, Pflegekinderdienst, Adoptionshilfewesen, Jugendgerichtshilfe) und Amtsvormundschaft, Amtpflegschaft/-beistandsschaft.

- Wahrung des Sozialgeheimnisses

Zur Wahrung des Sozialgeheimnisses wird das Personal besonders geschult und auf das Amtsgeheimnis verpflichtet. Bei einem Jugendamt ist die Anweisung ergangen, daß für Telefongespräche lediglich mit Vornamen der Betreuten zu operieren ist. Ansonsten werden z. B. Akten nicht mit Namen, sondern unter Registriernummern geführt. Die Aktenaufbewahrung entsprach datenschutzrechtlichen Erfordernissen.

Die zentrale Vorschrift des § 65 SGB VIII wird im allgemeinen eingehalten. Die Rechtsvorschrift schafft einen Vertrauenstatbestand zwischen dem Berater und dem Betroffenen, wenn personenbezogene Daten zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind. Nur in den dort aufgeführten Ausnahmefällen besteht eine Übermittlungsbefugnis. Die Anrufung des Gerichts zur Abwendung einer Gefährdung des Wohls des Kindes oder des Jugendlichen wird in den Fällen für notwendig erachtet, in denen Leib und Leben des Kindes bedroht und eine Entscheidung über das Aufenthaltsbestimmungsrecht zu treffen ist.

---

167 i. d. Fassung vom 3. Mai 1993, BGBl. I S. 637, zul. geänd. am 13. Juni 1994, BGBl. I S. 1229

Bei den mir zur Prüfung vorgelegten Vordruckformularen habe ich das Formular "Einverständniserklärung" begrüßt, weil es sich auf die unbedingt erforderlichen Angaben beschränkt. Darüber hinaus habe ich darauf hingewiesen, daß die dort vorgegebenen Zwecke der Auskunftserteilung, so z. B. zur Gewährung von Hilfen oder zur Jugendgerichtshilfe, angekreuzt oder zur Kennzeichnung des Einzelfalls markiert werden müssen. Bei von einzelnen Jugendämtern selbst erstellten Formularen war dagegen zu monieren, daß ein Hinweis auf die Rechtsgrundlage für die Datenerhebung fehlte.

- Aktenführung

Die sich aus § 65 SGB VIII ergebende Notwendigkeit einer Führung von Sonderakten zur Aufnahme besonders geschützter "anvertrauter" Daten habe ich bei den jeweiligen Jugendämtern angetroffen. Die Akten werden je nach Sachgebiet geführt, wobei eine Registrierung der Akten nach einem speziellen Aktenplan erfolgt. Die Zugriffsrechte werden durch die Amtsleiter/-innen festgelegt, wofür es ein gesondertes Genehmigungsverfahren gibt.

Im Rahmen der Jugendgerichtshilfe wird der gesamte Akteninhalt an das Amtsgericht übersandt. Im übrigen wird nur mit Einwilligung der Eltern das weitergeleitet, was für die Aufgabenerfüllung erforderlich ist. Bei Informationen quer durch die Akte wird geprüft, was in erforderlichen Auszügen mitgeteilt werden kann.

Hinsichtlich der Sperrung bzw. Löschung von Akten bestehen keine Erfahrungen. So sind bisher lediglich im Rahmen der Zusammenführung einzelne Papierstücke, wie z. B. Einladungen, vernichtet worden. Personenbezogene Akten werden im Archiv 30 Jahre aufbewahrt. Die Herausgabe von Akten wird protokolliert. Insbesondere in den Bereichen Hilfe für Erziehung, Pflegschaften/Vormundschaften wird zum Teil auf bereits archivierte Akten zurückgeriffen.

- Dienstanweisungen zum Datenschutz

Zum überwiegenden Teil existieren keine Dienstanweisungen zum Datenschutz. In einem Jugendamt wurde mir z. B. eine allgemeine Geschäftsanweisung übergeben, die unter dem Titel "Amtsverschwiegenheit, Datengeheimnis, Aussagegenehmigung" lediglich einen Hinweis auf das einzuhaltene Datengeheimnis enthielt. Eine solche allgemeine Geschäftsanweisung entspricht nicht den Anforderungen, die an eine Dienstanweisung i. S. d. § 78 a SGB X zu stellen ist. Nach dieser Vorschrift haben die in § 35 SGB I genannten Stellen, die selbst oder im Auftrag Sozialdaten verarbeiten, technische und organisatorische Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzbuches zu gewährleisten. Deshalb habe ich gefordert, daß eine Dienstanweisung zum Datenschutz erstellt werden muß. Die meisten Jugendämter haben bereits einen behördlichen Datenschutzbeauftragten eingesetzt.

- Räumliche Situation

Die räumlichen Verhältnisse, in denen die Jugendhilfesachbearbeiter arbeiten, sind in zahlreichen Ämtern Brandenburgs derart beengt, daß sie zumeist zu zweit oder sogar zu dritt in einem Raum sitzen. Gespräche mit mehreren Klienten in einem Raum finden nicht statt. Vertrauliche Gespräche mit den Klienten werden in einem gesonderten Beratungsraum durchgeführt. Die Jugendämter, die über einen solchen zusätzlichen Raum nicht verfügen, müssen die Klienten vor dem Gespräch um ihre Einwilligung bitten, ob sie mit der Anwesenheit weiterer Sozialarbeiter im selben Zimmer einverstanden sind. Denn die Beratung in einem Zimmer in Anwesenheit eines weiteren Mitarbeiters verstößt gegen § 35 Abs. 1 Satz 2 SGB I i. V. m. § 65 SGB VIII. § 35 Abs. 1 Satz 2 SGB I bestimmt, daß die Wahrung des Sozialgeheimnisses die Verpflichtung umfaßt, auch innerhalb des Leistungsträgers sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind oder nur

an diese weitergegeben werden. Wenn die Betroffenen sich mit der Anwesenheit eines zweiten Sozialarbeiters gem. § 65 Abs. 1 Nr. 1 SGB VIII einverstanden erklärt haben, ist dem Gesetz zwar formal Genüge getan, es ist aber zumindest zweifelhaft, ob Bürger in der beschriebenen Situation wirklich frei in ihrer Entscheidung sind, weil sie möglicherweise Nachteile befürchten. Daher müssen möglichst umgehend in allen einschlägigen Bereichen die erforderlichen Voraussetzungen für Einzelberatungen geschaffen werden. Bis dahin sollte in den Jugendämtern - wie bei allen Sozialleistungsträgern - darauf geachtet werden, daß in jedem Raum zur gleichen Zeit jeweils nur ein Gespräch mit Bürgern stattfindet.

Darüber hinaus habe ich auch festgestellt, daß in allen kontrollierten Jugendämtern ein Mithören auf Fluren aufgrund unzureichender Schallisolierungen der Türen möglich ist. Zur Verhinderung nach außen dringender vertraulicher Gespräche ist deshalb gerade im Hinblick auf die Besuchertage zu fordern, daß bauliche Maßnahmen - wie z. B. Schalldämmung der Türen oder Errichtung von Trennwänden - ergriffen werden müssen, um § 35 SGB I gerecht zu werden. Die zuständigen Stellen haben immer wieder ihre knappen Haushaltsmittel angeführt, die sie vorrangig für Sicherungszwecke (Brandsicherheit sowie Büroausstattung) verwenden müssen. Kostengründe können aber auf Dauer dem gesetzlich geschützten Grundsatz der Vertraulichkeit nicht entgegengehalten werden.

- Postöffnung im Jugendamt

Ein Jugendamt sprach mich auf die Problematik der Postöffnung an, d. h. es wurde bemängelt, daß Briefe zum Teil mit Verdienstbescheinigungen die Sachbearbeiterin geöffnet erreichen würden, obwohl eine direkte Zustellung möglich gewesen wäre. Hierzu verweise ich auf meine Ausführungen unter 9.1.5.

- ADV-Technik

Der Ausrüstungsstand der Jugendämter mit Rechentechnik ist im Land sehr unterschiedlich. Die Ausstattung reicht von Einzelplatz-PC bis hin zu lokalen Netzwerken. Ich mußte feststellen, daß besonders in Netzwerken nicht alle vom jeweiligen System zur Verfügung gestellten Sicherheitsfunktionen im vollen Umfang genutzt werden. Die Dateienregistermeldungen gem. § 24 Bbg DSG wurden mir noch nicht von allen Jugendämtern übersandt.

- Auskunftsrecht

In dem von mir zum Jahresende herausgegebenen Datenscheckheft befindet sich unter Ziff. 2 ein Musterschreiben ("andere Stellen"), das zur Durchsetzung von Auskunftsrechten verwendet werden kann. Nach Auskunft der Amtsleiter der Jugendämter machen die Betroffenen hiervon aber kaum Gebrauch. Überwiegend findet eine Einsichtnahme von klagenden Vätern statt, wobei hier Rechte Dritter - und zwar der Mütter - berührt sind und folglich zuvor deren Einwilligung eingeholt wird.

7.1.4 Schwangerschaftskonfliktberatung; Anerkennungsrichtlinien

Anknüpfend an meine Ausführungen im 2. Tätigkeitsbericht[168] hatte ich Gelegenheit, mit der Landesarbeitsgruppe (LAG) für Familienplanung, Sexualität und Schwangerschaft die praktische Umsetzung der dem Bundesverfassungsgerichtsurteil[169] zu entnehmenden Vorgaben sowie deren praktische Umsetzung für eine anonyme Beratung zu erörtern. Dabei stellte sich heraus, daß

168

169 s. unter 7.3.2, S. 127 ff.

vom 28. Mai 1993, BGBl. I S. 280

- für eine anonyme Beratung - von der nur in den seltesten Fällen Gebrauch gemacht wird - intern für das Protokoll eine Nummer vergeben wird und die Schwangere bei Ausstellung von Bescheinigungen ihren Namen selbst einträgt,

- bei Verlust der Bescheinigung die erneute Beratung wie eine Erstberatung behandelt wird und

- für die Ausstellung einer Beratungsbescheinigung kein Personalausweis, sondern lediglich die Vorlage einer auf den Namen der Schwangeren lautenden Bescheinigung verlangt wird.

Die Anerkennungsrichtlinien[170] sehen für die Schwangerschaftskonfliktberatungsstellen eine Aufbewahrungsfrist der Protokolle von max. zwei Jahren vor. Nach Abschluß des jährlich vorgesehenen Tätigkeitsberichts sind diese lediglich ein Jahr zu Kontrollzwecken für die Aufsichtsbehörde aufzubewahren. Aus meiner Sicht bestehen gegen diese zweijährige Aufbewahrungsfrist keine Bedenken.

Der Statistikbogen für die Schwangerenkonfliktberatung dient gleichzeitig zur Protokollierung einer stattgefundenen Beratung. Er enthält die im Bundesverfassungsgerichtsurteil festgelegten Angaben, wobei ich Wert darauf gelegt habe, daß das Alter lediglich mit dem Geburtsjahr angegeben wird. Daneben ist eine zusätzliche Abfrage über die soziale Situation der Schwangeren vorzusehen. Die Statistik soll Aussagen darüber ermöglichen, ob das Sozialpaket im Hinblick auf arbeitslose Frauen ausreichend ist. Diese Angaben werden - genauso wie die übrigen Angaben - auf freiwilliger Basis erhoben.

7.1.5 Kita-Beiträge: ein unendliches Thema!

Trotz meiner Ausführungen im 1. Tätigkeitsbericht[171] sowie in meinem 2. Tätigkeitsbericht[172] haben mich erneut Eingaben zu diesem Thema erreicht. Diesmal wies mich ein Bürger darauf hin, daß das Sozialamt alle Erziehungsberechtigten, deren Kinder Kita's im Amtsbereich besuchen, aufgefordert habe, eine Erklärung zum genauen Einkommen der Eltern auszufüllen. Darüber hinaus wurden dort die Formulare verteilt, zurückgenommen und anschließend für mehrere Tage aufbewahrt.

Nach der der Einkommensermittlung zugrunde liegenden Gebührenordnung war es meiner Auffassung nach lediglich erforderlich, die Betreuungsgebühren nach Einkommensgruppen festzulegen. Deshalb habe ich empfohlen, die jeweilige in der vom Petenten beigefügten Tabelle zur Betreuungsgebühr in Betracht kommende Einkommenskategorie (Jahresnettoeinkommen) unter Berücksichtigung der Betreuungszeit, der Anzahl und dem Alter der betreuten Kinder anzugeben.

Die Verteilung der Formulare und deren Rücknahme durch die Kindertagesstätten war erneut datenschutzrechtlich zu beanstanden. Nach § 17 Abs. 3 Satz 1 Brandenburgisches Kindertagesstättengesetz (BbgKita-Gesetz)[173] ist nicht die Kita die für die Festsetzung und Erhebung der Elternbeiträge zuständige Stelle, sondern grundsätzlich der Träger der Einrichtung. Die Beitragsfestsetzung durch Mitarbeiter der Kita kann lediglich dann vorgenommen werden, wenn diese auch neben pädagogischen Aufgaben

---

170

171 vom 1. Dezember 1994

172 s. unter 7.3, S. 45 ff.

173 s. unter 7.3.1, S. 126 ff.
vom 10. Juni 1992, GVBl. I S. 178

Verwaltungsaufgaben wahrnehmen. Anderenfalls müssen die Erziehungsberechtigten die Angaben in dem Formular gegenüber dem Betreiber machen, außer es sind alle Beteiligten mit der oben geschilderten Verfahrensweise einverstanden. Das war offensichtlich nicht der Fall.

Das Sozialamt hat meine Rechtsauffassung betreffend der widerrechtlichen Erhebung des genauen Einkommens geteilt und für die Zukunft folgendes Verfahren vorgeschlagen: Die Eltern erhalten weiterhin die Tabelle zur Einkommensgruppe und sollen lediglich die Angabe zur Höhe der von den Eltern selbst errechneten Gebühr notieren. Das Sozialamt behielt sich vor, bei Zweifeln einen Nachweis des Einkommens entsprechend § 17 Abs. 4 BbgKita-Gesetz zu verlangen. Die Formulare "Erklärung zum Einkommen" werden nach Aussage der Amtsleiterin unter Verschluß aufbewahrt, und nur eine Kollegin des Sozialamtes ist für die Herausgabe dieser Formulare zuständig. Auf die von dem Sozialamt gewählte Verfahrensweise, bei der Aushändigung der Formulare an die Eltern Unterstützung durch die Leiterinnen der Kindereinrichtungen zu erhalten, wird in Zukunft verzichtet werden. Außerdem wird künftig das Amt diese Vordrucke in geänderter Fassung selbst aushändigen.

Demgegenüber sind mir andere Erhebungsverfahren bekannt, in denen generell eine Glaubhaftmachung der Elternangaben verlangt wird. Dies geht auf ein Rundschreiben des MAGSF[174] zurück, in dem allen Jugendämtern der Kreise und kreisfreien Städte mitgeteilt wurde, daß im Interesse der Beitragsgerechtigkeit eine solche Überprüfung der Elternangaben einschließlich der Vorlage geeigneter Unterlagen zulässig sei.

Soweit die Verwaltung nicht bereit ist, von diesen Vorgaben abzurücken, ist ihr gegenüber leider keine datenschutzfreundlichere Vorgehensweise im Interesse der Betroffenen durchzusetzen.

174 vom 15. September 1992, ABl. S. 1918

7.2 Gesundheitswesen

7.2.1 Verwaltungsvorschriften und Verordnungen im Gesundheitswesen

7.2.1.1 Entwurf der Verordnung für Hebammen und Entbindungspfleger im Land Brandenburg

Auf die Berufsordnung bin ich schon in meinem 2. Tätigkeitsbericht[175] eingegangen. Ein mir im September vergangenen Jahres erneut vorgelegter Entwurf war zuvor mit den betroffenen Verbänden abgestimmt worden.

In § 5 Abs. 1 Satz 2 der Verordnung, der die Dokumentationspflicht regelt, ergeben sich die Mindestanforderungen für den Inhalt der von Hebammen und Entbindungspflegern zu führenden Aufzeichnungen. Näheres ist aus der Anlage 2 ersichtlich, wonach die Dokumentation anhand von Formblättern (Geburtsprotokoll) zu führen ist. Da in § 5 Abs. 1 Satz 3 festgelegt ist, daß das zu führende Geburtsprotokoll von Hebammen und Entbindungspflegern außerhalb von Krankenhäusern Mindestangaben entsprechend der Anlage 2 der Verordnung enthalten soll und es somit den Betroffenen freigestellt wird, ein im freien Handel oder selbst entwickeltes Formblatt zu verwenden, besteht damit die Gefahr, daß darüber hinaus datenschutzrechtlich unzulässige Angaben erhoben werden. Um diese Gefahr einzudämmen, habe ich vorgeschlagen, entweder für alle ein verbindliches Formblatt vorzuschreiben oder zumindestens einen schriftlichen Hinweis zu geben, daß z. B. die Angabe des Berufes der Mutter oder des Vaters zu Abrechnungszwecken nur für den Fall der fehlenden Berufstätigkeit des Partners zu erheben ist.

Begrüßt habe ich, daß § 5 Abs. 2 Satz 1 der Verordnung entsprechend meinen damaligen Vorgaben ergänzt worden ist. Jedoch ist dort nun bestimmt, daß bei Unterbrechung der beruflichen Tätigkeit der Hebammen und Entbindungspfleger um mehr als drei Jahre sowie bei Berufsaufgabe unverzüglich die Aufzeichnungen und die Geburtskontrolle dem örtlich zuständigen Gesundheitsamt zu übergeben sind. Die festgelegte Frist von drei Jahren ist aus meiner Sicht nicht nachvollziehbar. Außerdem hatte ich wegen des Gebots der Normenklarheit gefordert, daß die Aufzeichnungen im Falle des Todes der freiberuflich tätigen Hebammen und Entbindungspfleger dem zuständigen Gesundheitsamt zu übergeben sind, um damit den Zugang Unbefugter von vornherein auszuschließen. Das Ministerium ist diesem Vorschlag bislang nicht gefolgt.

Die in § 6 festgelegte Schweigepflicht der Verordnung sollte auch nach Beendigung der beruflichen Tätigkeit fortgelten und § 203 StGB als gesetzliche Grundlage hierfür ausdrücklich genannt werden.

7.2.1.2 Verwaltungsabkommen zum Krebsregister

Unabhängig von den Bestrebungen des Bundes, ein Krebsregistergesetz zu verabschieden (s. unter 6.3.1), bestand für die neuen Bundesländer und Berlin die Notwendigkeit, anstelle des nur bis zum 31. Dezember 1994 geltenden Krebsregistersicherungsgesetzes[176] eine lückenlos greifende Nachfolgeregelung zu schaffen. Im Vorgriff darauf haben sich diese Länder bereits im Mai 1993 politisch geeinigt, das sog. nationale Krebsregister der DDR als Gemeinsames Krebsregister über das Jahr 1994 hinaus fortzuführen, und Berlin federführend beauftragt, die dazu erforderlichen gesetzlichen Regelungen vorzulegen sowie verwaltungsmäßigen Voraussetzungen zu schaffen. Mit dem Inkrafttreten des

---

175

176 s. unter 7.2.6, S. 119 ff.

vom 21. Dezember 1992, BGBl. I S. 2335

Krebsregistergesetzes[177] waren jedoch diese Bemühungen zunichte gemacht. Es wurde der Abschluß eines Verwaltungsabkommens noch vor Ende 1994 angestrebt, um den Bestand und die Finanzierung des Gemeinsamen Krebsregisters übergangsweise zu sichern.

