Landtag Brandenburg **Drucksache 2/83**
2. Wahlperiode

Zweiter Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. Januar 1993 bis 31. März 1994

Datum des Originals: 10.11.1994 / Ausgegeben: 24.11.1994

Landtag Brandenburg **Drucksache 2/83**
2. Wahlperiode

Zweiter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. Januar 1993 bis 31. März 1994

Inhaltsverzeichnis Seite

Datum des Originals: 13.05.1994 / Ausgegeben: 18.05.1994

1 Datenschutzrechtliche Entwicklungen in Brandenburg

1.1 Einleitung

Im Verlauf des Berichtszeitraumes ergab sich für meine Tätigkeit eine grundsätzliche Wende. Während im Vorjahr die unumgängliche Auseinandersetzung mit dem riesigen Erbe personenbezogener Datenbestände aus der ehemaligen DDR bei der Lösung der aktuellen Datenschutzprobleme im Land Brandenburg im Vordergrund gestanden und zugleich der Aufbau der Dienststelle die Arbeit meiner Behörde im wesentlichen bestimmt hatten, war nunmehr das Engagement auf diesem Gebiet nur noch in einzelnen Bereichen erforderlich. Ich konnte mich daher zukunftsausgerichteten Aufgabenstellungen zuwenden.

Besondere Beachtung hat im Berichtszeitraum die Schaffung möglichst normenklarer spezialgesetzlicher Regelungen für das Land Brandenburg gefunden, da das Brandenburgische Datenschutzgesetz (Bbg DSG)[1] als Übergangsregelung im Januar 1996 seine Gültigkeit für die Erhebung, Speicherung und Übermittlung personenbezogener Daten verlieren wird, und diese Bestimmungen die Grundlage für eine effektive Kontrolltätigkeit meiner Behörde bilden werden. In dieser Hinsicht wurden große Fortschritte speziell im Bereich des Gesundheitswesens erzielt, obwohl nicht alle vom Parlament verabschiedeten Gesetze als "großer Wurf" gelten können. Spürbar zugenommen hat das Interesse an einer gründlichen Debatte von Datenschutzproblemen in den einzelnen Ausschüssen. Ich verbinde damit die Hoffnung, daß in der nächsten Legislaturperiode - wie in anderen Parlamenten auch - ein Unterausschuß für Datenschutz gebildet wird.

Die Vor-Ort-Kontrollen meiner Behörde konzentrierten sich schwerpunktmäßig auf den Polizei- und Krankenhausbereich. Dabei waren - vor allem bei den organisatorischen und sicherheitstechnischen Maßnahmen - zum Teil gravierende Mängel festzustellen, die ohne entsprechende investive Maßnahmen nicht beseitigt werden können. Beharrlichkeit und Geduld sind hier gefordert, um zumindest schrittweise den in den alten Bundesländern erreichten Standard durchzusetzen.

Als besondere Herausforderung hat sich die Praxis der Datenverarbeitung im Auftrag erwiesen, deren datenschutzrechtliche Brisanz auch im Land Brandenburg noch vielfach nicht erkannt wird.

Ausdrücklich bedanken möchte ich mich für die vielen Anfragen und Eingaben. Sie reflektieren ein kontinuierlich gewachsenes Vertrauen in die Arbeit meiner Behörde und stellen darüber hinaus für mich eine unersetzliche Information über die Probleme dar, die die Bürger im Land Brandenburg in bezug auf ihr Recht auf informationelle Selbstbestimmung bewegen. Sie finden ihren Niederschlag auch in diesem Tätigkeitsbericht und mögen auf diese Weise Informationen und Anregungen an Bürger, Verwaltungen und den Landtag zugleich vermitteln. Die aktive Rolle der Bürger ist für die Durchsetzung des Datenschutzes im Land Brandenburg unverzichtbar!

Insgesamt ist nicht zu übersehen, daß der Datenschutz im Land Brandenburg inzwischen Konturen gewonnen hat, die jedoch nicht losgelöst von dem vorgegebenen Umfeld zu sehen sind und maßgeblich durch andere Entwicklungen - in erster Linie der Bundesgesetzgebung - bestimmt werden. In bezug auf die aktuelle Situation möchte ich hier lediglich auf zwei Probleme aufmerksam machen:

- Die Bemühungen, das Recht auf informationelle Selbstbestimmung unmittelbar im

---

[1] vom 20. Januar 1992, GVBl. I, S. 2

Grundgesetz zu verankern, sind - auch 10 Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht im sog. "Volkszählungsurteil"[2] - an der erforderlichen Zweidrittelmehrheit im Bundestag und Bundesrat gescheitert. Dabei wird argumentiert, es ließe sich auch ohne eine Ergänzung des Grundgesetzes aus dem Art. 2 i.V.m. Art. 1 Abs. 1 (Allgemeine Persönlichkeitsrechte) ableiten. Dies ist für den Rechtsunkundigen nicht ohne weiteres nachzuvollziehen.

- Es zeichnet sich die Tendenz ab, für die neuen Bundesländer die aus dem Einigungsvertrag herrührenden und zum Aufbau der Verwaltungen vorübergehend hinzunehmenden Sonderregelungen festzuschreiben. Angesichts der Gefahr, daß eine solche Ungleichbehandlung am Ende den Schutz des Grundrechts auf informationelle Selbstbestimmung aushöhlen kann, auf den die Menschen in den neuen Bundesländern einen ebenso selbstverständlichen Anspruch haben wie in den alten Bundesländern, beobachte ich diese Tendenz mit Sorge.