Über diese Bemühungen wurde ich nicht von unserem zuständigen Ministerium, sondern von meiner Thüringer Kollegin informiert. Die von den Datenschutzbeauftragten erhobenen Bedenken sowie Verbesserungsvorschläge konnten in den Entwurf nicht mehr einfließen, weil die Zeit bis zur bereits festgesetzten Paraphierung des Verwaltungsabkommens nicht mehr reichte. Dies betraf insbesondere die Frage, welche Landesdatenschutzgesetze für Neumeldungen aus dem öffentlichen Bereich gelten sollen. Um so mehr bedarf es eines Länderausführungsgesetzes zum Krebsregistergesetz, denn der verfassungsrechtliche Gesetzesvorbehalt kann nicht durch eine untergesetzliche Verwaltungsvorschrift umgangen werden. Der Entwurf für ein Gesetz sollte deshalb bereits im ersten Quartal 1995 erarbeitet werden; dieser liegt bisher nach meiner Kenntnis aber noch nicht vor.

7.2.2 Landesärztekammer Brandenburg

7.2.2.1 Beitragsordnung der Ärzte

Protest kam bei vielen Ärzten des Landes auf, als die Beitragsordnung der Landesärztekammer Brandenburg durch eine neue abgelöst wurde, nach der nun die Mitglieder Nachweise über die Höhe der Einkünfte aus ärztlicher Tätigkeit vorlegen müssen. Die Ländesärztekammer verspricht sich dadurch eine nachvollziehbarere Beitragsgerechtigkeit. Die betroffene Ärzteschaft hingegen empfindet die Übergabe eines Einkommenssteuerbescheides an die Ärztekammer als Zwang und die Zahlung des Höchstbetrages von 4.000 DM bei Weigerung eines Nachweises als "Strafbetrag".

Nach Auskunft der hiesigen Landesärztekammer sei sie zur neuen generellen Vorlagepflicht durch das Bemühen, fehlerhafte Selbsteinstufungen und damit eine tatsächliche Ungleichbehandlung der Kammermitglieder zu verhindern, bewogen worden. Weiterhin sei die Vorgehensweise insofern datenschutzrechtlich bedenkenfrei, als der Einkommenssteuerbescheid bis auf die relevanten Teile geschwärzt werden könne. Durch eine streng zweckgebundene Verwendung der Daten, der Vernichtung der Angaben zur Höhe der Einkünfte nach Einstufung des Kammermitgliedes sowie der Beschränkung des Kreises der Einsichtsberechtigten glaubt die Landesärztekammer alle datenschutzrechtlichen Bedenken ausgeräumt zu haben. Des weiteren verweist sie auf ähnliche Verhältnisse wie z. B. im Land Hamburg.

Die Rechtsgrundlage für die Vorlagepflicht der Einkommenshöhe ergibt sich aus § 26 Abs. 1 i. V. m. § 5 Abs. 1 Heilberufsgesetz (HeilBerG)[178]. Nach § 5 Abs. 1 HeilBerG können die Kammern von den Kammerangehörigen Auskünfte verlangen, die sie zur Wahrnehmung ihrer gesetzlichen Aufgaben benötigen. Die Durchsetzung einer den tatsächlichen Bedingungen entsprechende Beitragserhebung ist notwendige Voraussetzung für die Wahrnehmung und Aufnahme der Kammertätigkeit und den hiermit verbundenen Aufgabenfeldern. Die Satzungsermächtigung für die Beitragsordnung der Ärztekammer enthält zwar keine ausdrückliche Ermächtigung von den Kammermitgliedern, auch Auszüge des Einkommenssteuerbescheides zu verlangen, jedoch überträgt die Satzungsermächtigung die Regelung dieses Bereiches in die Selbstverwaltung der Betroffenen.

Die Kammerversammlung selbst, also das Selbstverwaltungsorgan der Betroffenen, hielt die

---

177

178 vom 4. November 1994, BGBl. I S. 3551
vom 28. Januar 1992, GVBl. S. 30, zul. geänd. durch 1. ÄndG. vom 15. Dezember 1993, GVBl. I S. 511

Novellierung ihrer Beitragsordnung für geboten. Die Datenerhebung aus dem Steuerbescheid des Bezugsjahres der Beitragsbemessung bzw. der Bestätigung durch den Steuerberater zur Erfüllung der Kammeraufgaben ist meiner Auffassung nach gem. § 12 Abs. 1 Bbg DSG erforderlich. Dennoch erscheint es mir unverhältnismäßig, den Nachweis der Einkünfte aus ärztlicher Tätigkeit von allen Kammermitgliedern zu fordern, zumal in Brandenburg - wie in anderen Bundesländern gerade durch umfangreiche Stichprobenprüfungen bestätigt - keine konkreten Fälle von Fehleinstufungen durch die Ärzte bekannt geworden sind.

Aus diesem Grunde hielt ich folgendes zweistufiges Stichprobenverfahren für ausreichend: Zunächst sollte es bei der Selbsteinstufung mit Hilfe der beizufügenden Beitragstabelle durch die Kammerangehörigen bleiben und stichprobenartig quer durch alle 29 Beitragsstufen die angegebene Höhe der Einkünfte aus ärztlicher Tätigkeit anhand der vorzulegenden Kopien einzelner Ärzte überprüft werden. Erst nach erneuter Bewertung der veränderten Sachlage, z. B. bei im Rahmen der Stichprobenprüfungen festgestelltem Mißbrauch im Beitragsverhalten der Ärzte, halte ich für die Durchsetzung einer hohen Beitragsgerechtigkeit eine generelle Vorlagepflicht für alle Ärzte für zulässig.

Von der Landesärztekammer wird nach wie vor die Effektivität der Stichprobenprüfung als mildestes Mittel gegenüber der generellen Vorlagepflicht unterschätzt. Die Landesärztekammer geht davon aus, daß ein solches Verfahren zu einem erheblichen Finanzierungsrisiko der Kammer führen kann, das nur über eine generelle Anhebung des Kammerbeitrages kalkulierbar sein könnte.

Dem ist zu entgegnen, daß jeder Arzt nach eigener Selbsteinstufung damit rechnen muß, einen Nachweis über seine Angaben erbringen zu müssen, da anfangs noch nicht feststeht, welcher Arzt zur Stichprobe herangezogen wird.

7.2.2.2 Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Kassenarzt

Für die Zulassung von Ärzten zur vertragsärztlichen Versorgung sind Voraussetzungen und Verfahren in § 95 ff. SGB V und in der Zulassungsordnung für Vertragsärzte (Ärzte-ZV)[179] geregelt, wobei nach § 18 Abs. 2 Buchst. b Ärzte-ZV dem Antrag auf Zulassung als Vertragsarzt ein polizeiliches Führungszeugnis "beizulegen" ist. Dem Wortlaut nach handelt es sich um das "Privatführungszeugnis" nach der Belegart N gem. § 30 Abs. 1 BZRG; denn nur dieses Führungszeugnis schickt das Bundeszentralregister demjenigen, der es beantragt, selbst zu. Für die Prüfung der in § 21 Ärzte-ZV aufgeführten Ausschlußkriterien (Trunk- und Rauschgiftsucht in den letzten fünf Jahren) sieht § 18 Abs. 1 Buchst. e aber lediglich die Vorlage einer Erklärung vor.

Auf Nachfrage teilte mir die Kassenärztliche Vereinigung Brandenburg mit, sie halte es - abweichend von der Gesetzesvorgabe für die Zulassung zur vertragsärztlichen Tätigkeit - sogar für erforderlich, das "Behördenführungszeugnis" nach der Belegart O gem. § 30 Abs. 5 BZRG zu verlangen. Dieses enthält ggf. auch Angaben über die o. g. Ausschlußkriterien und wird vom Bundeszentralregister direkt an die Behörde geschickt, für die es bestimmt ist.

Nach der derzeitigen Rechtslage kann der zuzulassende Arzt aber weder veranlaßt werden, ein polizeiliches Führungszeugnis beizubringen, noch ist aufgrund der abschließenden spezialgesetzlichen Regelung die Anforderung des "Behördenführungszeugnisses" zulässig, selbst wenn für das Bundeszentralregister die allgemeinen Übermittlungsvoraussetzungen

---

179 vom 28. Mai 1957, BGBl. I S. 572 , ber. S. 608; zul. geänd. durch Gesundheitsstrukturgesetz vom 1. Dezember 1992, BGBl. I S. 2266

nach dem BZRG vorliegen sollten. Insoweit steht dringend entweder eine Änderung der Verfahrensweise des Zulassungsausschusses oder der Ärzte-ZV an. Das MAGSF hat mir zugesagt, sich für letzteres beim Bundesministerium für Gesundheit einzusetzen.

7.2.3 Staatliches Gesundheitswesen

7.2.3.1 Umgang mit Impfdateien

Von den Bestimmungen des sog. Runderlasses über "Meldung, Aufbewahrung und Nutzung von Patientenunterlagen ... aus ehemaligen Gesundheitseinrichtungen der DDR"[180] sind Impfdateien seinerzeit ausdrücklich ausgenommen worden und sollten nach Ziff. 3 Nr. 4 durch ein gesondertes Rundschreiben geregelt werden. Mehrfache Anfragen veranlaßten mich, die noch ausstehende Regelung beim MAGSF anzumahnen. Von dort erhielt ich deshalb Anfang 1995 eine Einladung zu einer Beratung der Impfkommission. Dort mußte ich bedauerlicherweise feststellen, daß noch immer keine sachliche Konzeption hinsichtlich der Weiterführung der Impfkarteien in den staatlichen Gesundheitsämtern entwickelt worden ist, die datenschutzrechtlich bewertet werden kann. Dieser Zustand ist um so verwunderlicher, als sich die mit der Sache befaßten Ärzte der Bedeutung der Pflege einer Impfdatei sehr wohl bewußt sind und wiederholt auf die Folgen hingewiesen haben, wenn im Seuchenfall nicht annähernd genau der Durchimpfungsgrad der Bevölkerung abgeschätzt werden kann.

Die in den vergangenen Jahren hierzu erhaltenen Anfragen aus den staatlichen Gesundheitsämtern belegen, daß dort sehr unterschiedliche Verfahren im Umgang mit der Einwilligungserklärung über die Führung und die zu erteilenden Auskünfte aus den vorhandenen Dateien angewandt werden. Diese Eigeninitiativen sind einerseits zu begrüßen; sie ersetzen aber andererseits keine zentralen Vorgaben über die Führung von Impfdateien in den staatlichen Gesundheitsämtern.

Als Rechtsvorschrift, die die Voraussetzung für die Abgabe der Einwilligungserklärung festlegt, ist § 4 Abs. 2 i. V. m. § 12 Abs. 3 Bbg DSG heranzuziehen. Danach bedarf die Einwilligungserklärung der Schriftform; der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten bei einer beabsichtigten Übermittlung, über die Empfänger der Daten sowie den Zweck der Übermittlung aufzuklären. Bei weitem nicht alle mir vorgelegten Einwilligungserklärungen erfüllen diese Anforderungen.

Das MAGSF hat mir gegenüber signalisiert, daß es eine landesweite Konzeption zur Führung von Impfdateien entwickeln wird.

7.2.3.2 Überwachung der klinischen Prüfung von Arzneimitteln

Die ab dem 17. August 1995 in Kraft tretende Vorschrift des § 40 Abs. 1 Nr. 2 Arzneimittelgesetz (AMG)[181] sieht vor, daß die Person, bei der eine klinische Prüfung durchgeführt werden soll, "mit ihrer Einwilligung hierzu gleichzeitig erklärt, daß sie mit der im Rahmen der klinischen Prüfung erfolgenden Aufzeichnung von Krankheitsdaten und deren Weitergabe zur Überprüfung an den Auftraggeber, an die zuständige Überwachungsbehörde oder die zuständige Bundesoberbehörde einverstanden ist".

Das Landesamt für Soziales und Versorgung hat als Überwachungsbehörde gem. § 1 Nr. 3

180

181 vom 22. November 1993, ABl. S. 1725
vom 9. August 1994, BGBl. I S. 2071

Brandenburgische Verordnung über die Zuständigkeiten im Arzneimittelwesen[182] die von dem Patienten vor der Durchführung einer klinischen Prüfung abzugebenden Einwilligungserklärung zu überprüfen. Der mit der Übernahme der klinischen Prüfung Beauftragte darf sich durch Einblick in die betreffenden Unterlagen bei dem Prüfarzt davon überzeugen, daß eine schriftliche Einverständniserklärung eingeholt wurde. Das kann nicht mit dem Hinweis auf die ärztliche Schweigepflicht abgelehnt werden.

Die Einwilligungserklärung hat neben den Grunddaten (Name, Anschrift, Geburtsdatum) die Bezeichnung der Studie sowie die Probandennummer als Hilfsmerkmal für den Prüfbogen zu enthalten; über den Wortlaut des § 40 Abs. 1 Nr. 2 neue Fassung und § 40 Abs. 2 AMG[183] ist der Proband unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und jederzeit widerrufen kann.

7.2.3.3 Melde-Formulare nach dem Bundesseuchengesetz

Der Landesbeauftragte für den Datenschutz eines anderen Bundeslandes hat mir von dem neuen Melde-Formblatt zur Erfassung von "humanen spongiformen Enzephalopathien" berichtet sowie auf eine mögliche Reidentifizierung bei der Verwendung dieser Formblätter hingewiesen. Der für die "anonyme Meldung" über die zuständigen Landesbehörden und an das Robert-Koch-Institut zu übersendende Durchschlag des Formblattes enthält keine durch einen Schlüssel vorgegebenen, sondern als Freitext einzutragende Angaben zum Beruf, die allein in Verbindung mit den ersten drei Stellen der Postleitzahl, Geburtsmonat, Jahr und Staatsangehörigkeiten sowie - insbesondere bei Vorhandensein entsprechenden Zusatzwissens - Hinweise auf bestimmbare natürliche Personen ergeben können.

Die Personenbeziehbarkeit halte ich datenschutzrechtlich für bedenklich. Das MAGSF teilt diese Bedenken und hat zugesagt, den Verfasser der Formblätter zu bitten, beim Eintrag unter dem Begriff "Beruf" die ausbildungsbedingt erworbenen Fähigkeiten entsprechend dem Berufsbildungsgesetz zu verschlüsseln und auf eine Funktion, wie z. B. Landrat, zu verzichten. Vorgesehen ist ein entsprechender Hinweis in der Veröffentlichung bzw. als Information in den Fachorganen der Landesärztekammern. Darüber hinaus hat es dem Bundesministerium für Gesundheit meine datenschutzrechtlichen Bedenken mitgeteilt sowie die Gesundheitsämter entsprechend informiert.

7.3 Krankenhauswesen

7.3.1 Entwurf: Brandenburgisches Psychisch-Kranken-Gesetz (BbgPsychKG)

Nachdem ich in meinem 2. Tätigkeitsbericht[184] auf das Unterlassen der Aufnahme bereichsspezifischer Regelungen in diesem Gesetzentwurf hingewiesen habe, ist mir im Berichtszeitraum ein überarbeiteter Entwurf mit der Bitte um Stellungnahme zugeleitet worden. Dieser Entwurf behandelt die Regelung von besonderen Hilfsmaßnahmen, die öffentlich-rechtliche Anordnung und ggf. sofortige Einleitung von freiheitsentziehenden Maßnahmen für psychisch Kranke und seelisch Behinderte.

Für begrüßenswert halte ich den durchgehenden Begründungs- und Dokumentationszwang bei Einschränkungen hinsichtlich der Rechte der Betroffenen sowie die Aufnahme von

---

182

183 vom 27. Oktober 1992, GVBl. II S. 693

184 § 40 Abs. 1 Nr. 7 a eingef. durch Art. 1 Nr. 23, Ges. v. 16. August 1986, BGBl. I S. 1296

s. unter 7.2.3.2, S. 111

Vorschriften zur Datenverarbeitung (§ 48) und über das Zusammenwirken mit anderen Behörden und Einrichtungen (§ 49). Da die Einzelbestimmungen aber wegen ihrer starken Orientierung an dem novellierungsbedürftigen Brandenburgischen Gesundheitsdienstgesetz (BbgGDG) Unzulänglichkeiten aufwiesen, habe ich u. a. zur Normenklarheit folgende ergänzende Forderungen aufgestellt:

- Es soll sichergestellt werden, daß von Kenntnissen, die bei der Überwachung des Schriftwechsels von untergebrachten Personen erlangt werden, nur unter klar bestimmten, engen Voraussetzungen Gebrauch gemacht werden darf. In ihrem Kernbereich sollen nämlich die Persönlichkeitsrechte der Betroffenen - soweit möglich - trotz der einschränkenden Maßnahmen unangetastet bleiben. So darf z. B. auch der Schriftwechsel der untergebrachten Person mit dem Landesbeauftragten für den Datenschutz nicht eingesehen werden.

- Die von mir grundsätzlich begrüßte Regelung der Schaffung eines Patientenfürsprechers im Rahmen des Beschwerderechts der untergebrachten Person läßt offen, welche Rechte (z. B. Akteneinsichtsrechte) sowie Pflichten (insbesondere in Bezug auf die Verschwiegenheitspflicht der ihm anvertrauten Daten) ihm obliegen.

- Eine klare Benennung der Aufgabenfelder der Besuchskommissionen sollte die Wahrung der Rechte der untergebrachten Personen mit umfassen. Darüber hinaus sollten auch hier die Rechte der Kommissionsmitglieder bzw. deren Pflichten (Verschwiegenheitspflicht) näher bestimmt werden.

- Den eingefügten datenschutzrechtlichen Bestimmungen (s. oben) sollte ein weiterer Paragraph vorangestellt werden, der die grundsätzliche Gültigkeit des Brandenburgischen Datenschutzgesetzes sowie die Geltung des Landeskrankenhausgesetzes klar hervorhebt.

- Die Übermittlung personenbezogener Daten sollte an öffentliche Stellen nur zulässig sein, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und weitere einschränkende Voraussetzungen nach § 13 Bbg DSG vorliegen. Da diesbezüglich der Entwurf nicht normenklar war, sollte der Begriff der Übermittlung entfallen und in einem späteren eigenständigen Paragraphen festgelegt werden.

- Die Voraussetzungen der Datenspeicherung sollten - um deren Stellenwert angemessen zu berücksichtigen - in einem eigenen Paragraphen aufgeführt werden.

- Die im Entwurf des BbgPsychKG enthaltenen drei unterschiedlichen Zwecke, und zwar

  1. die Hilfeleistung zugunsten der psychisch Kranken,
  2. die Schutzmaßnahmen vor diesen sowie
  3. die Vollzugsmaßnahmen im Rahmen der Unterbringung,

  müssen informationell klar getrennt werden[185]. Zur Verdeutlichung des Zweckbindungsgebotes habe ich darauf hingewiesen, daß eine Verarbeitung von Daten nur zu dem Zweck in Betracht kommt, zu dem sie auch erhoben worden sind. So dürfen personenbezogene Daten, die im Zusammenhang mit den Hilfen nach diesem Gesetz vom sozialpsychiatrischen Dienst erhoben worden sind, nicht gleichzeitig für den Bereich der Unterbringungsmaßnahmen verarbeitet werden.

- Die Löschung aller gespeicherten Daten, die bei der Durchführung dieses Gesetzes

185 BVerfGE 65, 1

anfallen, sollten aus Transparenzgründen in einem Absatz geregelt werden.

- Eine Übermittlung erforderlicher personenbezogener Daten "in Fällen von Verstößen gegen gesetzliche Vorschriften" an die zuständigen Verwaltungsbehörden muß in der Weise klargestellt werden, daß nur solche Verstöße gemeint sind, die im Zuge der Wahrnehmung der Aufgaben im Rahmen der Einrichtungen und Stellen nach dem BbgPsychKG auftreten.
- Die Übermittlungsmodalitäten müssen wegen des Gebots der Normenklarheit präziser gefaßt werden. So sollte eine Übermittlung gegenüber dem zuständigen Gericht oder der zuständigen Betreuungsbehörde nur zulässig sein, soweit dies erforderlich ist, um die Notwendigkeit einer dem Schutz oder der Betreuung einer betroffenen Person dienenden Anordnung nach diesem Gesetz oder nach dem Betreuungsgesetz[186] zu begründen.