Ein wichtiges Ereignis war für meine Behörde die Ausrichtung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam. Ihre Ergebnisse sind als Anlage 16 - 21 dem Tätigkeitsbericht angefügt. Gleichfalls als Anlage sind die Entschließungen der Datenschutzkonferenzen seit dem Bestehen meiner Behörde aufgenommen. Damit soll ein Versäumnis des letzten Tätigkeitsberichts nachgeholt werden.

Zu danken habe ich wiederum meinen Kollegen vom Bund und den anderen Bundesländern, insbesondere dem Berliner Datenschutzbeauftragten, die es mir und meinen Mitarbeitern mit freundlicher Selbstverständlichkeit ermöglichen, die langjährigen Erfahrungen ihrer Behörden zu nutzen.

Danken möchte ich an dieser Stelle auch der für den privaten Bereich zuständigen Aufsichtsbehörde für den Datenschutz beim Ministerium des Innern für die gute Zusammenarbeit und den weiterführenden Austausch über gemeinsam interessierende datenschutzrechtliche Fragestellungen.

Für den Jahresbericht wurde als Stichtag der 31. März 1994 gewählt.

1.2 Besondere Probleme bei der Umsetzung des Brandenburgischen Datenschutzgesetzes

1.2.1 Datenverarbeitung im Auftrag

Die mir bisher bekanntgewordene Praxis der Datenverarbeitung im Auftrag im Land Brandenburg (s. unter 1.2.1.4) hat mich vor Probleme bei der Erfüllung meiner Aufgaben gem. § 23 Abs. 1 und Abs. 2 Satz 1 Bbg DSG gestellt. Insbesondere sind meine Möglichkeiten gering, die verantwortlichen Entscheidungsträger in den Kommunalverwaltungen zu erreichen und die notwendigen Verständnisvoraussetzungen zu vermitteln. Da ich nach meinen bisherigen Informationen von gravierenden Rechtsverletzungen bei der Datenverarbeitung im Auftrag ausgehen muß, soll deshalb an dieser Stelle der Versuch unternommen werden, über meinen Tätigkeitsbericht die

[2] BVerfGE 65, 1 ff.

Problematik der Datenverarbeitung im Auftrag als eine datenschutzrechtliche Frage von besonderer Bedeutung an den Landtag und die Landesregierung heranzutragen und dabei nicht nur den ihr zugrundeliegenden Sachverhalt zu schildern, sondern auch die zu seiner Beurteilung erforderlichen datenschutzrechtlichen Kriterien zu erläutern und auf den aus meiner Sicht unverzichtbaren Handlungsbedarf (s. unter 1.2.1.5) hinzuweisen.

1.2.1.1 Begriffsbestimmung

Der Begriff der Datenverarbeitung im Auftrag setzt voraus, daß es sich um eine Verarbeitung personenbezogener Daten i.S.v. § 3 Abs. 2 Bbg DSG handelt und daß dieser Datenverarbeitung ein entgeltliches oder unentgeltliches Auftragsverhältnis i.S.d. §§ 662, 675 des Bürgerlichen Gesetzbuches (BGB)[3] zugrunde liegt. Dabei muß die vertragliche Hauptleistungspflicht des Auftragnehmers gerade in der Datenverarbeitung bestehen, d. h. die Verar-beitung personenbezogener Daten darf nicht bloße Nebenfolge einer anderen - der eigentlichen - vertraglichen Leistung sein.

Damit ist die Datenverarbeitung im Auftrag abzugrenzen von solchen Geschäftsbesorgungsverträgen, mit denen dem Auftragnehmer eine öffentliche Aufgabe ganz oder teilweise zur selbständigen Erledigung übertragen wird und bei denen so eine eigenständige, nach außen gerichtete Tätigkeit des Auftragnehmers erfolgen soll. In diesen Fällen handelt es sich um eine eigene Datenverarbeitung des Auftragnehmers zur Erfüllung seiner eigenen, vom Auftraggeber übernommenen Aufgaben. Datenverarbeitende Stelle (vgl. § 3 Abs. 4 Nr. 1 Bbg DSG) ist deshalb der Auftragnehmer. Er verarbeitet die Daten für sich selbst.

Bei der Datenverarbeitung im Auftrag wird dagegen dem Auftragnehmer nur die Datenverarbeitung übertragen, die zur Erfüllung der Aufgabe der öffentlichen Stelle erforderlich ist. Die Aufgabe selbst wird weiterhin von der öffentlichen Stelle wahrgenommen. Sie läßt dazu lediglich die Daten durch den Auftragnehmer verarbeiten und bleibt deshalb datenverarbeitende Stelle i.S.v. § 3 Abs. 4 Nr. 1 Bbg DSG. Man spricht in diesen Fällen auch davon, daß der Auftraggeber "Herr der Daten" bleibt, und das Gesetz weist ihm in § 11 Abs. 1 Satz 1 Bbg DSG gegenüber dem Betroffenen die ausschließliche Verantwortlichkeit für die Einhaltung der Vorschriften über den Datenschutz zu.