Das MAGSF hat meine Änderungsvorschläge weitestgehend berücksichtigt. Nach wie vor bleibt es jedoch unklar, welche Rechte dem Patientenfürsprecher eingeräumt bzw. welche Pflichten ihm auferlegt werden. In diesem Zusammenhang ist lediglich festgelegt worden, daß Kenntnisse, die im Rahmen einer Beschwerde über persönliche Belange einer untergebrachten Person erlangt werden, vertraulich zu behandeln sind. Dies ist kein Equivalent zu der von mir geforderten Verschwiegenheitsverpflichtung i. S. v. § 203 StGB. Im übrigen hat das MAGSF darauf verzichtet, die Voraussetzungen der Speicherung sowie der Löschung aller anfallenden Daten in eigenständigen Paragraphen zu regeln.

7.3.2 Krankenhausdatenschutzverordnung - eine Geduldsprobe für die Anwender

Wie bereits schon in meinem 2. Tätigkeitsbericht[187] angekündigt, wurde mir Ende März 1994 vom MAGSF der Entwurfstext einer Verordnung zum Schutz von Patientendaten im Krankenhaus (KHDsV) zur Abstimmung übergeben, der sich an der Ermächtigungsnorm im Krankenhausgesetz des Landes Brandenburg (LKGBbg)[188] orientiert und in seinem Regelungsinhalt meine damaligen Vorgaben aufgegriffen hat.

Gespräche mit Fachleuten aus der Praxis haben mich darin bestärkt, verschiedene Einzelregelungen weiter zu präzisieren. Dies betraf insbesondere nachfolgende Punkte:

- Datenspeicherung:

  Im Zuge der fortschreitenden Technisierung muß sichergestellt werden, daß bereits heute absehbare Entwicklungen von zur Verfügung stehenden Datenträgern im Krankenhausbereich Berücksichtigung finden müssen. Für Patientendaten sind aber nur Datenträger geeignet, die eine Löschung und Speicherung zulassen (s. hierzu auch unter 1.3.6).

- Verarbeitung von Patientendaten:

  Zu Aus-, Weiter- und Fortbildungszwecken in Berufen des Gesundheitswesens sind lediglich Patientenunterlagen in anonymisierter Form erforderlich.

- Übermittlung von Patientendaten:

  Eine Übermittlung von Patientendaten an Personen außerhalb des Krankenhauses ist

---

186

187 vom September 1990, BGBl. I S. 2002

188 s. unter 7.2.3.1
vom 11. Mai 1994, GVBl. I S. 106

zulässig, soweit sie erforderlich ist zur Unterrichtung der Angehörigen, soweit die Patientin oder der Patient keinen gegenteiligen Willen geäußert haben oder sonstige Anhaltspunkte bestehen, daß eine Übermittlung für den Betroffenen nachteilig wäre.

- Datenverarbeitung im Auftrag:

  Da die Datenverarbeitung im Auftrag grundsätzlich nur im Krankenhausbereich stattfinden soll und die Zulassung von Ausnahmen restriktiv zu handhaben ist, sind die Voraussetzungen, unter denen eine Datenverarbeitung durch "andere Personen oder Stellen" hingenommen werden kann, konkret zu bezeichnen. Deshalb empfahl ich eine gem. § 80 Abs. 5 SGB X entsprechende Formulierung aufzunehmen, nach der die Verarbeitung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen nur zulässig ist, wenn anders beim Auftraggeber Störungen im Betriebsablauf nicht vermieden oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfaßt.

- Datenschutz bei Forschungsvorhaben:

  Die Einwilligung des Patienten soll bei einer Datenverarbeitung für Forschungszwecke entbehrlich sein, wenn der Zweck eines bestimmten Forschungsvorhabens nicht anders zu erfüllen ist und das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegt. Mit einer solchen Bestimmung ist für den Normanwender nicht nachvollziehbar, wann das Allgemeininteresse gegenüber dem Geheimhaltungsinteresse des Patienten überwiegt. Um einen Mißbrauch möglichst zu verhindern, habe ich im Interesse einer sachgerechten Abwägung zwischen dem Forschungsinteresse einerseits und dem Interesse des einzelnen an der Nichtverwendung seiner Daten andererseits vorgeschlagen, vor einer Einzelentscheidung durch die zuständige oberste Aufsichtsbehörde auf jeden Fall auch meine Behörde anzuhören.

Zwischenzeitlich hat mir das Ministerium einen überarbeiteten Entwurf vorgelegt, in dem alle meine Anregungen und Formulierungen sowie weitere Stellungnahmen der Landesärztekammer Brandenburg, des Landkreistags Brandenburg und einem Klinikum eingearbeitet worden sind. Jedoch ist das Ministerium auf meine mehrfachen Hinweise, daß die Abfassung des Patientendatenschutzes in Gestalt einer Rechtsverordnung nicht den im Volkszählungsurteil festgelegten Anforderungen an ein Gesetz im formellen Sinne entspricht, mit keiner Silbe weder im Zusammenhang mit der Stellungnahme der Landesregierung zu meinem 2. Tätigkeitsbericht (LT-Drs. 2/169) noch im sonstigen Schriftverkehr eingegangen. Mir wurde lediglich in Aussicht gestellt, daß der Entwurf noch im Jahr 1994 in den zuständigen Gesundheitsausschuß eingebracht werden könne. Dort ist er aber bis heute nicht angekommen. Ich muß daher vermuten, daß die Landesregierung in der Angelegenheit offensichtlich keine Eilbedürftigkeit sieht. Die in den nachfolgenden Abschnitten aufgeführten, möglicherweise darauf zurückzuführenden Vorkommnisse stellen vermutlich nur "die Spitze eines Eisberges" datenschutzrechtlicher Verstöße im Krankenhausbereich dar.

7.3.2.1 Einwilligungserklärung für Übermittlungen an Dritte

Den Hintergrund hierfür habe ich - sowohl was die rechtliche Seite als auch die landesweit bestehenden Unzulänglichkeiten der praktischen Handhabung dieser Problematik anbelangt - in meinem 2. Tätigkeitsbericht[189] dargestellt. Ich habe angekündigt, in Abstimmung mit dem Ministerium für Arbeit, Gesundheit, Soziales und Frauen zu prüfen, ob nicht zur Abstellung

189 s. unter 7.2.3.6, S. 115 ff.

dieser Mängel eine Mustererklärung entwickelt und zumindest in den Krankenhäusern in öffentlicher Trägerschaft zur Verwendung empfohlen werden könnte.

Die daraufhin angesprochene Krankenhausgesellschaft Brandenburg e. V. ließ sich für die Umsetzung dieser Vorstellung erfreulicherweise gewinnen und hat zwischenzeitlich allen Krankenhäusern des Landes empfohlen, den mit meiner Behörde abgestimmten Aufnahmebeleg als Ergänzung zum Krankenhausaufnahmevertrag[190] zu verwenden. Im übrigen bleibt es den einzelnen Krankenhäusern überlassen, entsprechend ihren technischen Möglichkeiten die im Aufnahmebeleg verbindlichen, inhaltlichen Vorgaben unmittelbar in den Aufnahmevertrag einzubeziehen.

Ich hoffe, daß damit inzwischen auch die wohl zu Recht im Berichtszeitraum mehrfach an mich herangetragenen Beschwerden von Krankenhausseelsorgern, ihnen würden wegen des Datenschutzes die sog. "Pfarrer-Listen" vorenthalten, durch diesen Lösungsvorschlag auch in der Praxis gegenstandslos sind.

7.3.2.2 Patientenliste im Hausmüllcontainer - belanglose Daten?

Einer Lokalzeitung habe ich entnehmen können, daß ein Computerausdruck u. a. mit

- Patientennummer,
- Patientenname,
- Geburtsdatum,
- Aufnahme, Uhrzeit,
- Station und
- Fachrichtung

im Hausmüllcontainer eines Kreiskrankenhauses aufgefunden worden sei. Solche Listenausdrucke über Patienten werden zu statistischen Zwecken der Patientenverwaltung ausgewertet und außerdem mit Einverständnis des Patienten für die täglichen Auskünfte an der Pforte genutzt.

Wenn es sich dabei nur um ein bedauerliches menschliches Versagen gehandelt hätte, wäre an dieser Stelle nichts zu berichten. Aber die Einschätzung der Verwaltungsleiterin - mit dieser Liste seien "in keinem Fall sensible Daten an die Öffentlichkeit gelangt" - ließ mich aufhorchen. Es kann nicht oft genug gesagt werden, daß es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum gibt[191]. Bereits die Tatsache des Krankenhausaufenthaltes stellt für den einzelnen ein schutzwürdiges Datum dar, weil es geeignet ist, daraus Rückschlüsse auf den Gesundheitszustand des Betroffenen zu ziehen.

Immerhin war die Krankenhausverwaltung durch den Vorfall soweit sensibilisiert worden, daß sie ihrerseits die Erarbeitung einer Dienstanweisung für den Datenschutz und die Datensicherheit in Angriff nahm und mich dabei um Mithilfe bat. Ich würde es begrüßen, wenn auch andere Krankenhäuser diesem Beispiel, den Umgang mit Patientendaten im Krankenhaus für die Ärzte sowie die übrigen Mitarbeiter mittels Dienstanweisung verbindlich zu regeln, folgen würden.

7.3.2.3 Verletzung der ärztlichen Schweigepflicht?

Eine Petentin beschwerte sich bei mir darüber, daß die Tatsache sowie der Grund eines Krankenhausaufenthaltes ihrer Tochter über den psychiatrischen Dienst des Krankenhauses

---

190

191 siehe Anlage 2

BVerfGE 65, 1 (45)

zum Jugendamt gelangt sei. Hierin sah die Petentin eine Verletzung der ärztlichen Schweigepflicht.

Hintergrund der Beschwerde war folgender Sachverhalt: Die Chefärztin der Kinderabteilung eines Kreiskrankenhauses hatte sich am Tage nach der Entlassung der Tochter der Petentin, die gegen ärztlichen Rat erfolgte, telefonisch sowohl an eine Mitarbeiterin des sozialpsychiatrischen Dienstes als auch an die nachbehandelnde Ärztin gewandt, um auf die aus ihrer Sicht noch nach wie vor gegebene suizidale Gefährdung des Kindes hinzuweisen. Angesichts der möglichen Gefahr im Verzuge - die dadurch vorlag, daß das Mädchen bereits mehrere Suizidversuche unternommen hatte und somit Wiederholungsversuche nicht auszuschließen waren - und nach sorgsamer Abwägung der Rechtslage schaltete die Mitarbeiterin des sozialpsychiatrischen Dienstes ihrerseits das Jugendamt ein mit der Bitte, sich mit dem Kind in Verbindung zu setzen.

Unter diesen Umständen konnte ich in den für mich nachvollziehbaren Bemühungen der Chefärztin keine Verletzung ihrer ärztlichen Schweigepflicht gem. § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB)[192] erkennen. Ein solcher Verstoß setzt eine unbefugte Offenbarung eines fremden Geheimnisses voraus, das jemandem z. B. als Arzt anvertraut oder sonst bekannt geworden ist. Hier war die Ärztin zur Offenbarung befugt, da diese erforderlich war zum Schutze eines höherwertigen Rechtsgutes, nämlich das Leben des Kindes, hinter der das Geheimhaltungsinteresse der Mutter zurücktreten mußte. Die Offenbarung vom sozialpsychiatrischen Dienst an das Jugendamt erfolgte ebenfalls im Interesse des Kindes zur Klärung der Frage, ob und in welcher Form Hilfe benötigt werde, um einen eventuellen Wiederholungsversuch abzuwenden. § 8 Abs. 3 Kinder- und Jugendhilfegesetz (KJHG)[193] eröffnet die Möglichkeit der Beratung von Kindern und Jugendlichen ohne Kenntnis des Personensorgeberechtigten, wenn die Beratung aufgrund einer Not- und Konfliktlage erforderlich ist und solange durch die Mitteilung an den Personensorgeberechtigten der Beratungszweck vereitelt würde. Die Entlassung der Tochter gegen ärztlichen Rat ist zumindest als ein Indiz für das Vorliegen dieser Umstände zu werten.

Auch wenn man zu dem Ergebnis einer Verletzung der ärztlichen Schweigepflicht in diesem Fall gekommen wäre, so lägen die Voraussetzungen der Offenbarung im Notstand gem. § 34 StGB vor. Nach dieser Vorschrift handelt derjenige nicht rechtswidrig, der in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben etc. eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Da es hier um die Abwendung ernstlicher Gefahren für Leib und Leben der Tochter der Petentin ging, überwog im Rahmen der Interessenabwägung das Recht auf Offenbarung an das Jugendamt, um prüfen zu lassen, ob eine intensive Betreuung des Kindes geboten wäre.

7.3.2.4 Offenlegung personenbezogener Daten in einem Rechtsstreit vor einem Amtsgericht: Kein Ende des Datenschutzes nach dem Tod

In einem Rechtsstreit vor einem Amtsgericht hatte ich die Verwendung einer Liste über Krankenhausaufenthalte einer verstorbenen Patientin datenschutzrechtlich zu beurteilen. Der ärztliche Direktor des Krankenhauses hatte diese Liste zur Verfolgung seiner persönlichen Rechtsansprüche in einem Zivilrechtsstreit über die Nutzung einer ihm gehörenden

---

192 i. d. Fassung vom 10. März 1987, BGBl. I S. 945, ber. S. 1160

193 i. d. Fassung vom 3. Mai 1993, BGBl. I S. 637

Mietwohnung dem Gericht vorgelegt. Für die Übermittlung der Liste über Krankenhausaufenthalte der Verstorbenen kam als Rechtsgrundlage § 28 Abs. 2 Krankenhausgesetz i. V. m. § 16 Abs. 1 Buchst. c Bbg DSG in Betracht. Nach § 16 Abs. 1 Buchst. c Bbg DSG ist ein rechtliches Interesses des Auskunftsbegehrenden glaubhaft zu machen. Darüber hinaus darf kein Grund zu der Annahme bestehen, daß das Geheimhaltungsinteresse des Betroffenen (hier: verstorbene Patientin) überwiegen könnte. Ein solches rechtliches Interesse ist im Hinblick auf den Rechtsstreit vor dem Amtsgericht und der Tatsache, daß die Patientendaten zum Zwecke der Erwiderung auf einen Schriftsatz der Beklagten mit dem Ziel der Wahrung von Rechtsansprüchen vorgetragen wurde, zu bejahen. Der Zeitpunkt der Glaubhaftmachung ließ sich jedoch nicht mehr feststellen.

Unter der Voraussetzung, daß die Glaubhaftmachung des Interesses vor Auskunftserteilung und Übergabe der Auflistung gegenüber der Patientenverwaltung erfolgte, überwog im Rahmen der Interessenabwägung das Geheimhaltungsinteresse der verstorbenen Patientin das rechtliche Interesse an der Kenntnisnahme der zu übermittelnden Daten seitens des Klägers nicht, denn dem Gericht war bereits aus dem Schriftsatz der Beklagten deren langjähriger Krankenhausaufenthalt erkennbar.

Zur zukünftigen besseren Gewährleistung des Datenschutzes hat die Krankenhausleitung mit der Bereitschaft zur Bestellung eines krankenhausinternen Datenschutzbeauftragten sowie durch verstärkte Schulungsmaßnahmen für das Personal zur Umsetzung des Datenschutzes ein erstes Signal gesetzt.

7.3.3 Klinische Arzneimittelprüfung

Von einer Fachklinik wurde mir die Teilnahme an einer klinischen Arzneimittelprüfung angezeigt und dazu eine siebenseitige Patienteninformation und Einverständniserklärung zugesandt. Obwohl es sich bei dem Sponsor dieser Studie um eine renommierte Pharmafirma handelte und insofern Sachkenntnisse vorausgesetzt werden dürften, waren weite Teile dieses "einheitlichen Dokumentes" zu bemängeln. Die Nachbesserung erforderte einen längeren Briefwechsel, schließlich wurde zugesichert, daß auch auf eine Übermittlung der Initialen (Voraussetzung für eine vollständige Anonymisierung) verzichtet und die Anforderungen an eine Einwilligungserklärung (s. hierzu auch unter 6.2.2) akzeptiert würden.

Hellhörig wurde ich, als von einer Datenerfassung mittels Laptop die Rede war und sich schließlich auf Nachfrage herausstellte, daß der in Rede stehenden klinischen Arzneimittelprüfung ein - "wohl etabliertes" - DV-System zugrunde liegt, das es ermöglicht, die in den verschiedenen beteiligten europäischen Prüfzentren erfaßten Daten durch Fernübertragung an einen Zentralcomputer in London zeitunabhängig zu übermitteln, auf den nur Befugte eines speziell eingerichteten elektronischen Mitteilungssystems zugreifen können. Dabei können - entsprechend den Prüfrichtlinien der Good Clinical Practice Guidelines - die bei der Studie erfaßten Daten zwar in Papierform ausgedruckt werden, jedoch wird darauf verzichtet, wenn dazu nicht aufgrund von Anforderungen - beispielsweise seitens zentraler europäischer Zulassungsbehörden - kein Anlaß besteht. Im Routinefall werden die Daten nur noch dezentral ADV-mäßig zwischengespeichert und in gewissen Zeitabständen in der beschriebenen Weise übermittelt. Dieses veränderte technologische Umfeld bei klinischen Arzneimittelprüfungen hat gravierende Folgen für datenschutzrechtliche Prüfungen auf diesem Gebiet. Es wird deshalb auch im speziellen Fall noch zu klären sein, inwieweit die zugesagten Änderungen bei der Patienteninformation und der Einverständniserklärung auch mit einer Änderung des DV-Systems einhergehen.

8 Ernährung, Landwirtschaft und Forsten

8.1 Agrarförderung mittels InVeKoS

Zur Inanspruchnahme von Beihilfen (Agrarfördermittelanträge 1995) im Zusammenhang mit dem integrierten Verwaltungs- und Kontrollsystem (InVeKoS) der Europäischen Union müssen sich die Landwirte immer wieder durch umfangreiche Konvolute von Antragsformularen hindurcharbeiten, mit denen die für eine Leistungsbewilligung erforderlichen Angaben bei ihnen abgefragt werden. Um zumindest etwas Licht in das Dunkel der zahlreichen verwirrenden Regelungen zu bringen[194], ist es wichtig, durch eine den Bestimmungen der §§ 4 Abs. 2, 12 Abs. 3 Bbg DSG entsprechende Aufklärung in den Antragsformularen zumindest ein Minimum von Transparenz für den Antragsteller zu schaffen, so daß diesem wenigstens in etwa nachvollziehbar werden kann, welche Stellen am Ende zu welchen Zwecken über welche Angaben von ihm verfügen. Bei dem Versuch, dieses "Kunststück" zu verwirklichen, hat das Ministerium für Ernährung, Landwirtschaft und Forsten (MELF) auch in diesem Jahr wieder um meine Unterstützung gebeten und meine Empfehlungen gern berücksichtigt.

Zur Bearbeitung der Beihilfeanträge im InVeKoS setzt die Verwaltung das Programmsystem PROFIL ein. Zwischenzeitlich habe ich das ADV-System PROFIL.AMT exemplarisch bei zwei Landwirtschaftsämtern prüfen können. Dabei war insbesondere zu beanstanden, daß jeder berechtigte InVeKoS-Anwender sich seine Paßwörter der letzten 12 Monate für dieses Programm im Klartext anzeigen lassen konnte. Der Systemverwalter konnte dies sogar für alle Mitarbeiter erreichen. Paßwörter dürfen jedoch stets nur verschlüsselt gespeichert werden. Andernfalls wäre die Zugriffssicherheit des gesamten PC-Systems gefährdet. Das MELF hat zugesagt, die Software-Firma umgehend mit der erforderlichen Programmänderung zu beauftragen, so daß das Programmsystem den Landwirtschaftsämtern möglichst bald in einer neuen Version zur Verfügung gestellt werden kann. Im übrigen hat das MELF in Abstimmung sowohl mit dem Landesrechnungshof als auch mit mir eine Musterdienstanweisung für das Verfahren der Antragsbearbeitung bei den Landwirtschaftsämtern erstellt und den Landkreisen zur Übernahme empfohlen.