Die rechtliche Konsequenz der begrifflichen Abgrenzung ist folgende: Bei der Datenverarbeitung im Auftrag ist der Auftragnehmer gegenüber dem Betroffenen zur Verarbeitung der personenbezogenen Daten im selben Umfang legitimiert wie der Auftraggeber. Der Betroffene kann sich zur Abwehr etwaiger Beeinträchtigungen seines Rechts auf informationelle Selbstbestimmung grundsätzlich nur an den Auftraggeber wenden.

Anders ist es, wenn der Auftragnehmer die personenbezogenen Daten in Verfolgung eigener Geschäftszwecke für sich selbst verarbeitet. In diesen Fällen ist der Auftragnehmer nicht in die Legitimation des Auftraggebers einbezogen, sondern bedarf als selbständige datenverarbeitende Stelle einer eigenen Befugnis zur Verarbeitung personenbezogener Daten. Ist der Auftragnehmer eine nicht-öffentliche Stelle, so ist eine solche Ermächtigung in Ermangelung bereichsspezifischer Regelungen grundsätzlich nicht gegeben, da das Brandenburgische Datenschutzgesetz nur für die Datenverarbeitung durch öffentliche Stellen gilt. Auch eine Befugnis des (öffentlichen) Auftraggebers zur Weitergabe personenbezogener Daten besteht in diesen Fällen grundsätzlich nicht: Da die Aufgabenerfüllung einer anderen datenverarbeitenden Stelle zugewiesen wird, würde es sich bei der Weitergabe von personenbezogenen Daten durch den Auftraggeber gem. § 3 Abs. 2 Nr. 4 i.V.m. Abs. 4 Nr. 2 Bbg DSG um eine Übermittlung handeln, die in Ermangelung bereichsspezifischer

---

[3] vom 18. August 1896, RGBl., S. 195, zuletzt geänd. am 29. Oktober 1993, BGBl. I, S. 1838

Regelungen nach Maßgabe von § 16 Bbg DSG regelmäßig nicht zulässig wäre.

Nach den genannten Kriterien handelt es sich beispielsweise um Datenverarbeitung im Auftrag, wenn der Auftragnehmer für den Auftraggeber durch entsprechende Datenverarbeitungsprozesse Berechnungen vornimmt, deren Ergebnisse dann von der öffentlichen Stelle zum Erlaß von z. B. Gebührenbescheiden abgerufen werden; so z. B. wenn eine Kreisverwaltung, die die Abfallentsorgung selbst durchführt, die Gebührenbescheide von einer anderen öffentlichen oder nicht-öffentlichen Stelle erstellen läßt. In diesem Fall führt der Auftragnehmer lediglich im Sinne einer unselbständigen Hilfstätigkeit die zur Erfüllung der Aufgaben der öffentlichen Stelle erforderliche Datenverarbeitung durch; der Erlaß des Gebührenbescheides und damit die Wahrnehmung der öffentlichen Aufgaben erfolgt jedoch durch den Auftraggeber.

Anders ist es, wenn ein Landkreis die Aufgabe der Abfallentsorgung einer anderen Stelle überträgt, z. B. einer privaten Entsorgungsgesellschaft. In diesem Fall verarbeitet die Gesellschaft die Daten nicht im Auftrag des Kreises, sondern zur Erfüllung der von dem Kreis übernommenen eigenen Aufgaben. Das gleiche gilt bei der Beauftragung eines Rechtsanwalts oder eines Sachverständigen. In allen diesen Fällen steht nicht die Datenverarbeitung im Vordergrund, sondern eine andere Leistung, die als die eigentliche erbracht werden soll (z. B. Abfallentsorgung, Rechtsberatung, Sachverständigengutachten).

Auch bei der Beauftragung privater Schreibbüros ist dies grundsätzlich der Fall. Bei dieser (Hilfs-)Tätigkeit steht ebenfalls nicht die zugleich mit der Textverarbeitung erfolgende Verarbeitung von Daten im Vordergrund, sondern das Erstellen von Schriftsätzen als eigenständige Werkleistung. Soweit dazu auch die Verarbeitung personenbezogener Daten erforderlich wäre, ist deshalb die Beauftragung privater Schreibbüros durch öffentliche Stellen grundsätzlich unzulässig.

1.2.1.2 Wartung und Fernwartung

Eine besondere Form der Datenverarbeitung im Auftrag ist die Wartung und Fernwartung automatisierter Datenverarbeitungssysteme bei öffentlichen Stellen durch zumeist private Dienstleistungsunternehmen.

Da das Brandenburgische Datenschutzgesetz jede Verwendung personenbezogener Daten ungeachtet der dabei angewendeten Verfahren als Datenverarbeitung definiert (§ 3 Abs. 2 Nr. 7 Bbg DSG), handelt es sich bei der Wartung von ADV-Systemen um Datenverarbeitung. Dabei ist zu betonen, daß die Verarbeitung personenbezogener Daten begrifflich nicht voraussetzt, daß gerade auch der Informationsgehalt der Daten genutzt wird; vielmehr reicht es, daß für eine Person oder Stelle die faktische Möglichkeit besteht, sich ohne weiteres jederzeit die das Grundrecht der Betroffenen beeinträchtigende Kenntnis von den personenbezogenen Daten zu beschaffen. Dies ist bei der Systemwartung grundsätzlich ebenso der Fall wie z. B. bei der bloßen Aufbewahrung von Akten.