8.2 Umsetzung des Gesetzes zur Ausführung des Tierseuchengesetzes

Erneut hatte ich im Berichtszeitraum zu datenschutzrechtlich relevanten Verfahren und Vorhaben der Tierseuchenkasse (TSK) bei der Umsetzung des Gesetzes zur Ausführung des Tierseuchengesetzes (AGTierSGBbg)[195] Stellung zu nehmen[196]. Wie von mir empfohlen, fügt die TSK den als Postkarte konzipierten Vordrucken für die Meldungen der Tierhalter nach § 6 Abs. 2 Satz 3 AGTierSGBbg inzwischen zur besseren Gewährleistung des Datenschutzes einen voradressierten Umschlag für die Rücksendung bei, den ca. 90% der Tierhalter für ihre Tierbestandsmeldungen genutzt haben.

Des weiteren habe ich die Realisierung des ADV-Projekts der TSK geprüft; hierzu dauern die Beratungen mit dem Landesamt für Ernährung, Landwirtschaft und Flurneuordnung (LELF) noch an. Auch in diesem Fall wäre es von Vorteil gewesen, wenn das LELF zur Gestaltung seiner vertraglichen Beziehungen zu dem von ihm mit der Datenverarbeitung beauftragten Unternehmen auf ein Muster hätte zurückgreifen können, in dem die wesentlichen datenschutzrechtlichen Vertragselemente vorformuliert werden (s. hierzu auch unter 3.3).

8.3 Arbeitszeitanalyse in der Forstverwaltung

194

195 s. 2. Tätigkeitsbericht unter 9.1, S. 137 ff.

196 vom 2. März 1993, GVBl. I S. 58

s. 2. Tätigkeitsbericht unter 9.2, S.139 f.

Als gem. § 29 Abs. 1 Bbg DSG/§ 57 Abs. 4 LBG grundsätzlich datenschutzgerecht habe ich ein vom MELF zum Zweck der Personalplanung durchgeführtes automatisiertes Verfahren zur Arbeitszeitanalyse in der Forstverwaltung beurteilt. Mit ihm soll anhand entsprechender Angaben der Betroffenen in von ihnen quartalsweise zu führenden Erfassungsbögen sehr detailliert der bei den Ämtern für Forstwirtschaft auf die einzelnen Tätigkeiten entfallende Zeitbedarf ermittelt werden. Dabei kann wegen der tätigkeitsbedingten besonderen Gegebenheiten in der Forstverwaltung die Analyse in allen ihren Phasen zweckentsprechend zwar codiert, aber stellenbezogen - und dies bedeutet personenbeziehbar - durchgeführt werden. Während mir die vorgesehenen technischen Maßnahmen zur Datensicherung im wesentlichen ausreichend zu sein schienen, waren Unsicherheiten bezüglich der die Analyse anordnenden und regelnden Dienstanweisungen festzustellen, die nach Form und Inhalt auch unter datenschutzrechtlichen Gesichtspunkten nachbesserungsbedürftig waren. Ich erwarte eine Klärung der bislang offen gebliebenen Frage, wann die erhobenen Daten, die immerhin auch Angaben zu krankheits- und urlaubsbedingten Fehlzeiten enthalten, gelöscht oder vollständig anonymisiert werden.

9 Stadtentwicklung, Wohnen und Verkehr

9.1 Stadtentwicklung und Wohnen

9.1.1 Bekanntgabe erteilter Baugenehmigungen - Verfahren jetzt korrekt geregelt

In meinem letzten Tätigkeitsbericht[197] hatte ich ein Verfahren bemängelt, bei dem Bauaufsichtsämter einzelner Kreisverwaltungen Informationen über erteilte Baugenehmigungen an Baustellenverlage (Baustelleninformationsdienste) weitergaben. Der Mangel bestand darin, daß weder die nach § 4 Abs. 1 Bbg DSG erforderliche Rechtsgrundlage vorlag, noch ersatzweise die Einwilligung der betroffenen Bauherren eingeholt wurde.

Zwar enthält auch die unterdessen in Kraft getretene Brandenburgische Bauordnung (BbgBO)[198] als Spezialnorm keine bereichsspezifische Regelung für Datenübermittlungen im genannten Zusammenhang. Jedoch hat das Ministerium für Stadtentwicklung, Wohnen und Verkehr (MSWV) "aus diesem Grunde und um die angegebenen Schwierigkeiten zu vermeiden" die Bauaufsichtsämter in einem Runderlaß "Übermittlung von Angaben über Bauvorhaben an Dritte, insbesondere die Weitergabe an sog. Baustelleninformationsdienste"[199], auf die zu beachtenden Vorschriften nach dem Bbg DSG hingewiesen und ein rechtlich einwandfreies Verfahren entwickelt. Dabei ist insbesondere festgelegt worden, daß Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur weitergegeben werden dürfen, falls der Bauherr im Bauantrag ausdrücklich zugestimmt hat. Sofern der Bauherr in seinem Antrag dazu keine eindeutige Bestimmung getroffen hat, darf fiktiv hieraus nicht auf ein Einverständnis geschlossen werden. Ich begrüße es, daß die Landesregierung damit meiner Rechtsauffassung gefolgt ist.

9.1.2 Wohnungskarteien der ehemaligen DDR

Eigentlich dürften sie in ihrer ursprünglichen Form und in ihrem ursprünglichen Umfang überhaupt nicht mehr vorhanden sein - die Wohnungskarteien, die in der ehemaligen DDR bei den Gemeinden in der Regel im Bereich der Wohnraumlenkung zum Zweck der Wohnbestandsfortschreibung geführt und bis zum 31. Dezember 1989 regelmäßig aktualisiert wurden.

Zwar war mit dem Einigungsvertrag[200] die Fortgeltung des Gesetzes über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen (WoBelegG)[201] bestimmt worden und in § 3 dieses Gesetzes ausgeführt, daß im Rahmen der Belegungswirtschaft die in Frage kommenden Wohnungen - soweit nicht bereits Unterlagen vorhanden sind - zu erfassen, auf dem laufenden zu halten und ihr Inhalt im Datenspeicher Wohnungspolitik zu registrieren sind. Jedoch war der erforderliche Rahmen hinsichtlich der Art und des Umfangs der personenbezogenen Daten an dieser Stelle nicht konkret geregelt; entsprechende Regelungen fanden sich lediglich in der Anlage zur

---

197

198 s. 2. Tätigkeitsbericht unter 10.2, S. 142 f.

199 vom 1. Juli 1994, GVBl. I S. 126

200 Runderlaß des MSWV, Nr. 2/1993 vom 18. Oktober 1993

vom 31. August 1990, BGBl. II S. 889 in Anl. II, Kap. XIV,
201 Abschn. III

vom 22. Juli 1990, DDR-GBl. I S. 894

Durchführungsbestimmung[202] des genannten Gesetzes. Entgegen dem Gesetz selbst war diese untergesetzliche Bestimmung jedoch nicht mit dem Einigungsvertrag übergeleitet worden.

Insbesondere im Gesetz fehlte der entscheidende konkrete Hinweis auf eine berechtigte Fortnutzung noch vorhandener Datenbestände in den früheren Wohnungskarteien. Vermutlich hatten aus diesem Grund viele Gemeinden ihre Wohnungskarteien vernichtet, wenn dies nicht nach Wegfall des Aufgabenzwecks ordnungsgemäß bereits mit Ablauf der Wohnbestandsfortschreibung zum 31. Dezember 1989 geschehen war.

Eine nachträgliche Erweiterung des WoBelegG in § 3 Abs. 3[203], daß § 2 Wohnungsbindungsgesetz (WoBindG)[204] entsprechend anzuwenden ist, führte zu keiner Änderung der Rechtslage, da auch in diesem Zusammenhang keine gesetzliche Befugnis ableitbar ist, daß örtliche Wohnungsämter auch Datenbestände noch vorhandener Wohnungskarteien aus DDR-Zeiten nutzen dürfen oder gar zu nutzen haben.

Zusammenfassend ist festzustellen, daß weder unmittelbar nach Ablauf der Wohnbestandsbewirtschaftung in der ehemaligen DDR, noch zu einem späteren Zeitpunkt ein Recht oder gar eine Verpflichtung zur Fortnutzung der Datenbestände in den gemeindlichen Wohnungskarteien für die neuen Aufgabenzwecke materiell-rechtlich festgelegt wurde. Damit können die Daten, soweit sie für die Erfüllung der Aufgaben nach dem WoBelegG, das zum 31.12.1995 ausläuft, bzw. vom 01.01.1996 an nach dem WoBindG unbedingt erforderlich sind, nur noch im Rahmen der "Altdatenregelung" des § 34 Abs. 1 Bbg DSG genutzt werden[205].

Es wäre wünschenswert, wenn das MSWV den Gemeinden geeignete Empfehlungen für eine einheitliche Verfahrensgestaltung an die Hand gäbe. Dabei könnte in Betracht gezogen werden, die jetzt erforderlichen und insoweit zur Nutzung zulässigen Daten aus den alten Beständen herauszuziehen (dies ist nach dem WoBelegG für den Datenspeicher Wohnungspolitik ohnehin gefordert), die Wohnungskarteien in ihrer ursprünglichen Form insgesamt zu sperren und der Archivierung zuzuführen.

Vorsorglich muß ich aber an dieser Stelle darauf hinweisen, daß das WoBindG hinsichtlich der Beschreibung des Rahmens und des Umfangs der zu erhebenden bzw. zur Verfügung zu stellenden Daten in § 2 nicht hinreichend normenklar ist, so daß gem. § 41 Bbg DSG vom 20. Januar 1996 an jede Form der Datenverarbeitung unzulässig wäre, weil dann nicht mehr allein auf die Erforderlichkeit abgestellt werden darf (so unter 2.1).

9.1.3 Landeseinheitliches Wohngeldverfahren

Für die Wohngeldberechnung kommt in Brandenburg ein aus Nordrhein-Westfalen übernommenes zentrales Verfahren, das auf einem IBM-Großrechner im Landesamt für Datenverarbeitung und Statistik (LDS) in Potsdam für das gesamte Land abgearbeitet wird, zur Anwendung. Die ca. 60 im Land verteilten Wohngeldstellen nehmen die Anträge der Bürger entgegen und bearbeiten sie - abhängig von ihrem technischen Ausstattungsgrad - in unterschiedlicher Weise. Verfügt die Wohngeldstelle über eine eigene PC-Ausstattung, so übernimmt der zuständige Sachbearbeiter die Daten direkt auf Disketten, die im LDS

202

203 vom 27. Juli 1990, DDR-GBl. I S. 1262

204 durch Gesetz vom 6. Juni 1994, BGBl. I S. 1184
i. d. Fassung vom 19. August 1994, GBGl. I S. 2166, ber. S. 2319

205 s. 1. Tätigkeitsbericht unter 5.2.3, S. 17 ff.

weiterverarbeitet werden. Liegt keine entsprechende PC-Ausstattung vor, so übernimmt der Sachbearbeiter die Antragsdaten lediglich manuell in Eingabewertbögen, und die Datenerfassung wird zentral im LDS vorgenommen. In beiden Fällen können Disketten und Eingabewertbögen von den Wohngeldstellen zum LDS in Potsdam sowohl mit der Post als auch durch einen Kurier transportiert werden.

Nach mehreren Prüf- und Bearbeitungsschritten im LDS erfolgt die Berechnung und Zahlbarmachung des Wohngeldes. Die betreffenden Zahlungsanweisungen werden der Landeshauptkasse zur Ausführung übergeben. Im Rücklauf erhalten die dezentralen Wohngeldstellen die Bescheide für ihre Antragsteller zur weiteren Bearbeitung. Nachfragen und Beschwerden von Bürgern werden grundsätzlich dort behandelt. Ihre Bearbeitung bedingt allerdings häufige telefonische Rückfragen durch die zuständigen Sachbearbeiter bei der zentralen Wohngeldstelle.

Bei einer Besichtigung konnte ich mich davon überzeugen, daß im Rechenzentrum des LDS ein hoher Sicherheitsstandard herrscht. Die eigentlichen Schwachstellen des Verfahrens liegen auf den Transportwegen der Datenträger zwischen dem LDS und den Wohngeldstellen und in besonderem Maße im telefonischen Austausch von personenbezogenen Informationen zwischen den betreffenden Einrichtungen. So gingen beispielsweise unterwegs auch schon Disketten verloren und wurden dann, um die rechtzeitige Wohngeldzahlung zu sichern, durch Duplikate von der Wohngeldstelle ersetzt.

Ich habe deshalb dem LDS empfohlen, in das IT-Sicherheitskonzept für das Wohngeldverfahren auch alle Kommunikations- und Transportwege von und zu den Wohngeldstellen einzubeziehen. Ferner erscheint es mir im Interesse der Sicherheit des Gesamtverfahrens Wohngeld erforderlich, daß das LDS seine fachliche Kompetenz und seine Beratungsfunktion für die kommunalen Einrichtungen dazu nutzt, den Wohngeldstellen entsprechende Sicherheitskonzepte vorzuschlagen. Eine diesbezügliche Antwort durch das LDS und das MSWV - dem Auftraggeber des Wohngeldverfahrens - steht noch aus.

Weiterhin habe ich das LDS aufgefordert, für die Nutzer des telefonischen Auskunftssystems in den Wohngeldstellen geeignete organisatorische Verhaltensregelungen zu erarbeiten, die gewährleisten, daß ein Mißbrauch durch Unbefugte weitestgehend ausgeschlossen wird und daß für Dritte, selbst beim Mithören eines Telefongesprächs, über die Daten kein komplettes Bild zu einer bestimmten oder bestimmbaren Person entsteht. Vom LDS wurden unverzüglich entsprechende organisatorische Verhaltensregelungen für telefonische Anfragen bei der zentralen Wohngeldstelle erarbeitet und für alle Wohngeldstellen als verbindlich erklärt.

Ferner habe ich empfohlen, bis spätestens Januar 1996 die Voraussetzungen zu schaffen, daß alle Daten auf Disketten - unabhängig von der Versandform - in geeigneter Weise verschlüsselt werden (s. auch unter 1.3.5).

9.1.4 Neue technische Lösung

Zur Beschleunigung des Wohngeldverfahrens und zur Erhöhung der Verarbeitungssicherheit beabsichtigt das LDS, den Diskettentransport von den Wohngeldstellen weitestgehend durch einen Filetransfer über das Datex-P-Netz der Telekom zu ersetzen. Im Berichtszeitraum sollte eine Erprobung des Verfahrens mit der Wohngeldstelle Brandenburg erfolgen, und ich wurde um Prüfung und Stellungnahme gebeten. Dem dafür vorgelegten Sicherheitskonzept, das wesentlich aus der Einbindung der Sicherheitssoftware RACF in die Datenübermittlungssoftware besteht, habe ich unter der Voraussetzung zugestimmt, daß spätestens von 1997 an zusätzlich alle personenbezogenen Daten bei Übertragungen in öffentlichen Netzen verschlüsselt werden (s. unter 1.4.2).

9.1.5 Datenschutz in den Wohngeldstellen

Im Berichtszeitraum habe ich exemplarisch die Einhaltung der technisch-organisatorischen Datenschutzmaßnahmen in einer Wohngeldstelle überprüft. Die räumlichen Sicherungsmaßnahmen habe ich beanstandet. Die Wohngeldstelle befand sich in einer eingeschossigen Holzbaracke, in die bereits zweimal eingebrochen worden war. Aufgrund meiner Beanstandung reagierte der zuständige Landrat prompt und verlagerte die Bearbeitung der Wohngeldanträge in ein dafür geeigneteres Gebäude (s. unter 1.3.1.11).

Außerdem waren im Rahmen einer Fortbildungsveranstaltung des MSWV für Sachbearbeiter der Wohngeldstellen zahlreiche Fragen hinsichtlich datenschutzrechtlicher Probleme bei der praktischen Bearbeitung von Wohngeldanträgen beim Informationsaustausch mit Antragstellern oder Dritten sowie bei der Gestaltung des internen Postwegs aufgetaucht. Auch war die Frage zu klären, wie zu verfahren sei, wenn ein Antragsteller auf dem Antragsformular die obligatorische Bestätigung, ihm sei bekannt, daß die für die Berechnung zur Zahlung des Wohngeldes erforderlichen Daten im Wege der automatisierten Datenverarbeitung gespeichert und verarbeitet werden, durchstreicht.

Zunächst ist festzustellen, daß der Zweck des Wohngeldes in § 1 Wohngeldsondergesetz (WoGSoG)[206] weitergehend geregelt ist (Gewährung des Wohngeldes als Zuschuß nicht nur zu Aufwendungen für den Wohnraum, sondern zu den Kosten für Wärme und Warmwasser) als in § 1 Wohngeldgesetz (WoGG)[207], es sich aber auf jeden Fall im Kern um die Sozialleistung Wohngeld i. S. v. § 26 SGB I handelt (wenngleich an dieser Stelle nur auf die Bestimmungen des WoGG abgehoben wird).

Insoweit sind meine nachfolgenden Aussagen zum Schutz des Sozialgeheimnisses im Zusammenhang mit der Bearbeitung von Wohngeldangelegenheiten sowohl für den Geltungsbereich des WoGSoG (bis längstens 30. Juni 1995) als auch für den Geltungsbereich des bis spätestens danach anzuwendenden WoGG zutreffend. Sie greifen außerhalb der Wohngeldspezifischen Regelungen, aber auch in allen Bereichen, in denen "Sozialdaten" verarbeitet werden.

- Nach § 35 SGB I i. V. m. § 76 Abs. 1 SGB X ist sicherzustellen, daß persönliche oder sachliche Verhältnisse Verfahrensbetroffener im Zusammenhang mit der Wohngeldbearbeitung - und dazu zählt bereits die Tatsache, daß Wohngeld beantragt ist oder gewährt wird -nicht unbefugt übermittelt werden; d. h. eine Übermittlung ist nach §

---

206 i. d. Fassung vom 16. Dezember 1992, BGBl. I S. 2406, zul. geänd. durch Gesetz vom 29. Juli 1994, BGBl. I S. 1890

207 i. d. Fassung vom 1. Februar 1993, BGBl. I S. 183, zul. geänd. durch Gesetz vom 22. Dezember 1993, BGBl. I S. 2438

67 d Abs. 1 SGB X - und auch dann nur im erforderlichen Umfang und Rahmen - zulässig, wenn eine gesetzliche Übermittlungsbefugnis gem. §§ 68 - 77 SGB X oder nach einer anderen im Sozialgesetzbuch genannten Rechtsvorschrift vorliegt.

Bei telefonischen Auskünften kann nicht mit Sicherheit festgestellt werden, ob es sich bei dem Gesprächspartner wirklich um den jeweiligen Verfahrensbetroffenen handelt. Selbst Hinweise Anrufender auf die Wohngeldnummer, nähere Umstände, vereinbarte Erkennungszeichen usw. lassen letztlich keine eindeutige Identifizierung zu. Insoweit nicht zu verhindernde Verstöße gegen das Sozialgeheimnis in Einzelfällen würden jeweils einen Verstoß gegen die grundgesetzlich geschützten Persönlichkeitsrechte der Betroffenen darstellen und dürfen daher nicht billigend in Kauf genommen werden.

Somit müssen den Sachbearbeitern in den Wohngeldstellen Verfahrenswege vorgegeben werden, die sie gar nicht erst in die Gefahr bringen, auch ungewollt gegen das Sozialgeheimnis mit allen rechtlichen (auch evtl. dienst- oder arbeitsrechtlichen) Konsequenzen zu verstoßen. Dies wird bei vielen Wohngeldempfängern/Antragstellern auf Unverständnis stoßen, gleichwohl muß aus Rechtsgründen auf jede Form einzelfallbezogener Auskünfte und Informationen am Telefon verzichtet werden.

- Aus der Wohngeldnummer ist unmittelbar kein Personenbezug herzustellen, daher spricht auch nichts dagegen, die Wohngeldnummer auf die Aktendeckel der Wohngeldakten zu setzen. Dagegen würde durch den Zusatz persönlicher Daten - insbesondere des Namens der Betroffenen - ein unmittelbarer Personenbezug auf den Aktendeckeln hergestellt werden. Dies wäre nur insoweit zulässig, als die Akten während aller Bearbeitungsgänge der Inaugenscheinnahme unbefugter Dritter entzogen wären.

  Dies läßt sich erfahrungsgemäß regelmäßig nicht bewerkstelligen. In der Praxis wird sich nicht vermeiden lassen, daß noch zu bearbeitende Akten auf dem Tisch der Sachbearbeiter/-innen liegen, deren Aktendeckel zwangsläufig von anderen Antragstellern/Leistungsempfängern gelesen werden könnten. Daher sollte bei der Beschriftung der Aktendeckel auf jeden Personenbezug verzichtet werden.

- Nach § 14 WoGSoG bzw. § 25 WoGG sind auch sonstige Personen, die mit dem Antragsberechtigten Wohnraum gemeinsam bewohnen, verpflichtet, Angaben über ihre wirtschaftlichen Verhältnisse zu machen. Dabei muß dem insoweit Betroffenen selbstverständlich mitgeteilt werden, daß und in welchem Zusammenhang er seiner gesetzlichen Verpflichtung nachzukommen hat. Dabei wird es sich um eine zulässige Übermittlung i. S. v. § 35 SGB I i. V. m. § 67 d Abs. 1 2. Altern. SGB X handeln, soweit diesem lediglich zur Kenntnis gegeben wird, daß er von dem/der (Name) als gemeinsamer Bewohner des Wohnraums im Zusammenhang mit einem Antrag auf Wohngeld genannt worden sei.

  Weitere Informationen über die Antragsteller wie Alter, nähere Familienverhältnisse, Einkünfte usw. sind zur Begründung der Auskunftspflicht sonstiger Personen, die mit dem Antragsberechtigten Wohnraum gemeinsam bewohnen, nicht erforderlich. Deren Weitergabe würde einen Verstoß gegen das Sozialgeheimnis nach § 35 SGB I darstellen.

- Art und Weise der Auskunftserteilung an den Betroffenen über die zu seiner Person gespeicherten Sozialdaten sind nicht in § 18 Abs. 2 Brandenburgisches Datenschutzgesetz (Bbg DSG) geregelt, sondern bestimmen sich nach § 83 SGB X.

  Im Unterschied zu den für Sozialdaten nicht anwendbaren allgemeinen Regelungen im Bbg DSG setzt die spezialgesetzliche Regelung des SGB X nicht voraus, daß der Betroffene von der Tatsache der Speicherung seiner personenbezogenen Daten in einer automatisierten Datei - sozusagen "von Amts wegen" - schriftlich zu benachrichtigen sei. Gleichwohl bestimmt die speichernde Stelle nach § 83 Abs. 1 Satz 4 SGB X das

Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. So ist es durchaus begrüßenswert, daß den Antragstellern bei der Datenerhebung Hinweise auf die automatisierte Form der Datenverarbeitung im Zusammenhang mit der Berechnung und Zahlung des Wohngeldes gegeben werden.

Ungeachtet der Tatsache, daß ein Antragsteller auch von der besagten Textstelle Kenntnis nimmt, wenn - oder gerade weil - er sie im Antragsformular durchstreicht, ist die automatisierte Verarbeitung seiner Daten im genannten Zusammenhang nicht von seiner Zustimmung abhängig; insoweit kann eine Streichung keine Konsequenzen für die Antragsbearbeitung haben und wäre unbeachtlich. Auf keinen Fall könnte der Antragsteller - sofern er an seinem Antrag festhalten will - etwa eine individuelle manuelle Einzelbearbeitung verlangen.

- Nach § 35 SGB I ist im Rahmen des Schutzes des Sozialgeheimnisses auch innerhalb des Leistungsträgers sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind und nur durch diese weitergegeben werden. Dies hat die Konsequenz, daß auch die Korrespondenzen zwischen den zuständigen Bearbeitern in den Wohngeldstellen und den Wohngeldempfängern/Antragstellern unmittelbar erfolgen. So sollte durch interne Dienstanweisungen (zu denen die in § 35 SGB I genannten Stellen gem. § 78 Satz 1 SGB X verpflichtet sind) geschäftsordnungsmäßig festgelegt werden, daß

  a) Eingangspost, die offensichtlich für die Wohngeldstelle bestimmt ist, in der Poststelle nicht geöffnet, sondern mit Eingangsstempel auf dem Umschlag (evtl. auch auf Begleitzettel) versehen und direkt dem Wohngeldamt zugeleitet wird,

  b) Eingangspost, der erst nach Öffnung in der Poststelle zu entnehmen ist, daß sie für die Wohngeldstelle bestimmt ist, mit Eingangsstempel versehen, wieder verschlossen (2. Umschlag, verschließbare Postmappe o. ä.) und direkt dem Wohngeldamt zugeleitet wird,

  c) vom Wohngeldamt abgehende Post bereits dort verschlossen kuvertiert und in der Poststelle lediglich noch frankiert wird.

  Das Restrisiko nach b) könnte eingeschränkt werden, indem die Wohngeldstellen den Antragstellern empfehlen, bei Schriftwechsel im Anschriftenfeld auch ein Stellenzeichen (nicht die Wohngeldnummer oder das Aktenzeichen!) anzugeben. Allerdings sollte mit dem Stellenzeichen Außenstehenden kein Hinweis auf das Wohngeldamt und somit auf den Sachzusammenhang des Schriftwechsels gegeben werden (z. B. könnte dem jeweiligen Behördennamen lediglich ein numerisches Zeichen hinzugefügt werden, das grundsätzlich erst in der Poststelle der jeweiligen Behörde als Zuordnungsmerkmal erkannt wird). Im übrigen müßte geschäftsordnungsmäßig auch sichergestellt werden, daß die Wohngeldstellen selbst in ihren Absenderangaben (Stempeln oder sonstigen Aufdrucken auf Briefumschlägen) keine konkreten Hinweise bieten.

- Auch wenn gem. § 14 WoGSoG bzw. § 25 WoGG Vermieter auskunftspflichtig sind, sind sie dies nur, wenn und soweit es zur Durchführung des jeweiligen Gesetzes erforderlich ist. Da auch gegenüber dem Vermieter der Anfragegrund ggf. zur Begründung seiner Auskunftspflicht genannt werden muß, ist die Übermittlung der hierfür erforderlichen Daten gem. § 67 d Abs. 1 2. Altern. SGB X zulässig.

  Aus dem jeweiligen Zusatz "Wenn und soweit die Durchführung dieses Gesetzes es erfordert ..." ist jedoch zu schließen, daß die spezialgesetzliche Auskunftspflicht der Vermieter nicht uneingeschränkt gilt. Insoweit ist dem Grundsatz des § 67 a Abs. 2 Satz 1 SGB X Rechnung zu tragen, daß die Daten zunächst beim Betroffenen selbst zu erheben sind. Wenn hierzu z. B. der Antragsteller nicht Willens oder in der Lage ist, oder der begründete Verdacht besteht, daß dieser falsche Angaben macht bzw. gemacht hat, dürfen

die erforderlichen Informationen gem. § 14 WoGSoG bzw. § 25 WoGG unmittelbar beim Vermieter eingeholt werden, soweit durch sie die Durchführung der Maßnahme (hier: die Entscheidung über eine Bewilligung und ggf. über die Höhe des Wohngeldes) möglich ist. Insoweit schließt sich auch eine pauschale, vorsorgliche Anfrage bei Vermietern nach Mietschulden oder Mietrückständen aus.

- Eine Übermittlung von Sozialdaten, also auch von Informationen über persönliche und sachliche Verhältnisse im Zusammenhang mit der Wohngeldbearbeitung an andere Sozialleistungsträger ist in ihrem Umfang und Rahmen gem. § 69 Abs. 1 Ziff. 1 SGB X i. V. m. § 35 SGB I auch ohne konkrete Anfrage und Aufforderung insoweit möglich, als die Wohngeldstelle feststellt, daß diese Informationen für die (ordnungsgemäße) Erfüllung einer dortigen Sozialleistungsaufgabe erforderlich ist. Hierzu sind aufgrund der gleichen Bestimmung und im gleichen Rahmen und Umfang auch andere Sozialleistungsträger gegenüber den Wohngeldstellen (natürlich die Wohngeldstellen auch untereinander) berechtigt. Dies trifft umsomehr bei konkret begründeten Auskunftsersuchen zu.

  Eine Verpflichtung zur Auskunftserteilung ist sowohl den Bestimmungen des SGB X als auch den Bestimmungen des WoGSoG bzw. des WoGG nicht zu entnehmen. Immerhin trägt nach § 67 d Abs. 2 Satz 1 SGB X die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Datenübermittlung. Bei konkreten, begründeten Übermittlungsersuchen dürfte sich diese Verantwortlichkeit regelmäßig nicht negativ auf die Praxis auswirken, da die anfragende Stelle nach Satz 2 dieser Bestimmung zumindest verantwortlich ist für die Richtigkeit der Anfragedaten, so auch des angegebenen Rechtsgrundes hinsichtlich der Erforderlichkeit der erbetenen Daten.

9.2 Verkehr

9.2.1 Daten aus Fahrlehrer- und Fahrschuldateien

Im Zusammenhang mit der bevorstehenden Kommunalisierung des Fahrlehrerrechts auf die Kreise/kreisfreien Städte waren eine Fahrlehrer- und eine Fahrschulbestandsdatei vom Landesamt für Verkehr und Straßenbau Brandenburg (BLVS) erstellt und den Straßenverkehrsämtern übersandt worden.

Verständlicherweise hatten aus fachlicher Sicht auch der Fahrlehrerverband Land Brandenburg e. V. und die Technische Prüfstelle der DEKRA e. V. Interesse an diesen Listen bekundet. Ohne weiteren Verwaltungsaufwand hätte das MSWV diese Listen an diese beiden Stellen weiterleiten können, es vermutete jedoch datenschutzrechtliche Probleme und bat mich um Beurteilung der rechtlichen Möglichkeiten. Der vorliegende Fall steht für viele Vergleichsfälle und ist für eine exemplarische Darstellung besonders gut geeignet.

Bei beiden Listen handelte es sich um eine Sammlung personenbezogener Daten i. S. v. § 3 Abs. 1 i. V. m. Abs. 4 Nr. 3 Altern. 2 Bbg DSG. Der Personenbezug war auch für die Liste "Fahrschulen-Bestand" festzustellen, weil aus der Firmierung von Fahrschulen regelmäßig die "dahinterstehende" natürliche Person bestimmbar ist.

Nach § 4 Abs. 1 i. V. m. § 3 Abs. 2 Bbg DSG ist jede Form der Datenverarbeitung, also auch die Nutzung von zur Verfügung gestellten Daten davon abhängig, ob für die Bereitstellung eine spezielle materiell-rechtliche Befugnisnorm vorliegt oder die Betroffenen zuvor eingewilligt haben oder sich unmittelbar aus dem Bbg DSG eine Befugnisnorm ergibt. In diesem Zusammenhang hatte das MSWV zunächst zu überprüfen, ob es selbst einen Rechtsgrund zur eigenen Nutzung der Daten hatte, dazu mußte gem. § 13 Abs. 1 Bbg DSG die Nutzung der Daten zu eigenen Zwecken zumindest zur rechtmäßigen Aufgabenerfüllung erforderlich, d. h. zur Erfüllung einer gesetzlich zugewiesenen Aufgabe unabdingbar, sein. Erst danach war zu prüfen, ob auch eine Befugnisnorm zur Übermittlung an den Fahrlehrerverband Land Brandenburg e. V. bzw. die Technische Prüfstelle der DEKRA e. V. bestand.

Da es sich in beiden Fällen um private Unternehmen handelt, war vom MSWV nach § 16 Abs. 1 Bbg DSG unter gleichzeitiger Beachtung der Zweckbindungsregelung in § 13 Abs. 1 Bbg DSG zu prüfen, ob es zur Übermittlung gesetzlich berechtigt oder verpflichtet war. Anderenfalls hatte es zu prüfen, ob gem. § 16 Abs. 1 Buchst. b eine der Voraussetzungen nach § 13 Abs. 2 Buchst. b, d oder f Bbg DSG vorlag:

- Einwilligung des Betroffenen

- Erforderlichkeit zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person

- Entnahme der Daten aus allgemein zugänglichen Quellen (aber auch hier nicht gegen das Interesse der Betroffenen).

Eine weitere Möglichkeit zur Datenübermittlung hätte sich aus § 16 Abs. 1 Buchst. c Bbg DSG ergeben können, jedoch hätten sowohl Fahrlehrerverband als auch DEKRA nach meiner Einschätzung allenfalls ein berechtigtes, nicht aber ein rechtliches Interesse geltend machen können. Auch das Vorliegen eines öffentlichen Interesses nach Buchst. d konnte nicht festgestellt werden, so daß auf jeden Fall hätte sichergestellt werden müssen, daß die Betroffenen nicht widersprechen, sofern die Datenübermittlung mit dem berechtigten Interesse der beiden privaten Vereine oder mit der Entnahme aus öffentlichen Quellen hätte begründet werden sollen. Unter Beachtung von § 16 Abs. 2 Bbg DSG hätte dies aber nur

durch Einzelnachfrage bei den Betroffenen sichergestellt werden können, wobei vor einer Datenübermittlung an die beiden Unternehmen die Listen entsprechend den Widersprüchen hätten bereinigt werden müssen.

Wegen des hiermit verbundenen erheblichen Verwaltungsaufwandes hatte ich das MSWV auch auf das sog. Adreßmittlungsverfahren - eine andere Möglichkeit, dem Widerspruchsrecht Betroffener Rechnung zu tragen - hingewiesen. Bei diesem Verfahren tritt die öffentliche Stelle an die Betroffenen mit dem Wunsch der privaten Stelle auf Datenerhalt heran und stellt diesen frei, sich mit dem jeweiligen Unternehmen in Verbindung zu setzen. In diesem Fall würden sich die Betroffenen selbst und freiwillig gegenüber den Unternehmen offenbaren (s. unter 6.1.5).

Solche Verfahren sind - sofern sie nicht in irgendeiner Weise konditioniert sind - zwar datenschutzrechtlich einwandfrei, jedoch sind öffentliche Dienststellen - jedenfalls aus Datenschutzgründen - nicht verpflichtet, entsprechende - oft mit nicht unerheblichem Verwaltungsaufwand verbundene - Verfahren anzubieten. Das MSWV hatte sich jedenfalls entschlossen, die genannten Dateien nicht an den Fahrlehrerverband Land Brandenburg e. V. bzw. die DEKRA e. V. zu übermitteln.

9.2.2 (Wieder-)Erteilung von Fahrerlaubnissen

Eine Vielzahl von datenschutzrechtlichen Problemen beschäftigt die Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren im Zusammenhang mit der Erst- bzw. Wiedererteilung von Fahrerlaubnissen (Führerscheinen).

Da alle diesbezüglichen Maßnahmen sich überwiegend nach Bundesrecht auszurichten haben und insoweit die zuständigen Länderministerien verständlicherweise engen Kontakt zur Abstimmung möglichst einheitlicher Verfahrensregelungen halten, lassen sich datenschutzrechtlich einwandfreie Verfahren im Alleingang für das Land Brandenburg nur schwerlich durchsetzen. Gleichwohl konnte ich - wie einzelne nachfolgende Situationen zeigen - hier und da Übereinstimmung mit dem MSWV erreichen, oder das MSWV wurde von sich aus initiativ und sorgte durch Rundschreiben an die Führerscheinstellen des Landes für landeseinheitlich datenschutzgerechtere Bearbeitungsverfahren:

- Gem. § 2 Abs. 1 Satz 2 Straßenverkehrsgesetz (StVG)[208] ist eine Fahrerlaubnis zu erteilen, wenn nicht Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Antragsteller zum Führen von Kraftfahrzeugen ungeeignet ist. Gem. § 9 Straßenverkehrszulassungsordnung (StVZO)[209] ist die Führerscheinstelle befugt, bei anderen Dienststellen zu ermitteln, wenn ihr aufgrund der zur Ausstellung eines Führerscheines vorgelegten Unterlagen oder bei ihr bereits vorhandener Informationen Bedenken kommen, ob der Antragsteller die Voraussetzungen zur Ersterteilung einer Fahrerlaubnis gem. § 2 Abs. 1 Satz 2 StVG erfüllt: Daraus läßt sich allerdings keine Befugnis ableiten, bei jedem Antrag auf Ersterteilung einer Fahrerlaubnis bei den Polizeidienststellen nachzufragen, ob dort Eignungsbedenken bekannt sind. Zwar haben die Verwaltungsbehörden von Amts wegen zu ermitteln, ob bei den Antragstellern Eignungsbedenken zum Führen von Kraftfahrzeugen vorliegen. Das Verfahren zur Ermittlung der Eignung eines Antragstellers ist in zahlreichen Vorschriften der StVZO und des StVG geregelt. So ist zum Beispiel in § 9 a StVZO ein Sehtest vorgeschrieben; gem. § 2 StVG muß der Antragsteller im Rahmen der Prüfung Kenntnisse über die Gefahren, Lehre und über eine umweltbewußte Fahrweise (vgl. § 11 a StVZO) nachweisen; außerdem muß der Prüfling den Nachweis erbringen, daß er in der Lage ist, Unfallverletzte sachgemäß zu versorgen (Erste-Hilfe-Kurs). Zur

---

208

209 vom 19. Dezember 1952, BGBl. I S. 837
i. d. Fassung vom 28. September 1988, BGBl. I S. 1793

Ermittlung, ob der Antragsteller bereits nach dem StGB oder dem Ordnungswidrigkeitengesetz (OWiG)[210] im Zusammenhang mit der Teilnahme am Straßenverkehr in Erscheinung getreten ist, können die Verwaltungsbehörden auf das Verkehrszentralregister (vgl. § 30 Abs. 2 StVG) zugreifen.

Jedoch sind darüber hinausgehende Anfragen zur Eignungsfeststellung bei anderen Behörden im Wege der Amtshilfe grundsätzlich unverhältnismäßig und mit dem Gebot, die Daten grundsätzlich beim Betroffenen selbst zu erheben, nicht vereinbar. Nur wenn konkrete Anhaltspunkte vorliegen, die auf die Möglichkeit der Nichteignung hinweisen, können weitere Ermittlungsmaßnahmen gerechtfertigt sein.