Bei einer Novellierung des Brandenburgischen Datenschutzgesetzes sollte die rechtliche Zuordnung der Wartung und Fernwartung zur Datenverarbeitung im Auftrag ausdrücklich klargestellt werden.

1.2.1.3 Rechtliche Grenzen der Datenverarbeitung im Auftrag

Nach der begrifflichen Bestimmung (s. unter 1.2.1.1) kommt es bei der Datenverarbeitung im Auftrag zwar nicht zu einer Übermittlung personenbezogener Daten i.S.v. § 3 Abs. 2 Nr. 4 i.V.m. Abs. 4 Nr. 2 Bbg DSG. Die zu verarbeitenden personenbezogenen Daten werden bei der Datenverarbeitung im Auftrag jedoch offenbart. Eine Offenbarung personenbezogener

Daten liegt in jedem Verhalten einer öffentlichen Stelle, durch das einem anderen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person bekannt werden können. Dies ist bei der Verarbeitung personenbezogener Daten im Auftrag der Fall.

Deshalb ist die Datenverarbeitung im Auftrag immer dann unzulässig, wenn einer Offenbarung personenbezogener Daten besondere gesetzliche Schutzvorschriften entgegenstehen. Solche Schutzvorschriften sind insbesondere die Berufsgeheimnisse (z. B. das Arztgeheimnis; vgl. § 203 Strafgesetzbuch - StGB -) und die besonderen Amtsgeheimnisse. So schließen z. B. das Steuergeheimnis (§ 30 Abgabenordnung)[4] und die verfassungsrechtliche Kompetenzzuweisung (Art. 108 Abs. 2 Satz 1 Grundgesetz) grundsätzlich jede Verarbeitung personenbezogener (Steuer-)Daten im Auftrag der Finanzverwaltung aus. Das gleiche gilt für die Verarbeitung personenbezogener Daten, die dem Personalaktendatengeheimnis (vgl. § 57 Landesbeamtengesetz - LBG[5] - i.V.m. Art. 33 Abs. 4 und 5 Grundgesetz) unterliegen. Für personenbezogene Daten, die dem Sozialgeheimnis unterliegen, hat der Bundesgesetzgeber die Datenverarbeitung im Auftrag nur in den engen Grenzen der abschließenden Regelung des § 80 Sozialgesetzbuch X (SGB X)[6] zugelassen. Für den Bereich des Ausländerwesens enthalten die bereichsspezifischen Regelungen im Ausländer- und Asylverfahrensgesetz[7] dagegen keine entsprechende Befugnis, so daß in diesem Bereich die Verarbeitung personenbezogener Daten grundsätzlich ausgeschlosen ist. Im Bereich des Meldewesens läßt das Meldegeheimnis eine Datenverarbeitung im Auftrag nur unter den Voraussetzungen der §§ 35 und 36 Meldegesetz (BbgMeldeG)[8] zu. Eine weitere bereichsspezifische Regelung ist im Hinblick auf das Statistikgeheimnis geplant (s. unter 3.9.3).

In diesem Zusammenhang ist darauf hinzuweisen, daß der Gesetzgeber die unbefugte Offenbarung personenbezogener Daten in § 203 Abs. 2 Satz 2 StGB grundsätzlich als Straftatbestand ausgestaltet hat und insbesondere die Verarbeitung von Steuerdaten im Auftrag in der Person der Verantwortlichen den objektiven Tatbestand einer Verletzung des Steuergeheimnisses (§ 355 StGB) erfüllen würde.

Die Verarbeitung personenbezogener Daten im Auftrag öffentlicher Stellen ist - abgesehen von einigen wenigen bereichsspezifischen Regelungen (z. B. in § 35 BbgMeldG) - in Brandenburg in § 11 Bbg DSG geregelt. Den Bestimmungen dieser Vorschrift waren gem. § 40 Abs. 6 Bbg DSG die zum Zeitpunkt des Inkrafttretens des Brandenburgischen Datenschutzgesetzes bereits bestehenden Auftragsverhältnisse innerhalb eines Jahres, d. h. bis zum 23. Januar 1993, anzupassen. Im einzelnen gilt nach der Regelung des § 11 Bbg DSG für die Datenverarbeitung im Auftrag folgendes:

- Gem. § 11 Abs. 1 Satz 1 Bbg DSG ist entsprechend der begrifflichen Bestimmung der Datenverarbeitung im Auftrag (s. unter 1.2.1.1) die auftraggebende öffentliche Stelle für die Einhaltung sämtlicher Vorschriften über den Datenschutz verantwortlich.

---

[4] vom 16. März 1976, St-Slg. Nr. 800, zuletzt geänd. am 21. Dezember 1992, BGBl. I, S. 2150

[5] vom 24. Dezember 1992, GVBl. I, S. 506

[6] vom 18. August 1980, BGBl. I, S. 1469, ber. 4. November 1982, BGBl. I, S. 1450, zuletzt geänd. am 24. Juni 1993, BGBl. I, S. 1038

[7] AuslG. vom 9. Juli 1990, BGBl. I, S. 1354, zuletzt geändert 30. Juni 1993, BGBl. I, S. 1062; vom AsylVfG i.d.Fass. der Bekanntmachung vom 27. Juli 1993, BGBl. I, S. 1361, zuletzt geändert 2. August 1993, BGBl. I, S. 1442

[8] vom 25. Juni 1992, GVBl. I, S. 236

- Der Auftragnehmer darf die personenbezogenen Daten nur im Rahmen der Weisung der öffentlichen Stelle verarbeiten (§ 11 Abs. 1 Satz 2 Bbg DSG).

- Die öffentliche Stelle hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach § 10 Bbg DSG notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 11 Abs. 1 Satz 3 Bbg DSG).

- Der Auftrag ist schriftlich zu erteilen (§ 11 Abs. 1 Satz 4, 1. Halbsatz Bbg DSG).

- Bei der Auftragserteilung sind erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen (§ 11 Abs. 1 Satz 4, 2. Halbsatz Bbg DSG).

- Ist der Auftragnehmer keine öffentliche Stelle, die gem. § 2 Abs. 1 Satz 1 Bbg DSG den Bestimmungen des Bbg DSG unterliegt, so ist die Auftragserteilung genehmigungspflichtig (§ 11 Abs. 1 Satz 5, 1. Halbsatz Bbg DSG); die Zustimmung erteilt bei öffentlichen Stellen des Landes die jeweilige zuständige oberste Landesbehörde, bei Gemeinden und Gemeindeverbänden das Ministerium des Innern (§ 11 Abs. 1 Satz 5, 2. Halbsatz Bbg DSG).

- § 11 Abs. 2 Bbg DSG enthält besondere Bestimmungen für den Fall, daß das Landesamt für Datenverarbeitung und Statistik, gemeinsame Gebietsrechenzentren, Fachrechenzentren, Hochschulrechenzentren oder kommunale Datenverarbeitungseinrichtungen personenbezogene Daten im Auftrag öffentlicher Stellen verarbeiten. Obgleich die genannten Einrichtungen in diesem Fall nicht selbst datenverarbeitende Stelle sind, gelten für sie auch -soweit es die Datenverarbeitung im Auftrag betrifft - die Bestimmungen des Brandenburgischen Datenschutzgesetzes über das Datengeheimnis, die technisch-organisatorischen Maßnahmen und die Kontrolle durch den Landesbeauftragten für den Datenschutz unmittelbar.

- § 11 Abs. 3 Bbg DSG regelt den Fall der Datenverarbeitung im Auftrag durch private Auftragnehmer sowie durch öffentliche Stellen außerhalb des Landes Brandenburg. In beiden Fällen hat die auftragserteilende öffentliche Stelle sicherzustellen, daß der Auftragnehmer die Bestimmungen des Brandenburgischen Datenschutzgesetzes befolgt. Wird die Datenverarbeitung in Brandenburg durchgeführt, so muß sich der private Auftragnehmer in dem Vertrag der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwerfen.

- Nicht vorgesehen ist eine datenschutzrechtliche Kontrolle in dem Fall, daß ein privater Auftragnehmer die Datenverarbeitung außerhalb des Landes Brandenburg durchführt. In diesem Fall soll vielmehr genügen, daß die am Ort der Datenverarbeitung zuständige Datenschutzkontrollbehörde unterrichtet wird (§ 11 Abs. 3 Satz 2 Bbg DSG).

  Insoweit ist jedoch von einem Versehen des Gesetzgebers auszugehen. Es kann nicht beabsichtigt sein, daß der Auftragnehmer einer öffentlichen Stelle im Land Brandenburg bei der für diese Stelle erfolgenden Datenverarbeitung geringeren datenschutzrechtlichen Verpflichtungen unterliegen soll, wenn er die Datenverarbeitung außerhalb des Landes durchführt. Da nach der Regelung in § 11 Abs. 3 Bbg DSG die Einhaltung der technisch-organisatorischen Maßnahmen (§ 10 Bbg DSG) und der anderen Vorschriften über den Datenschutz bei der Datenverarbeitung im Auftrag öffentlicher Stellen im Land Brandenburg außerhalb des Landes nicht mehr von unabhängigen Datenschutzbeauftragten kontrolliert werden kann, ist eine solche Datenverarbeitung im Hinblick auf die erhebliche Bedeutung, die der Beteiligung unabhängiger Datensschutzbeauftragter von Verfassungs

wegen zukommt[9], grundsätzlich unzulässig. Insoweit steht das Verfassungsrecht der in § 11 Abs. 3 Satz 2 Bbg DSG vom Gesetzgeber als zulässig vorausgesetzten Datenverarbeitung im Auftrag durch nicht-öffentliche Stellen außerhalb Brandenburgs entgegen, da die dazu getroffene Regelung den verfassungsrechtlichen Anforderungen nicht entspricht. Es kann nicht hingenommen werden, daß die personenbezogenen Daten der Bürger des Landes Brandenburg bei der Verarbeitung im Auftrag öffentlicher Stellen des Landes oder der Kommunen dem verfassungsrechtlichen Schutz der Kontrolle durch einen unabhängigen Datenschutzbeauftragten entzogen werden.

- Nach § 11 Abs. 3 Satz 3 Bbg DSG hat die öffentliche Stelle bei einer Auftragserteilung an einen privaten Auftragnehmer sowie an öffentliche Stellen außerhalb des Landes Brandenburg sowohl die Aufsichtsbehörde für den Datenschutz (§ 38 BDSG) als auch mich über die Beauftragung zu unterrichten.