Informationen über darüber hinausgehende Maßnahmen in anderen Bundesländern gaben mir Anlaß, das MSWV über seine Rechtsauffassung und über die Praxis im Land Brandenburg zu befragen. Mit Genugtuung konnte ich feststellen, daß der Ermittlungsauftrag nach § 9 StVZO in Brandenburg einheitlich eher restriktiv gesehen wird. Danach werden im Rahmen der Eignungsermittlung regelmäßig nur Anfragen an das Verkehrszentralregister in Flensburg gem. § 13 c StVZO gerichtet. Lediglich in Einzelfällen, sofern Anlaß zu der Annahme besteht, es könnten Eignungsmängel bestehen, fordert die Fahrerlaubnisbehörde gem. § 8 Abs. 3 StVZO ein Führungszeugnis und richtet eine Anfrage an die Polizeidienststellen. Eine regelmäßige Anforderung von Führungszeugnissen bzw. Anfragen an die Polizeidienststellen erfolgt im Land Brandenburg im Rahmen der Antragsbearbeitung nicht, unabhängig davon, welche Fahrerlaubnisklasse beantragt wurde. Gleichwohl kann es Schwierigkeiten bei der Beurteilung geben, in welchen Fällen Anlaß zur Annahme besteht, es könnten Eignungsmängel bestehen, die eine Anfrage bei Polizeidienststellen rechtfertigen. So gilt jedoch bei Anfragen zu laufenden Ermittlungsverfahren bis zu einer rechtskräftigen Verurteilung die auf dem Rechtsstaatsprinzip basierende Unschuldsvermutung mit der Konsequenz, daß die Nichteignung eines Fahrerlaubnisbewerbers nicht ausschließlich auf die Tatsache gestützt werden darf, daß gegen ihn ein Ermittlungsverfahren eingeleitet wurde. Dem entsprechen § 13 c StVZO und § 8 Abs. 3 StVG, wonach ausschließlich rechtskräftige Strafurteile (und damit keine Daten aus Ermittlungsverfahren) zur Frage der Eingungsfeststellung von Fahrerlaubnisbewerbern herangezogen werden dürfen. Jedenfalls ist feststellbar, daß zur Zeit klare, konkrete gesetzliche Vorgaben hinsichtlich der Mindestvoraussetzungen, die auch eine Ermittlung bei den Strafverfolgungsbehörden rechtfertigen, fehlen. Nur eine solche Vorschrift, mit der das "Wann", der "Übermittlungsweg" und der "Umfang" der erforderlichen Daten eindeutig definiert ist, könnte die notwendige Rechtssicherheit sowohl für die zuständigen Verkehrsbehörden, als auch für die betroffenen Bürger schaffen. Ich würde es begrüßen, wenn die Landesregierung für den Fall einer Novellierung der StVZO die Aufnahme weiterer konkretisierender Befugnisnormen für den Ermittlungsauftrag des § 9 StVZO unterstützen würde.

- Einen datenschutzrechtlichen Mangel sehe ich in der Verwaltungspraxis, daß bei der einer (Wieder-)Erteilung von Fahrerlaubnissen vorangestellten Eignungsprüfung strafrechtliche Verurteilungen verwertet werden, die im Bundeszentralregister (BZR) bereits gelöscht sind. Dieses Problem ist mit einigen Ausnahmen bundesweit feststellbar. Meine Bewertung entspricht der Beurteilung fast aller meiner Kolleginnen und Kollegen in den anderen Bundesländern. Der Wortlaut des § 52 Abs. 2 Bundeszentralregistergesetz (BZRG)[211] sieht eine Berücksichtigung früherer strafrechtlicher Verurteilungen vor in einem Verfahren, daß die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand

---

210

211 i. d. Fassung vom 19. Februar 1987, BGBl. I S. 602

i. d. Fassung vom 21. September 1984, BGBl. I S. 1229, ber. 1985, BGBl. I S. 195

hat, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister (VZR) einzutragen war. Damit ist das Verwertungsverbot gem. § 51 BZRG zeitlich unbegrenzt gelockert. Dies halte ich aus datenschutzrechtlicher Sicht zumindest dann für bedenklich, wenn es sich um Verurteilungen aus einem länger zurückliegenden Zeitraum (z. B. von zehn bis fünfzehn Jahren) handelt, und der Betroffene nur einmal verurteilt worden ist.

In seiner Stellungnahme weist das MSWV darauf hin, daß die Behörde aufgrund ihres gesetzlichen Ermittlungsauftrags nach § 9 StVZO zur Feststellung der Eignung eines Bewerbers auch eine umfassende Würdigung der Gesamtpersönlichkeit vorzunehmen habe. Je nach Art der Antragstellung (Ersterteilung/Erweiterung oder Neuerteilung einer Fahrerlaubnis) würden in Brandenburg zur Abklärung der charakterlichen Eignung grundsätzlich Auskünfte aus dem VZR und nur im Falle der Neuerteilung zusätzlich Auskünfte aus dem BZR eingeholt werden. Es verweist auf die Folge, daß somit nur bei Antragstellern, die eine Neuerteilung der Fahrerlaubnis begehren, meine vorgetragenen Bedenken regelmäßig zum Tragen kämen.

Dadurch reduziert sich das Problem zwar quantitativ, jedoch führt die grundsätzliche Haltung des MSWV nicht zu einer rechtlich einwandfreien Lösung, denn es wird zwar das grundsätzliche Verwertungsverbot hinsichtlich getilgter oder tilgungsreifer Eintragungen zum Nachteil des Betroffenen bestätigt, gleichzeitig aber darauf hingewiesen, daß dies nicht für Straftaten gelten könne, die sowohl im VZR als auch im BZR einzutragen sind. Diese seien grundsätzlich unbefristet für Verfahren zur Erteilung/Erweiterung, Neuerteilung oder Entziehung der Fahrerlaubnis im Rahmen des der Fahrerlaubnisbehörde obliegenden Ermessens und unter Beachtung des Grundsatzes der Verhältnismäßigkeit verwertbar. Das MSWV hält es im Interesse der Verkehrssicherheit für unverantwortlich, wenn es zu einer zeitlich befristeten Verwertung von Straftaten im genannten Zusammenhang käme.

Bereits seit vielen Jahren gibt es Ansätze, das Problem durch Ergänzung im BZRG zu lösen. Zuletzt weist ein Referentenentwurf für ein Gesetz zur Änderung des Straßenverkehrsgesetzes (Stand vom 10. August 1993) folgende Formulierung für § 52 Abs. 2 BZRG aus: "Abweichend von § 51 Abs. 1 darf eine frühere Tat ferner in einem Verfahren berücksichtigt werden, solange die Verurteilungen wegen dieser Tat nach den Vorschriften der §§ 28 bis 30 b des Straßenverkehrsgesetzes für das Verkehrszentralregister verwertet werden darf." Ich würde es begrüßen, wenn sich die brandenburgische Landesregierung bei der noch in dieser Legislaturperiode vorgesehenen Novellierung des BZRG dafür einsetzte, daß § 52 Abs. 2 in dieser Form geändert wird. Mit gleicher Intention ist der Bundesbeauftragte für den Datenschutz unterdessen an die Bundesministerien der Justiz und für Verkehr herangetreten.

- Nach § 9 StVZO hat die zuständige Verwaltungsbehörde auch zu ermitteln, ob Bedenken gegen die Eignung des Antragstellers zum Führen von Kraftfahrzeugen vorliegen ("z. B. ... , ferner Bedenken gegen die körperliche oder geistige Eignung"). Hierin liegt zwar ein Ermittlungsauftrag, jedoch ist die Form der zu führenden Ermittlungen lediglich in § 8 Abs. 3 StVZO (Anforderung eines Führungszeugnisses) und in § 13 c StVZO (Anforderung einer Auskunft aus dem VZR) geregelt. Eine Regelung, in welcher Weise der Gesundheitszustand eines Antragstellers ermittelt werden könnte, um insoweit in geeigneter Weise eventuelle Bedenken gegen die körperliche oder geistige Eignung ermitteln zu können, ist der StVZO nicht zu entnehmen. Zwar war bereits 1973 seitens der Bundesländer überlegt worden, wie eine möglichst frühzeitige Erkennung alters-/oder krankheitsbedingter Eignungsmängel erfolgen könnte, jedoch blieb die beabsichtigte Ergänzung des § 8 Abs. 2 Nr. 3 StVZO mit der Pflicht zur Vorlage eines Gesundheitsfragebogens aus. Gleichwohl war im Land Brandenburg ein Fragebogen zur Anwendung gekommen, der den damaligen Intentionen weitgehend folgte.

  In einem Rundschreiben vom 15. Februar 1995 hat nun das MSWV alle

Führerscheinstellen der Straßenverkehrsämter der Kreise/kreisfreien Städte des Landes gebeten, den Gesundheitsfragebogen nicht mehr zu verwenden, weil Zweifel bestehen, ob der Fragebogen vom geltenden Recht abgedeckt ist. Ich begrüße diesen Schritt und teile sämtliche Begründungspunkte hierzu, wenngleich ich bemerken muß, daß diese Begründungen gerade keinen Zweifel daran lassen, daß die Verwendung des Vordrucks "Angaben über den Gesundheitszustand" datenschutzrechtlich unzulässig war.

Nach § 2 StVG ist die Fahrerlaubnis zu erteilen, wenn der Bewerber seine Befähigung durch eine Prüfung dargelegt hat. Ausgenommen hiervon ist nur der Fall, daß Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Bewerber zum Führen von Kraftfahrzeugen ungeeignet ist. Das bedeutet, daß das Gesetz von der Eignungsvermutung des Bewerbers ausgeht. Durch die Verwendung eines Gesundheitsfragebogens wird jedoch - ungeachtet der Tatsache, daß eine gesetzliche Regelung hierfür nicht vorhanden ist - die grundsätzliche Eignung nicht mehr als vorgegeben anerkannt. Die Behörde versucht vielmehr ihr noch nicht bekannte Tatsachen zu ergründen, wozu die rechtliche Grundlage fehlt.

Zwar ist es zulässig, gem. § 4 Abs. 1 Buchst. b i. V. m. § 12 Abs. 3 Bbg DSG den Fahrerlaubnisbewerber über Krankheiten zu befragen, dessen Angaben aufzunehmen sowie eventuell bekannten körperlichen oder geistigen Mängeln des Bewerbers nachzugehen, jedoch wäre der Bewerber, da keine Auskunftspflicht besteht, auf die Freiwilligkeit seiner Angaben hinzuweisen. Aufgrund einer diesbezüglichen Weigerung dürfte die Fahrerlaubniserteilung jedoch nicht abgelehnt werden, weil dies rechtlich nur dann zulässig wäre, wenn der Verwaltungsbehörde Tatsachen vorliegen, die die Annahme der Ungeeignetheit rechtfertigen. Die Weigerung allein, über eventuelle Krankheiten Auskunft zu geben, ist keine auf eine Ungeeignetheit schließende Tatsache, weil sie keinen Schluß zuläßt, der Bewerber leide an einer die Eignung als Kraftfahrzeugführer ausschließenden körperlichen oder geistigen Krankheit. Die Auskunftsverweigerung kann auch nicht Anlaß für eine von der Verwaltungsbehörde anzuordnende amtsärztliche Untersuchung sein. Eine derartige Maßnahme ist nur gerechtfertigt, wenn die örtlich zuständige Behörde Tatsachen ermittelt, die Bedenken gegen die Eignung begründet. Vermutungen, die durch keine konkreten Anhaltspunkte gedeckt sind, können nicht als "Tatsachen" im Sinne des § 12 StVZO gelten, die die Maßnahme nach Abs. 1 dieser Bestimmung rechtfertigen könnten. Zweifel an der Eignung des Bewerbers genügen nicht zur Verweigerung der Fahrerlaubniserteilung.

- Im Zusammenhang mit der Wiedererlangung der Fahrerlaubnis war mir von einem Petenten die Kopie eines Antragsvordrucks zur datenschutzrechtlichen Bewertung übersandt worden. Dieser Vordruck sah u. a. auch eine Spalte vor, mit der eine Stellungnahme der Gemeinde/Verwaltungsgemeinschaft hinsichtlich möglicher Bedenken gegen die Eignung des Antragstellers zum Führen von Kraftfahrzeugen angefordert werden konnte. Dabei war insbesondere aufgefordert, Hinweise auf die nach § 9 StVZO aufgeführten Versagungsgründe (z. B. schwere oder wiederholte Vergehen gegen Strafgesetze, Neigung zum Trunk, zur Rauschgiftsucht oder zu Ausschreitungen, insbesondere Rohheitsvergehen, ferner Bedenken gegen die körperliche oder geistige Eignung) zu geben. Gegenüber dem MSWV wies ich darauf hin, daß es nicht einmal erkennbar sei, inwieweit eine Anfrage bei der Gemeinde bereits sachlich geeignet sein sollte, dem unter § 9 StVZO geregelten Ermittlungsauftrag der Führerscheinstelle nachkommen zu können, da die erforderlichen Angaben originär nur im Polizeibereich, im Verkehrszentralregister und im ärztlichen Bereich im Rahmen dortiger Zuständigkeit anfallen bzw. erstellt werden können, und allenfalls von dort abgefragt werden dürfen. Insoweit wäre aber auch jede Übermittlung von Angaben im Rahmen von § 9 StVZO durch die zuständige Gemeinde datenschutzrechtlich unzulässig, weil sie zum einen interne Abgrenzungen im Rahmen des funktionalen Behördenbegriffs beachten müßte und zum anderen gem. § 13 Bbg DSG nur über Daten verfügen und diese gem. § 14 Bbg DSG nur übermitteln dürfte, wenn und soweit dies zur jeweiligen rechtmäßigen Aufgabenerfüllung

erforderlich wäre. Ein zusätzliches datenschutzrechtliches Problem sah ich darin, daß zum einen die angefragte Gemeinde/Verwaltungsgemeinschaft kaum Kenntnis über die angeforderten Versagungsgründe haben könnte, ohne selbst eine Verletzung datenschutzrechtlicher Bestimmungen begangen zu haben, zum anderen dürften solche Erkenntnisse, selbst wenn sie vorlägen, nicht weitergeleitet werden.

In seiner Stellungnahme wies das MSWV darauf hin, daß der übersandte Vordruck zwar von einer Mehrzahl der Kreise und kreisfreien Städte Brandenburgs verwendet wird, im übrigen nur noch ein von drei weiteren verwendeten Vordrucken anderer Verlage ein entsprechendes Anfragefeld vorgesehen hat. Beruhigend war bereits die Feststellung, daß trotz der bestehenden Möglichkeit das beanstandete Feld von vierzehn Kreisen nicht genutzt wird. Begrüßt habe ich die Bestätigung des MSWV, daß es meine Rechtsauffassung in vollem Umfang teilt und deshalb die Kreise und kreisfreien Städte angewiesen habe, die Nutzung dieses Feldes zu unterlassen und die erforderlichen Stellen entsprechend zu informieren. Ich begrüße auch die Zusage, sich mit den in Frage kommenden Verlagsgesellschaften zu beraten, inwieweit eine Streichung des bemängelten Feldes möglich ist. Hier werden allerdings unterstützende Initiativen auch in anderen neuen Bundesländern zweckdienlich, wenn nicht sogar erforderlich sein, da dort z. T. gleiche Vordrucke verwendet werden.

9.2.3 Halterauskunft auch bei Falschparken auf privater Verkehrsfläche

Vermutlich werden sich einige Bürger mehr "Unterstützung vom Datenschutz" erhofft haben, als sie sich mit folgendem Problem an mich wandten: Nachdem eine private Wohnungsbaugesellschaft festgestellt hatte, daß es vor einem ihrer Häuserkomplexe wiederholt zu "undisziplinierten Parkverhalten" von ortsansässigen Bürgern gekommen war, bei dem Grünflächen und Gehwege mit Fahrzeugen zerfahren und zugestellt worden waren, hatte sie sich unter Nennung der Kfz-Kennzeichen an die Straßenverkehrsbehörde des zuständigen Landkreises mit der Bitte gewandt, Auskünfte über Namen und Anschriften der jeweiligen Kfz-Halter zu erteilen. Dieser Bitte war die Straßenverkehrsbehörde in den genannten Einzelfällen nachgekommen. Die Petenten hatten aber Zweifel, ob diese Datenübermittlung an Private zulässig war.

In dem konkreten Einzelfall konnte die Straßenverkehrsbehörde hinreichend darlegen, daß die Voraussetzungen für eine Auskunftserteilung an die Wohnungsbaugesellschaft sowohl dem Grund als auch dem Umfang nach gerechtfertigt war. Die Wohnungsbaugesellschaft erbat die Auskünfte, weil sie die bereits geschilderten Umstände nicht "länger dulden" und die betreffenden Bürger anschreiben wollte.

Hiermit lag für die Straßenverkehrsbehörde die Voraussetzung für eine Auskunftserteilung nach § 39 Abs. 1 StVG vor, insoweit die Fahrzeug- und Halterdaten zumindest "zur ... Befriedigung ... von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr ... benötigt" wurden (einfache Registerauskunft). Rechtfertigend wies sie darauf hin, es handele sich um Flächen, die einem unbestimmten, nicht durch persönliche Beziehungen verbundenen Personenkreis zur Benutzung offenständen, womit insoweit dort öffentlicher Verkehr stattfände, auch wenn die Gehweg- und Grünflächen Privatgelände der Wohnungsbaugesellschaft seien.

Tatsächlich wird die Eigenschaft einer reinen Privatfläche oder einer "privaten Straßenfläche mit öffentlichem Verkehr" ausschließlich durch die tatsächliche Nutzbarkeit bestimmt. Wenn diese Flächen wie oben beschrieben ohne faktische Sperren zugänglich sind, findet "tatsächlich öffentlicher Verkehr" im Sinne und nach den Bestimmungen des Straßenverkehrsrecht statt. Damit war auch das Kriterium des § 39 Abs. 1 StVG "... im Zusammenhang mit der Teilnahme am Straßenverkehr ..." als weitere Voraussetzung für eine Auskunftserteilung gegeben. Da die Bestimmungen des StVG als Spezialnorm den allgemeinen Bestimmungen des Bbg DSG vorangehen, konnte ich vor dem rechtlichen und

tatsächlichen Hintergrund der Angelegenheit keinen datenschutzrechtlichen Mangel feststellen.

9.2.4 Übersendung von Beweisfotos bei Verkehrsverstößen

In mehreren Fällen war Haltern "geblitzter" Kraftfahrtzeuge im Rahmen der ordnungsbehördlichen Ermittlungen nach §§ 55, 56 Ordnungswidrigkeitengesetz (OWiG)[212] bereits mit den ersten Anhörungsbögen Abzüge der Beweisfotos übersandt worden. In einem Fall hatte die Ehefrau des Fahrers (Halterin des Fahrzeuges) auf dem Foto eine andere weibliche Person erkannt, was zu nicht unerheblichen familiären Problemen führte. In einem anderen Fall war Halterin des Kfz eine Behörde, in deren dienstlichem Auftrag der betroffene Mitarbeiter das Fahrzeug zur Tatzeit geführt hatte. Beim Öffnen der Post in der Poststelle und ihrer Weiterleitung im üblichen Geschäftsgang der Verwaltung war der Vorfall in der Dienststelle einer Vielzahl von Personen bekannt geworden, was zu gesellschaftlichen und beruflichen Problemen führte.

In beiden Fällen lagen die Voraussetzungen für eine Übermittlung der Beweisfotos an die Halter gem. § 23 Nr. 2 Buchst. c Ordnungsbehördengesetz (OBG)[213] i. V. m. § 43 Abs. 3 Nr. 1 Satz 2 Polizeiaufgabengesetz (PAG)[214] nicht vor. Danach hätte die Übersendung der Beweisfotos (Datenübermittlung) zur Erfüllung der Aufgaben der Ordnungsbehörde erforderlich sein müssen; das war jedoch nicht der Fall. Vielmehr hätte die jeweilige Ordnungswidrigkeit in beiden Fällen verfahrensökonomisch und effektiv auch auf andere, für die Betroffenen weniger belastende Weise verfolgt werden können.

Das Ministerium des Innern hat dies inzwischen grundsätzlich eingeräumt und mir mitgeteilt, es beabsichtige eine Regelung, nach der andere Personen als der Fahrer des Kfz auf den Beweisfotos unkenntlich gemacht werden müssen. Außerdem soll vor einer Übersendung der Aufnahmen eine Plausibilitätskontrolle durchgeführt werden, durch die ausgeschlossen werden soll, daß das Beweismittel dem Anhörungsbogen auch in den Fällen beigefügt wird, in denen der Halter - z. B. wegen Geschlechtsverschiedenheit oder weil es sich um eine juristische Person handelt - als Fahrer nicht in Frage kommen kann.