  Hintergrund dieser Regelung ist die zutreffende Überlegung, daß ich die Wahrung der Grenzen der Zulässigkeit der Datenverarbeitung im Auftrag sowie die Einhaltung der bei der Datenverarbeitung zu beachtenden Vorschriften über den Datenschutz nicht kontrollieren kann, wenn mir die Auftragserteilung und ihre vertragliche Ausgestaltung unbekannt bleiben. Deshalb ist auch der Begriff des Unterrichtens in § 11 Abs. 3 Satz 3 Bbg DSG dahingehend zu verstehen, daß die Unterrichtung über die Beauftragung sämtliche für die datenschutzrechtliche Beurteilung der Datenverarbeitung im Auftrag erforderlichen Angaben enthalten muß.

  Unverständlich ist vor dem Hintergrund dieses Normzwecks, weshalb die gesetzliche Regelung in § 11 Bbg DSG keine Verpflichtung zur Unterrichtung meiner Behörde für den Fall vorsieht, daß eine öffentliche Stelle im Land Brandenburg mit der Datenverarbeitung beauftragt wird. Derzeit bin ich darauf angewiesen, diese Informationen den Dateienregistermeldungen zu entnehmen.

1.2.1.4 Die Praxis der Datenverarbeitung im Auftrag öffentlicher Stellen in Brandenburg

Ein genauer Sachstandsbericht zur Praxis der Datenverarbeitung im Auftrag öffentlicher Stellen im Land Brandenburg und insbesondere zum Stand der Anpassung bereits bestehender Auftragsverhältnisse an die gesetzliche Regelung in § 11 Bbg DSG gem. § 40 Abs. 6 Bbg DSG ist nicht möglich. Das Innenministerium hat mir auf Anfrage mitgeteilt, daß dort noch nicht einmal für den Bereich des Meldewesens ersichtlich ist, welche Stellen im Land Brandenburg welche Daten im Auftrag durch welche Stellen verarbeiten lassen.

Nach meinem bisherigen Kenntnisstand muß ich davon ausgehen, daß die Problematik der Datenverarbeitung im Auftrag und insbesondere die gesetzlichen Regelungen dazu im Brandenburgischen Datenschutzgesetz im Land Brandenburg weitgehend unbekannt sind. Ein Problembewußtsein habe ich insoweit bislang überhaupt nur bei der Aufsichtsbehörde für den Datenschutz feststellen können, durch die ich in einigen Fällen von einer Auftragserteilung an nicht-öffentliche Stellen informiert wurde, die davon gemäß ihrer Verpflichtungen nach § 38 BDSG die Aufsichtsbehörde für den Datenschutz unterrichtet hatten.

Meine Behörde ist bislang durch die auftragserteilenden öffentlichen Stellen gem. § 11 Abs. 3 Satz 3 Bbg DSG in keinem Fall unterrichtet worden. Dabei habe ich insbesondere infolge einer Anfrage eines an der kommunalen Datenverarbeitung im Auftrag maßgeblich beteiligten Datenverarbeitungsunternehmens feststellen müssen, daß es Städte gibt, die in wesentlichen Bereichen ihrer Verwaltung die Verarbeitung personenbezogener Daten ganz oder teilweise durch private Auftragnehmer durchführen lassen. Nach meinen bisherigen

---

[9] BVerfGE 65, 1 (46)

Informationen muß ich davon ausgehen, daß die Kommunen dabei auch in den Verfahren "Personal", "Soziales", "Steuer", "Ausländerwesen" und "Meldewesen" personenbezogene Daten im Auftrag verarbeiten lassen. Die von mir angesprochenen Kommunen scheinen sich der fehlenden Rechtmäßigkeit ihres Vorgehens allerdings nicht bewußt zu sein.

Obwohl mir bislang nur bei drei kreisfreien und zwei kreisangehörigen Städten erste Informationen zu einer Datenverarbeitung im Auftrag vorliegen, gehe ich aufgrund entsprechender Hinweise davon aus, daß kaum eine Kommunalverwaltung die Verarbeitung personenbezogener Daten vollständig und einschließlich der Wartung ihrer ADV-Systeme selbst durchführt und daß vielfach die Datenverarbeitung im Auftrag noch nicht einmal innerhalb Brandenburgs erfolgt, sondern bei Niederlassungen der Auftragnehmer in anderen Bundesländern. Auch von anderen öffentlichen Stellen ist mir bekannt, daß diese in bestimmten Bereichen personenbezogene Daten im Auftrag verarbeiten lassen.

Nach meinen bisherigen Erfahrungen ist die Praxis der Datenverarbeitung im Auftrag öffentlicher Stellen im Land Brandenburg als nicht datenschutzgerecht, sondern im Gegenteil als rechtswidrig zu beurteilen. Zum einen ist die praktizierte Verarbeitung personenbezogener Daten im Auftrag in bestimmten Bereichen bereits grundsätzlich unzulässig. Zum anderen trägt die Praxis der Datenverarbeitung im Auftrag den insoweit eindeutigen Verpflichtungen nach § 11 Bbg DSG nicht in der erforderlichen Weise Rechnung. Letzteres führt insbesondere dazu, daß ich meine Aufgaben der datenschutzrechtlichen Beratung und Kontrolle der datenverarbeitenden öffentlichen Stellen im Land Brandenburg nicht sachgerecht erfüllen kann, da es mir an den dazu erforderlichen Informationen fehlt und die personellen Kapazitäten meiner Behörde eine ohnehin kaum denkbare umfassende Kontrolle sämtlicher Verwaltungen mit dem Ziel der eigenständigen Informationsgewinnung nicht zulassen. Soweit ich bislang mit der dargestellten Problematik der Datenverarbeitung im Auftrag an einzelne Kommunen herangetreten bin, war diese den verantwortlichen Verwaltungsleitungen nicht bekannt.