Diese Lösungsvorschläge halte ich für rechtlich geboten und für grundsätzlich geeignet, eine datenschutzgerechte Praxis herbeizuführen, mit der sich im übrigen äußerst prekäre Situationen für die Betroffenen auf ein unvermeidbares Maß reduzieren lassen. Nicht nur unter verhältnismäßiger Berücksichtigung des öffentlichen Interesses an einer ökonomischen und effektiven Durchführung des Bußgeldverfahrens, sondern auch im Hinblick auf die Interessenlage, die im Regelfall bei den Haltern bestehen dürfte, scheint mir dagegen ein vollständiger Verzicht darauf nicht geboten zu sein, dem Halter das Beweisfoto schon bei der Erhebung des Tatvorwurfs zu übersenden, zu dem er sich in dem Anhörungsbogen äußern soll.

10 Finanzen und Wirtschaft

10.1 Steuernummern von Mitgliedern der IHK

In einer Eingabe machte mich der Petent darauf aufmerksam, daß er mittels

---

212

213 i. d. Fassung vom 19. Februar 1987, BGBl. I S. 602

214 vom 13. Dezember 1991, GVBl. S. 636, zul. geänd. d. Gesetz v. 30. Juni 1994, GVBl. I S. 230

vom 11. Dezember 1991, GVBl. S. 636

Erhebungsvordrucks von einer der Industrie- und Handelskammern (IHK) des Landes aufgefordert worden sei, im Zusammenhang mit der Bemessung der Mitgliedsbeiträge an die Kammer u. a. "unbedingt" auch die Gewerbe-Steuernummer anzugeben.

Die IHK stützte ihre Maßnahme auf § 9 Abs. 2 IHK-Gesetz (IHK-G)[215] und betont, daß die Bemessungsgrundlage eindeutig nur über die Steuernummer beim zuständigen Finanzamt erfragt werden könne. Ansonsten könnte bei nicht eindeutiger Zuordnung für eine Vielzahl von Kammerzugehörigen eine falsche Beitragserhebung nicht ausgeschlossen werden. Sie nannte hierzu viele Beispiele, in denen in der Vergangenheit in den Alt-Bundesländern nur über die Steuernummer die Bemessungsgrundlage beim zuständigen Finanzamt erfragt werden konnte.

Auch wenn zugestanden werden muß, daß die Verwendung der Steuernummer dem Zweck der korrekten Bemessung der Mitgliedsbeiträge nach § 9 Abs. 2 IHK-G dient und geeignet ist, Verwechslungen auszuschließen, kann hieraus eine Befugnisnorm, die die IHK-Mitglieder verpflichten könnte, die Gewerbe-Steuernummer zu nennen, nicht abgeleitet werden. Die Befugnisse zu der insoweit erforderlichen Datenerhebung sind i. S. v. § 4 Abs. 1 Buchst. a i. V. m. § 12 Abs. 1 Satz 1 Bbg DSG spezialgesetzlich und damit abschließend im IHK-G geregelt. Eine Befugnis zur Erhebung auch der Gewerbe-Steuernummern ist aber weder in § 9 IHK-G noch an anderer Stelle dieses Gesetzes normiert. Allerdings ist - wenn auch möglicherweise etwas aufwendig - rechtlich zulässig und für den Aufgabenzweck in gleicher Weise geeignet das Verfahren nach § 3 Abs. 3 Satz 5 2. Halbsatz IHK-G. Danach kann die IHK die erforderliche Steuernummer durch Einsichtnahme in die Geschäftsunterlagen feststellen, wenn ihre Anfrage ohne Steuernummer bei den Finanzbehörden keinen Erfolg gehabt haben sollte.

Die IHK ist schließlich meinem Rat gefolgt, gem. § 4 Abs. 1 Buchst. b i. V. m. § 12 Abs. 3 Bbg DSG auf die Freiwilligkeit der Betroffenen abzustellen. In einem abgeänderten Fragebogen werden die Betroffenen jetzt ordnungsgemäß über den Verwendungszweck und die Tatsache aufgeklärt, daß die Angabe der Gewerbe-Steuernummer freiwillig ist, ansonsten aber die IHK gem. § 3 Abs. 3 IHK-G berechtig ist, erforderlichenfalls die zur Festsetzung der Beiträge erforderlichen Geschäftsunterlagen einsehen.

Ich gehe davon aus, daß die Angelegenheit auch für die anderen IHK und deren Mitglieder in unserem Land von Bedeutung ist. Falls nicht bereits geschehen, sollten sie die entsprechenden Verfahren an die datenschutzrechtlichen Erfordernisse angleichen.

10.2 Mißtrauen verpflichtet nicht zur Vorlage von Führungszeugnissen Spielhallenbediensteter

Als örtlich zuständige Ordnungsbehörde hatte ein Amt den Betreiber einer Spielhalle unter Fristsetzung aufgefordert, gem. § 4 der Verordnung zur Ausführung des Gaststättengesetzes (GastVO)[216] von jeder in seinem Betrieb beschäftigten Person ein Führungszeugnis zu übersenden. Bei zukünftigen Neueinstellungen sollte er das Führungszeugnis der betreffenden Person auch ohne besondere Aufforderung von sich aus dem Amt übergeben. Den Zweck und die Erforderlichkeit für diese Maßnahme begründete das Amt auf Anfrage mit dem Hinweis, daß es mit der Anforderung eines Führungszeugnisses für Beschäftigte in Gaststätten evtl. strafbaren Handlungen vorbeugen wollte. Nicht ohne Grund bezweifelte der

---

215 vom 18. Dezember 1956, BGBl. I S. 920, zul. geänd. durch Gesetz vom 23. November 1994, BGBl. I S. 3475

216 vom 20. Oktober 1992, GVBl. II S. 60

Spielhallenbetreiber die Rechtmäßigkeit der behördlichen Aufforderung.

Aus § 4 GastVO, auf das das Amt seine Forderung stützte, ist lediglich ersichtlich, daß der Betreiber u. U. zur Anzeige seiner Beschäftigten verpflichtet werden kann bei gleichzeitiger Nennung bestimmter personenbezogener Daten wie Vor- und Zunamen, Geburtsdatum, Geburtsort, letzter Aufenthaltsort, letzte Beschäftigungsstelle und Beginn der Beschäftigung. Der Umfang der Datenerhebung ist an dieser Stelle abschließend geregelt. Eine Verpflichtung zur Übermittlung weiterer Fremddaten, auch von Führungszeugnissen, ist aus dieser Rechtsgrundlage nicht ableitbar. Im übrigen setzen die besonderen Rechte von Behörden auf Auskunft aus dem Bundeszentralregister nach § 30 oder § 31 Bundeszentralregistergesetz (BZRG)[217] andere Sachverhalte voraus, sind ggf. von den Behörden selbst einzuholen und mußten insoweit für den vorliegenden Fall irrelevant sein.

Zwar gab das Amt vor, mit der Anforderung eines Führungszeugnisses für Beschäftigte in Gaststätten evtl. strafbaren Handlungen vorbeugen zu wollen, jedoch sind - soweit Strafverfolgungsmaßnahmen erforderlich werden - diese ausschließlich von Strafverfolgungsbehörden aufgrund dort geltender spezialgesetzlicher Regelungen durchzuführen. Ansonsten bleiben der örtlich zuständigen Ordnungsbehörde ausschließlich die in § 4 der GastVO festgelegten Möglichkeiten gegenüber dem Gewerbetreibenden. Dieser Rechtsauffassung konnte das Amt nicht widersprechen.

Aus den genannten Rechtsgründen habe ich die Forderung an den Spielhallenbetreiber bemängelt, jedoch von einer förmlichen Beanstandung gem. § 25 Bbg DSG abgesehen, nachdem das Amt zu einem frühen Zeitpunkt in einem persönlichen Gespräch mit dem Petenten von dieser Forderung abgerückt war und es uns schriftlich bestätigt hatte, daß entsprechende Forderungen nicht dort gängiger Praxis entsprächen und es zukünftig datenschutzgerechte Verfahren anstreben würde.

10.3 Weitere Hinweise zum Betrieb digitaler Telekommunikationsanlagen

Bereits im 2. Tätigkeitsbericht[218] hatte ich meinen Standpunkt zum Betrieb von digitalen Telekommunikationsanlagen ausführlich dargelegt. Dabei bildeten einige aus der Sicht des Datenschutzes besonders kritische Leistungsmerkmale und Fragen der Gebührenabrechnung den Schwerpunkt. Ferner berichtete ich bereits dort[219] über den Erlaß einer allgemeinen Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg (Dienstanschlußvorschrift - DAV)[220] des Ministeriums der Finanzen und über eine Dienstvereinbarung über die Nutzung der ISDN-Telekommunikationsanlage des Telekommunikationsverbundes, die als Muster für die obersten Landesbehörden des Landes Brandenburg dienen sollte. Zu meinem Bedauern bleiben einige Einrichtungen aus nicht erkennbaren Gründen in wesentlichen datenschutzrelevanten Punkten in ihren Dienstvereinbarungen dahinter zurück. In Zukunft werde ich derartige Abweichungen beanstanden.

---

217 i. d. Fassung vom 21. September 1984, BGBl. I S. 1229, ber. 1985, BGBl. I S. 195

218 s. unter 1.4.1, S. 21 ff.

219 s. 2. Tätigkeitsbericht unter 11.1, S. 143 ff.

220 vom 30. November 1993, ABl. 1993, S. 1775

In Ergänzung zu meinen Ausführungen im 2. Tätigkeitsbericht sollen hier noch einige Hinweise zum Umgang mit den Verbindungsdaten in internen Telekommunikationsanlagen gegeben werden:

- Zu den Verbindungsdaten gehören Angaben darüber, wer wann mit wem wie lange in welcher Form kommuniziert hat. Diese Verbindungsdaten werden ebenso wie die Inhaltsdaten von Kommunikationsdiensten durch das Fernmeldegeheimnis geschützt und ihre Speicherung ist deshalb nur in wenigen in Ziff. 3.1.3 der DAV festgelegten Fällen zulässig.

- Für die Abrechnung und Kostenkontrolle von dienstlichen Gesprächen können monatlich Gesamtgebühren, ggf. aufgeteilt nach einzelnen Ressorts oder Kostenstellen, ermittelt werden. Eine komplette Aufzeichnung der Verbindungsdaten aller abgehenden Dienstgespräche ist dafür nicht erforderlich und abzulehnen.

- Für die Abrechnung von Privatgesprächen sollte für jeden Nutzer ein Wahlrecht darüber bestehen, ob alle Verbindungsdaten mit der um mindestens drei Ziffern verkürzten Zielrufnummer oder nur die Gesamtgebühren gespeichert werden.

- Um eine mißbräuchliche Nutzung der dienstlichen Fernsprecheinrichtungen zu unterbinden und ihre kostenbewußte Inanspruchnahme zu fördern, dürfen die Verbindungsdaten dienstlicher Gespräche nur in einem sehr begrenzten Umfang stichprobenartig aufgezeichnet werden. Dabei sind die Stichproben bereits vor Beginn des Abrechnungszeitraumes möglichst durch ein automatisiertes Zufallsprinzip konkret festzulegen. Die vorbeugende Aufzeichnung der Verbindungsdaten aller abgehenden Gespräche und eine anschließende Auswahl der Stichproben daraus ist abzulehnen.

11 Aus der eigenen Behörde

In den letzten Jahren erreichten mich nur verhältnismäßig wenig Bürgereingaben (25 Prozent aller schriftlichen Vorgänge). Dies veranlaßte mich, über die bisherige übliche Presse- und Informationsarbeit hinaus nach Mitteln zu suchen, die einerseits attraktiv genug wären, den Bekanntheitsgrad meiner Behörde zu fördern, zum anderen aber geeignet wären, weitgestreut die Bürger zu ermutigen, ihre unmittelbaren Rechte gegenüber den Verwaltungen insbesondere auf Auskunft- und Akteneinsicht zu nutzen. Diesem Zweck diente bereits die Veröffentlichung von "Tips zum Adressenhandel"[221]. Aber erst mit dem sog. "Datenscheckheft"[222] konnte ein entscheidender Schritt in diese Richtung getan werden; ob - trotz der bereits in den ersten drei Monaten des Jahres 1995 verteilten ca. 10.000 Exemplare - der Durchbruch gelungen ist, wird allerdings erst in einiger Zeit beurteilt werden können.

Spürbar ist seit Verteilung der Broschüre in den letzten drei Monaten die Zahl der Eingaben im Vergleich zu den ersten neun Monaten des Berichtszeitraums um 60 Prozent gestiegen. Dabei ist gleichzeitig auch eine Qualitätssteigerung zu beobachten, weil diesen Eingaben schon erste Kontakte der Petenten mit den Verwaltungen zugrundeliegen und mir nur dann

---

221 Broschüre "Tips zum Adressenhandel und gegen die Papierflut im Briefkasten" aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert", 1. Auflage September 1994

222 Broschüre "Datenscheckheft" aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert", 1. Auflage Dezember 1994

Beschwerden vorgetragen werden, wenn datenschutzrechtliche Probleme zwischen den Betroffenen und der jeweiligen Verwaltung (noch) nicht ausgeräumt werden konnten bzw. solche erst mit der jeweiligen Anfrage für die Betroffenen offensichtlich und somit konkretisierbar werden. Gleichzeitig erreichen mich nunmehr auch Eingaben aus weiter entfernt liegenden Landesteilen.

Unter meinem Vorsitz fand die 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam statt. Mit 21 Tagesordnungspunkten hatte die Konferenz ein umfangreiches Arbeitspensum zu bewältigen, wobei zu neun Tagesordnungspunkten zum Teil mehrere Entschließungsvorschläge vorlagen, von denen fünf einvernehmlich verabschiedet wurden. Diese Entschließungen sind in den Anlagen 4 bis 8 wiedergegeben. Vermutlich hat auch die besondere Atmosphäre des Schlosses Lindstedt im Park von Sanssouci als Tagungsstätte mit zu dem Erfolg dieser Konferenz, der unser Minister des Innern, Herr Alwin Ziel, vor Ort die Grüße der Landesregierung überbrachte, beigetragen.

Neben selbst durchgeführten Informationsgesprächen mit den Datenschutzverantwortlichen der Landkreise hat das Ministerium des Innern (MI) eine Erweiterung des Unterrichts zum Datenschutz in den Fortbildungsveranstaltungen des Landesamts für Datenverarbeitung und Statistik und der Stiftung Weiterbildung der ÖTV ermöglicht. Ich bin froh, die angelaufenen Fortbildungsgänge (so z. B. im Rahmen von Anpassungslehrgängen für Angestellte) als Podium für die Verbreitung des Datenschutzgedankens in der Verwaltung nutzen zu können. Es bleibt zu wünschen, daß das Datenschutzrecht fester Bestandteil in den Ausbildungsplänen der Landesakademie und der Fachhochschule für öffentliche Verwaltung wird. Zur dringend erforderlichen Aus- und Fortbildung der Mitarbeiter des öffentlichen Dienstes hat das MI die Studieninstitute für kommunale Verwaltung im Land Brandenburg gebeten, in ihre Fortbildungsprogramme auch Veranstaltungen zum Thema Datenschutz aufzunehmen.

Leider muß ich mich aus Kapazitätsgründen auf eine Lehrbeteiligung an den behördlichen Ausbildungsinstituten für die Landesverwaltungen beschränken, da ich mit meinen Mitarbeiterinnen und Mitarbeitern schon im Rahmen der laufenden Beratungsarbeit häufig für Informationsgespräche, Einzelvorträge, Podiumsdiskussionen usw. auch außerhalb "normaler" Dienstzeiten zur Verfügung stehe. Daher sollten die obersten Landesbehörden verstärkt prüfen, ob nicht z. B. durch bereichsspezifische erläuternde Rundschreiben den in ihren Geschäftsbereichen Beschäftigten die relevanten datenschutzrechtlichen Bestimmungen praxisnah und aufgabenbezogen vermittelt werden können. Für die Erarbeitung derartiger Konzepte biete ich gern meine Hilfe an.

Bei den für jedermann erkennbaren rasanten technologischen Entwicklungen, die alle gesellschaftlich relevanten Gebiete betreffen (z. B. Chipkarten, elektronische Objektidentifizierung), wird die weitere Durchsetzung des Grundrechts auf informationelle Selbstbestimmung absehbar immer mehr von der Technikausgestaltung bestimmt. Dies verlangt eine weitaus größere Beachtung der informationstechnischen Qualifikationen und Aufgaben, als dies bisher die gesetzlichen Bestimmungen unmittelbar erkennen lassen. Aus diesem Grund ist es erforderlich, daß meine Mitarbeiterinnen und Mitarbeiter selbst - insbesondere im technischen Bereich - durch fortbildende Maßnahmen ständig auf dem letzten Entwicklungsstand gehalten werden. Leider mußte ich die hierfür vorgesehenen Haushaltsmittel im Jahr 1994 zur Verstärkung der unabdingbar notwendigen Mittel für Reisekosten heranziehen, die für mich vorhersehbar zu knapp bemessen waren. Ich hoffe, die Restdefizite im Jahr 1995 etwas ausgleichen zu können, nachdem mir für dieses Haushaltsjahr ein verstärkter Ansatz für die Aus- (und Fort)bildung der Bediensteten zur Verfügung steht.

Dankbar bin ich für die Unterstützung durch den Präsidenten des Landtags und die Mitglieder des Präsidiums, des Hauptausschusses sowie des Ausschusses für Haushalt und Finanzen, die Voraussetzung dafür war, daß mir der Landtag mit dem am 23. März 1995 verabschiedeten Haushalt 1995 die Anhebung zweier Planstellen im juristischem Bereich, einer

Angestelltenstelle im Verwaltungsbereich und zweier Angestelltenstellen im technischen Bereich, insbesondere aber zwei zusätzliche Planstellen des höheren nichttechnischen Verwaltungsdienstes im juristischen Bereich bewilligt hat. Damit kann zum einen auf absehbare Zeit eine aufgaben- und anforderungsgerechte Einstufung aller Mitarbeiter/-innen vorgenommen werden, die auf eine Kontinuität der gewachsenen Kompetenzen zugunsten der Behörde hoffen lassen. Zum anderen werde ich nach Besetzung der beiden neuen und einer seit Januar 1995 durch Abgang freigewordenen Stelle die Zuständigkeitsgebiete neu so zuweisen können, daß eine sachgerechtere Aufgabenerfüllung als bisher erreicht wird.

Kleinmachnow, den 24. Mai 1995

Dr. sc. Dietmar Bleyl
Der Landesbeauftragte für den Datenschutz

Rede des Landesbeauftragten für den Datenschutz vor dem Plenum des Landtages Brandenburg am 23. März 1995

Sehr geehrter Herr Präsident! Sehr geehrte Damen und Herren Abgeordnete! Sehr geehrter Herr Ministerpräsident! Sehr geehrte Frauen Ministerinnen! Sehr geehrte Herren Minister! Seit Abgabe meines zweiten Tätigkeitsberichtes Anfang Mai letzten Jahres an den Präsidenten dieses Hohen Hauses ist inzwischen fast ein Jahr vergangen. Eine Reihe von Problemen, die uns im Berichtsjahr 1993/94 intensiv beschäftigt haben und die folglich einen Schwerpunkt im Tätigkeitsbericht bildeten, sind unterdessen erfreulicherweise gelöst worden. So haben beispielsweise die Polizeipräsidien in einer beispielhaften Kraftaktion ihre Kriminalaktenbestände, die sie übernommen haben, bis zum Jahresende 1994 bereinigt. Ich bin darüber glücklich.