Die derzeitige Praxis bei der Datenverarbeitung im Auftrag soll anhand der nachfolgenden *Einzelfälle* gezeigt werden:

- Nach Auskunft des Ministeriums des Innern hatte dort eine Stadtverwaltung angefragt, ob es sich bei dem Erwerb eines ADV-Systems für den Bereich des Meldewesens von einem privaten Datenverarbeitungsunternehmen um eine zustimmungspflichtige Datenverarbeitung im Auftrag handelt. Durch entsprechende Informationen von seiten des Datenverarbeitungsunternehmens ist mir bekannt, daß die Datenverarbeitung im Bereich des Meldewesens im Auftrag der betreffenden Kommune durch das Unternehmen erfolgt. Dem Ministerium war in der Anfrage jedoch ein völlig anderer Sachverhalt dargestellt worden.

- Ein Landkreis läßt durch das Amt für Datenverarbeitung eines nordrhein-westfälischen Landkreises in den Verfahren "Personal", "Kassen- und Haushaltswesen", "Grundbesitzabgaben" und "Abfallbehälterkataster" personenbezogene Daten im Auftrag verarbeiten. Bekannt wurde mir dies durch die Eingabe einer Bürgerin, die auf den Fluren des Landratsamtes über die Kartons mit den - einsehbaren - Müllgebührenbescheiden gestolpert war.

- Eine kreisfreie Stadt hat mir durch ihre behördliche Datenschutzbeauftragte mitteilen lassen, auf die Lohn- und Gehaltsabrechnung, die die Stadt bereits seit 1991 im Auftrag durch eine nicht-öffentliche Stelle durchführen lasse, könne § 11 Abs. 3 des erst 1992 in Kraft getretenen Brandenburgischen Datenschutzgesetzes keine Anwendung finden. Die Stadt sieht deshalb keine Veranlassung, ihre Praxis der Datenverarbeitung im Auftrag zu überprüfen.

- Nachdem ich davon aus der Presse Kenntnis erhalten hatte, teilte mir das Ministerium des

Innern erst auf meine Nachfrage mit, daß in der Vergangenheit von den Polizeipräsidien private Fotolabors mit der Entwicklung von Filmen im Zusammenhang mit der Verfolgung und Ahndung von Ordnungswidrigkeiten gem. § 24 Straßenverkehrsgesetz (StVG)[10] beauftragt waren. Seit der Einrichtung und Inbetriebnahme polizeieigener Fotolabors wird die Entwicklung von Filmen ausschließlich in den Behörden vorgenommen.

- Ein privates Unternehmen betreibt eine Aktenvernichtungsanlage, in der es auch Akten mit personenbezogenen Daten für öffentliche Stellen vernichtet. Darüber wurde ich lediglich von der Aufsichtsbehörde für den Datenschutz unterrichtet.

- Eine Wirtschaftsförderungsgesellschaft verarbeitet als Dienstleistungsunternehmen personenbezogene Daten im Auftrag eines Landkreises. Auch davon habe ich Kenntnis nur durch eine Mitteilung der Aufsichtsbehörde erhalten. Weitere Informationen liegen mir nicht vor.

- Die Landesagentur für Struktur und Arbeit (LASA), eine GmbH, bei der das Land Brandenburg Anteilseigner zu 100 % ist, hat mich darüber informiert, daß sie im Auftrag des Ministeriums für Arbeit, Gesundheit, Soziales und Frauen "die Weiterbildungsdatenbank Brandenburg verarbeite". Mir ist nicht bekannt, ob der LASA zur Erfüllung ihrer eigenen Aufgaben dazu personenbezogene Daten übermittelt werden oder ob dabei eine Verarbeitung personenbezogener Daten im Auftrag erfolgt.

- Ein Wachschutzunternehmen wollte auch öffentlichen Stellen im Land Brandenburg die Aufbewahrung von Aktenbeständen anbieten und erkundigte sich bei mir nach der datenschutzrechtlichen Zulässigkeit einer solchen Datenverarbeitung. Ich kann nicht ausschließen, daß öffentliche Stellen im Land Brandenburg zwischenzeitlich von einem solchen Angebot Gebrauch gemacht haben.