In anderen Bereichen dagegen fehlt es noch erheblich an Problembewußtsein bei den zuständigen Stellen, geschweige denn, daß eine Lösung in Sicht wäre. Als Beispiel sei hier auf die Datenverarbeitung im Auftrag verwiesen.

Der Logik knapper Haushaltsmittel folgend, lassen zahlreiche öffentliche Stellen im Land ihre Verwaltungsdaten von Privatfirmen verarbeiten. In vielen Fällen sind das Rechenzentren von Großunternehmen in anderen Bundesländern. Dagegen kann man aus arbeitsmarktpolitischen Überlegungen heraus Einwände erheben. Dies ist aber nicht mein Thema. Datenschutzrechtlich wäre nichts dagegen einzuwenden, wenn die gesetzlichen Vorgaben bekannt wären und eingehalten würden.

Vor allem die Kommunalverwaltungen halten die gesetzlichen Einschränkungen nicht ein. Das Brandenburgische Meldegesetz verbietet eindeutig die Verarbeitung von Meldedaten in anderen Bundesländern. Steuer- und Sozialgeheimnis sollten wirksame Schranken gegen die Verarbeitung von Informationen aus diesen Bereichen durch Privatfirmen sein. Dennoch werden sowohl Meldedaten, aber auch die besonders sensiblen Sozial- und Steuerdaten auf On-line-Verbindungen über unzulänglich geschützte Netzverbindungen in andere Bundesländer geschickt und dort verarbeitet.

Ich vermisse eine Stelle im Land Brandenburg, die genau weiß, welchen Umfang unterdessen die Datenverarbeitung im Auftrag angenommen hat. Ich vermisse darüber hinaus ein zwischen allen beteiligten Stellen und meiner Behörde abgesprochenes Verfahren, das verbindlich festlegt, wie die Datenverarbeitung im Auftrag betrieben werden soll.

Ein Ansatz zur Problemlösung könnte in den allenthalben betriebenen Gründungen kommunaler Zweckverbände zu finden sein. Bei der erforderlichen Umorganisation der Verwaltungsstrukturen ließe sich auch die Datenverarbeitung im Auftrag verfassungskonform gestalten. Voraussetzung dafür ist allerdings, daß die verantwortlichen Stellen den Willen aufbringen, einheitliche Verfahrensregelungen zu entwickeln und zu befolgen, so daß dem derzeitigen Wildwuchs bei der Datenverarbeitung im Auftrag ein Ende bereitet wird.

Meine Damen und Herren, Ihnen liegt eine Beschlußempfehlung des Innenausschusses vor, den ich nur begrüßen kann. Wie schon im Vorjahr wird die Landesregierung aufgefordert, die Zusammenarbeit auf ministerialer Ebene mit meiner Behörde zu suchen und zu verbessern. Im Tätigkeitsbericht war in puncto Zusammenarbeit noch ein großes Defizit zu beschreiben. Dieses und jenes hat sich verbessert, dieses und jenes ist geblieben. Dennoch muß ich ein Beispiel bringen, das mich sehr verärgert hat. Wo war und ist beispielsweise die frühzeitige Beteiligung des Datenschutzbeauftragten bei der Erarbeitung des neuen Polizeiaufgabengesetzes? "Erweiterte Abhörbefugnisse" soll es enthalten, entnehme ich der Presse. Befugniserweiterungen einer Behörde lassen immer einen Datenschutzbeauftragten aufhorchen. Nichts gegen

Presseinformationen, aber ich darf erwarten, darüber auch an anderer Stelle aus erster Hand informiert zu werden, zumal ich denke, daß meine Behörde in der Vergangenheit bereits ausreichend die Sottise widerlegt hat, Datenschutz sei Tatenschutz.

Die Wahrung des Rechts auf informationelle Selbstbestimmung der Bürger obliegt aber im übrigen nicht nur der Landesregierung, sondern allen öffentlichen Stellen des Landes und auch Ihnen als Legislative.

Ich vermisse eine größere Bereitschaft bei Ihnen, meine Damen und Herren, auch datenschutzrechtliche Aspekte der zur Diskussion und Entscheidung anstehenden Sachverhalte aufzugreifen und in den entsprechenden Aussprachen zu problematisieren.

Während ich in der Vergangenheit noch dafür Verständnis aufbringen konnte, daß die Bürger im Land Brandenburg wirklich andere Sorgen hätten, als ihr Recht auf informationelle Selbstbestimmung wahrzunehmen, kann ich diesen Eindruck angesichts der überwältigenden Nachfrage nach dem zum Jahresende herausgegebenen Datenscheckheft meiner Behörde nicht mehr teilen. Ganz offensichtlich bewegt es die Bürger Brandenburgs doch, wer wann was über sie weiß, auf welchen Wegen personenbezogene Informationen ausgetauscht werden und wo sich Informationen über sie befinden.

Dies hängt sicherlich auch damit zusammen, daß wir inzwischen bereits mitten in einer Revolution der menschlichen Kommunikation stehen. Wo dies hinführen wird, wagt im Augenblick keiner vorherzusagen. Ein Vergleich mit den Olympischen Spielen der Neuzeit ist vielleicht nicht ganz abwegig. "Schneller, höher, stärker" - dieses Motto stand für eine völkerverbindende Idee. Ich frage Sie: Was ist daraus entwickelt worden?

Heute wird im Zusammenhang mit Datenautobahnen und deren Nutzung durch gegebenenfalls kombinierte Peripherie wie Computer, Telefon und Fernsehgeräte geworben - schneller, vielseitiger, mobiler, praktischer usw. Mit dieser Entwicklung wäre es möglich, einen Landtag in Brandenburg per Konferenzschaltung technisch durchzuführen. Sie können sich dieses Beispiel einmal theoretisch durch den Kopf gehen lassen und überlegen, welche Konsequenzen daraus zu ziehen wären.

Auffällig ist, mit welcher unkritischen Euphorie die Öffentlichkeit dieser Entwicklung gegenübersteht. Wo wird die Wahrung von Persönlichkeitsrechten durch gezielte Gestaltung der Einzeltechnik diskutiert? In diesem Sinne sollten beispielsweise für die neuen interaktiven Dienste wie Teleshopping oder Pay-TV anonyme Zugriffs- und Zahlverfahren, etwa in Form von vorausbezahlten Karten, angeboten werden, bzw. dort, wo auf Grund der eingesetzten Technik unvermeidlich eine sogenannte Datenspur hinterlassen wird, muß durch bundesweit einheitliche Regelungen die Herstellung von Kommunikationsprofilen untersagt bzw. sogar strafbewehrt werden.

Angesichts des rasanten technologischen Fortschritts auf dem Gebiet der Informationsverarbeitung, angesichts von Datenautobahnen, auf denen Informationen als Massengut in kürzester Zeit weltweit versandt werden können, bedarf es nicht zuletzt des interessierten und informierten Bürgers, wenn das Recht auf informationelle Selbstbestimmung des einzelnen nicht zur Worthülse ohne Bedeutung verkommen soll. Es bedarf, um seine Wirkung entfalten zu können, auch eines Rechts auf Zugang zu Informationen. Dazu müssen Sie, meine Damen und Herren, auch im Lande entsprechende rechtliche Möglichkeiten schaffen, damit der einzelne die "Datenautobahnauffahrten" benutzen kann. Ich meine hier ein allgemeines Akteneinsichtsrecht.

Schließlich möchte ich wenigstens kurz auf Aktivitäten meiner Behörde auf Bundesebene eingehen. Hier standen zum einen Stellungnahmen zu wichtigen Gesetzen an. Dabei habe ich insbesondere Bedenken gegen das Bundeskriminalamtsgesetz angemeldet, weil dort unter anderem die Befugnisse des BKA als Zentralstelle zur Datenerhebung und -übermittlung bis hin

zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit der jeweils verantwortlichen Länderpolizei festgeschrieben werden.

Damit wird in unzulässiger Weise in Länderkompetenzen eingegriffen. Dies ist insoweit auch höchst aktuell, da ab kommenden Sonntag das Schengener Informationssystem seine Arbeit aufnimmt. Hier handelt es sich um eine Datenbank der europäischen Polizeibehörden, die immerhin auf 10 Millionen Fahndungsdaten ausgelegt ist. Über das BKA als Zentralstelle werden dort auch brandenburgisch Betroffene eingestellt werden.

Zum anderen oblag es Brandenburg im vergangenen Jahr, die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ähnlich wie bei der IMK auszurichten. In diesem Zusammenhang habe ich seitens des Präsidenten des Landtages und der Landesregierung tatkräftige Unterstützung erhalten und möchte mich dafür ausdrücklich an dieser Stelle bedanken.

Angesichts zahlreicher und schwieriger Aufgaben, die im Bereich des Datenschutzes anstehen und die wir nur gemeinsam lösen können, freue ich mich, meine Damen und Herren, auf eine gedeihliche weitere Zusammenarbeit im kommenden Jahr. - Ich danke Ihnen für Ihre Aufmerksamkeit.

Entschließung

der Datenschutzbeauftragten des Bundes und der Länder
vom 25. August 1994

zum

Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik

- EG-Statistikverordnung -

(KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer **Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik** (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger

belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 26./27. September 1994 in Potsdam

zu

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 26./27. September 1994 in Potsdam

zu

Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz)
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 26./27. September 1994 in Potsdam

zu

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten
der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 26./27. September 1994 in Potsdam

zu

Art. 12 Verbrechensbekämpfungsgesetz
zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtssprechung des Bundesverfassungsgerichts sicherzustellen.

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 26./27. September 1994 in Potsdam

zu

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz
im ISDN und in Mobilfunknetzen vom 13. Juni 1994
(KOM (94) 128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den

angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zum

Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz)
- Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts";

- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;

- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zum

Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von "lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an "sicherheitsempfindlichen Stellen" tätig sind. Als "lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, "die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur "Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,

- Zustimmung des Betroffenen als Verfahrensvoraussetzung,

- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,

- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,

- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,

- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,

- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,

- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zum

Datenschutz bei elektronischen Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte

Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze, z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.

7. Zur Beweissicherung einer stattgefunden Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:

   - Zustellung/Empfangsnachweise
   - Sende/Empfangsübergabenachweise

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zu

Automatische Erhebung von Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zu

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene ”Recht auf Vergessen” wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien (”Medienprivileg”) neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das "Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem masssenmedial vermittelten "modernen Pranger" werden.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zum

Sozialgesetzbuch VII

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung - einschließlich der Aufbewahrungsfristen -sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zu

Eingeschränkter Zugriff auf Versichertendaten
bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wieviele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten[1] halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen "Stammdatensatz" zugreifen. Dieser "Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

[1] bei Stimmenthaltung von Rheinland-Pfalz

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zu

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[1] erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

---

[1] bei Stimmenthaltung von Hamburg

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 9./10. März 1995 in Bremen

zum

Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung[1] gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

---

[1] Bei Gegenstimme von Baden-Württemberg zu Nr. 4.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden

- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Stichwortverzeichnis:

(Berichtszeitraum der Jahresberichte: I = März bis Dezember 1992; II = bis März 1994; III = bis März 1995 /Seitenangabe)

Abkürzungsverzeichnis

1. SRG	=	Erstes Schulreformgesetz für das Land Brandenburg
2. MeldDÜÄV	=	Zweite Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
2. SGBÄndG	=	2. Gesetz zur Änderung des Sozialgesetzbuches
a. F.	=	alte Fassung
ABl.	=	Amtsblatt
Abs.	=	Absatz
Abschn.	=	Abschnitt
ADV	=	Automatische Datenverarbeitung
AFIS	=	Automatisierte Fingerabdruck-Identfizierungssystem
AG	=	Ausführungsgesetz
AgrStaG-DVO	=	Verordnung über die Durchführung des Agrarstatistikgesetzes
AGTierSGBbg	=	Gesetz zur Ausführung des Tierseuchengesetzes
AMG	=	Arzneimittelgesetz
Änd.	=	Änderung
Anl.	=	Anlage
AO	=	Abgabenordnung
AO-GS	=	Ausbildungsordnung der Grundschule im Land Brandenburg
AOK	=	Allgemeine Ortskrankenkasse
Art.	=	Artikel
Ärzte-ZV	=	Zulassungsordnung für Vertragsärzte
Aufl.	=	Auflage
AufnV	=	Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg
AuslG	=	Ausländergesetz
AV	=	Allgemeine Verfügung
ca.	=	circa
Bbg DSG	=	Brandenburgisches Datenschutzgesetz
Bbg.	=	Brandenburgisch(es)
BbgArchG	=	Brandenburgisches Archivgesetz
BbgBO	=	Brandenburgische Bauordnung
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgKita-Gesetz	=	Brandenburgisches Kindertagesstättengesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgRAVG	=	Brandenburgisches Rechtsanwaltsversorgungsgesetz
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BDSG	=	Bundesdatenschutzgesetz
BdVP	=	Bezirksdirektionen der Volkspolizei
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BKAG-E	=	Bundeskriminalamtgesetz-Entwurf
BKGG	=	Bundeskindergeldgesetz
BlnDSG	=	Berliner Datenschutzgesetz
BLVS	=	Landesamt für Verkehr und Straßenbau Brandenburg
BND	=	Bundesnachrichtendienst
BR-Drs.	=	Bundesrats-Drucksache
BSS	=	Basisstationen
BStatG	=	Bundesstatistikgesetz
BT-Drs	=	Bundestags-Drucksache
Buchst.	=	Buchstabe

Bundes-SISY	=	bundesweites staatanwaltschaftliches Informationssystem
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BZR	=	Bundeszentralregister
BZRG	=	Bundeszentralregistergesetz
bzw.	=	beziehungsweise
CD-ROM	=	Compact Disc Read Only Memory
CSIS	=	Centrales Schengener Informationssystem
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DDR-GBl.	=	DDR-Gesetzblatt
DES	=	Data Encryption Standard
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DORA	=	Dialogorientertes Recherche- und Auskunftssystem
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
e. V.	=	eingetragener Verein
ed-Behandlung	=	erkennungsdienstliche Behandlung
EDU	=	European Drug Unit
EG	=	Europäische Gemeinschaft
EUROPOL	=	Europäisches Polizeiamt
EuWG	=	Europawahlgesetz
FDGB	=	Freier Deutscher Gewerkschaftsbund
ff.	=	folgende
GastVO	=	Verordnung zur Ausführung des Gaststättengesetzes
geänd.	=	geändert
GEK	=	Kohortenstudie "Gesundheit, Ernährung, Krebs"
gem.	=	gemäß
GG	=	Grundgesetz
GGG	=	Gesetz über die gesellschaftlichen Gerichte der DDR
GO	=	Gemeindeordnung
GVBl.	=	Gesetz- und Verordnungsblatt
GWG	=	Geldwäschegesetz
G 10	=	Gesetz zu Artikel 10 Grundgesetz
G 10 AG Bbg	=	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg
HeilBerG	=	Heilberufsgesetz
hrsg.	=	herausgegeben
i. d. Fassung	=	in der Fassung
IHK	=	Industrie- und Handelskammern
IHK-G	=	IHK-Gesetz
INPOL	=	Informationssytem der Polizei
InVeKoS	=	Integriertes Verwaltungs- und Kontrollsystem
ISO	=	International Organization for Standardization
i. S. v.	=	im Sinne von
i. V. m.	=	in Verbindung mit
ISDN	=	Integrated Services Digital Network (dienste-integrierendes Digitalnetz)
JMBl.	=	Justizministerialblatt
JVA	=	Justizvollzugsanstalt
KA	=	Kriminalakte
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
Kap.	=	Kapitel
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
KJHG	=	Kinder- und Jugendhilfegesetz

KKO	=	Konfliktkommissionsordnung
KRG	=	Krebsregistergesetz
LAG	=	Landesarbeitsgruppe
LBG	=	Landesbeamtengesetz
LDS	=	Landesamt für Datenverarbeitung und Statistik
LELF	=	Landesamt für Ernährung, Landwirtschaft und Flurneuordnung
LfD	=	Landesbeauftragter für den Datenschutz
LfV	=	Landesamt für Verfassungsschutz
LGG	=	Landesgleichstellungsgesetz
LHO	=	Landeshaushaltsordnung
LKA	=	Landeskriminalamt
LKGBbg	=	Krankenhausgesetz des Landes Brandenburg
LSPV	=	Lehrerstellen- und Personalverwaltung
LT-Drs.	=	Landtags-Drucksache
MAC	=	Medium Access Control
MAGSF	=	Ministerium für Arbeit, Gesundheit, Soziales und Frauen
MBJS	=	Ministerium für Bildung, Jugend und Sport
MdF	=	Ministerium der Finanzen
MdJ	=	Ministerium der Justiz und für Bundes- und Europaangelegenheiten
MDK	=	Medizinischen Dienst der Krankenkassen
MeldDÜÄV	=	Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MELF	=	Ministerium für Ernährung, Landwirtschaft und Forsten
MI	=	Ministerium des Innern
MiStra	=	Anordnung über Mitteilungen in Strafsachen
MOD	=	Magneto-optische Datenträger
MSWV	=	Ministerium für Stadtentwicklung, Wohnen und Verkehr
MWFK	=	Ministerium für Wissenschaft, Forschung und Verkehr
n. F.	=	neue Fassung
Nr.	=	Nummer
NSIS	=	Nationales Schengener Informationssystem
OWiG	=	Gesetz über Ordnungswidrigkeiten
PAK	=	Personenarbeitskartei
pB	=	Polizeiliche Beobachtung
PC	=	Personalcomputer
PersVG	=	Landespersonalvertretungsgesetz
PflRi	=	Pflegebedürftigkeits-Richtlinien
PHW	=	personenbezogener Hinweis
PolG	=	Polizeigesetz
PO-Nsch	=	Nichtschülerprüfungsverordnung
RAK	=	Referatsarbeitskartei
RSA-Algorithmus	=	nach den Entwicklern Rivest, Shamir und Adleman
RVO	=	Reichsversicherungsordnung
S.	=	Seite
s.	=	siehe
Sachgeb.	=	Sachgebiet
SchG	=	Schiedsstellengesetz
SCHUFA	=	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SchuVVO	=	Verordnung über das Schuldnerverzeichnis
SDÜ	=	Schengener Durchführungsübereinkommen
SGB	=	Sozialgesetzbuch
SIS	=	Schengener Informationssystem
1. SKWPG	=	Ersten Gesetzes zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms
SopV	=	Verordnung über Unterricht und Erziehung für junge Menschen

		mit sonderpädagogischem Förderbedarf
StA	=	Staatsanwaltschaft
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StUG	=	Stasi-Unterlagen-Gesetz
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
StVZO	=	Straßenverkehrszulassungsordnung
TK	=	Telekommunikation
TSK	=	Tierseuchenkasse
u. a.	=	unter anderem
UAG	=	Untersuchungsausschußgesetz
UIG	=	Umweltinformationsgesetz
u. U.	=	unter Umständen
VDMA	=	Verband Deutscher Maschinen- und Anlagenbau e.V
vgl.	=	vergleiche
VGO	=	Vollzugsgeschäftsordnung
VGPolGBbg	=	Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg
VPKÄ	=	Volkspolizeikreisämter
VV	=	Verwaltungsvorschrift
VV-Hausunterricht	=	Verwaltungsvorschriften über die Durchführung von Hausunterricht
VwVfGBbg	=	Verwaltungsverfahrensgesetz
VZR	=	Verkehrszentralregister
WoBelegG	=	Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen
WoBindG	=	Wohnungsbindungsgesetz
WoGG	=	Wohngeldgesetz
WoGSoG	=	Wohngeldsondergesetz
WORM	=	Write Once Read Many
ZBB	=	Zentrale Bezügestelle des Landes Brandenburg
Ziff.	=	Ziffer
ZPO	=	Zivilprozeßordnung
zul.	=	zuletzt
z. Z.	=	zur Zeit