1.2.1.5 Handlungsbedarf

Unverkennbar ist die Entwicklung zu einer fortschreitenden Privatisierung der Datenverarbeitung der öffentlichen Stellen. In vielen Bereichen steht dem nach Maßgabe der klaren verfassungsrechtlichen Vorgaben das Grundrecht der betroffenen Bürger auf informationelle Selbstbestimmung entgegen. Deshalb werden die Verwaltungen in den Stand gesetzt werden müssen, die Verarbeitung personenbezogener Daten auch selbst wirtschaftlich und sachgerecht durchführen zu können. Dazu sind aus datenschutzrechtlicher Sicht zunächst folgende Maßnahmen erforderlich:

- *Vom Gesetzgeber* ist eine normenklare und sachgerechte Neuregelung der Datenverarbeitung im Auftrag im Brandenburgischen Datenschutzgesetz zu fordern. Dabei sollten auch die Besonderheiten der Wartung und Fernwartung (s. unter 7.2.3.1) berücksichtigt werden. Die Erforderlichkeit von Übergangsregelungen wird zu prüfen sein.

- *Die Landesregierung* wird insbesondere die Kommunen bei der Entwicklung datenschutzgerechter Lösungen unterstützen müssen, deren Finanzieruzng - z.B. bei einer Errichtung kommunaler Datenverarbeitungszentren - Mittel in einer Größenordnung erfordern wird, die die Kommunen schwerlich aus eigener Kraft werden aufbringen können.

- *Die einzelnen öffentlichen Stellen* müssen zunächst erst einmal eine Bestandsaufnahme sämtlicher Verarbeitungen personenbezogener Daten in ihrem Auftrag leisten, bei deren

---

10 vom 19. Dezember 1952, BGBl. I, S. 837, zuletzt geänd. am 15. Dezember 1990, BGBl. I, S. 2804

datenschutzrechtlicher Beurteilung mir Gelegenheit zur Stellungnahme gegeben werden muß.

Es ist darauf hinzuweisen, daß es insoweit nicht lediglich um eine Beachtung verfahrensmäßiger Beteiligungsrechte eines Landesbeauftragten für den Datenschutz geht, sondern vor allem auch um die Frage des Informationszugangs des Parlaments im Hinblick auf regelungs- und kontrollbedürftige Sachverhalte.

1.2.2 Dateienregistermeldungen

Aufgrund des § 24 Abs. 1 Bbg DSG wird jede speichernde Stelle verpflichtet, meiner Behörde die Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung zu melden, wobei die in der Dateienregisterverordnung Brandenburg (DRegVOBbg)[11] veröffentlichten Formblätter zu verwenden sind. Die Registermeldungen müssen meiner Behörde bei Beginn des Anlegens der automatisiert geführten Dateien vorgelegt werden. Besonders weise ich darauf hin, daß diese Meldepflicht jedoch auch für alle früher angelegten Dateien gilt.

Im Regelfall gibt jede speichernde Stelle für jede von ihr geführte Datei eine Meldung ab. Nutzen mehrere Stellen die gleichen Programmsysteme mit dem gleichen Dateiaufbau für gleichartige Aufgaben, so können diese ausnahmsweise zur Vereinfachung des Verfahrens - nach vorheriger Abstimmung mit meiner Dienststelle - die Meldungen zum Dateienregister in zusammengefaßter Form vornehmen. Da - bis auf wenige Ausnahmen - das Dateienregister gem. § 24 Abs. 2 Bbg DSG bei berechtigtem Interesse von jedermann eingesehen werden kann, ist darauf zu achten, daß die betreffenden Eintragungen in den Formularen allgemeinverständlich sind und keine Angaben enthalten, die der Geheimhaltung unterliegen.

Zur Unterstützung der Dienststellen beim Ausfüllen der Meldeformulare wurde in der von meiner Behörde herausgegebenen Informationsschrift "Sicherheit am PC und in lokalen Netzen - Dateienregister" eine Ausfüllanleitung und die erforderlichen Formulare als Kopiervorlagen aufgenommen; diese kann jederzeit bei mir angefordert werden. Trotzdem gehen bei mir in der Behörde immer wieder Meldungen ein, die nicht den geforderten Formvorschriften entsprechen oder in denen wichtige Grundinformationen, wie z. B. Dateibezeichnung, Rechtsgrundlagen, betroffener Personenkreis, fehlen. Bei weitem sind noch nicht alle speichernden Stellen ihrer Meldepflicht nachgekommen. Bisher habe ich bei Versäumnissen in der Regel von Beanstandungen abgesehen, um den Verwaltungen eine angemessene Frist zur Realisierung der Dateienregistermeldungen einzuräumen. Zwei Jahre nach Inkrafttreten des Brandenburgischen Datenschutzgesetzes wird jedoch die Erfüllung der gesetzlichen Verpflichtung gem. § 24 Abs. 1 Bbg DSG künftig mit allem Nachdruck einzufordern sein.

Die teilweise angeführten Argumente, daß bei der Nutzung von Fremdsoftwaresystemen der erforderliche Aufbau der Datenbankdateien nicht bekannt und deshalb eine Dateienregistermeldung unmöglich sei, kann ich nicht akzeptieren. Vielmehr sollten die Vertragsbedingungen beim Kauf neuer Softwaresysteme so gestaltet werden, daß die Dokumentationsunterlagen alle zur Dateibeschreibung erforderlichen Informationen enthalten. Für bereits vorhandene Systeme, bei denen es mit vertretbarem Aufwand nicht möglich ist, die Informationen der einzelnen Datenbankdateien zu erhalten, können die Dateibeschreibungen ausnahmsweise nach vorheriger Abstimmung mit mir anhand der Datenbank vorgenommen werden.

In diesem Zusammenhang ist darauf hinzuweisen, daß die Bestellung entsprechend

---

11 vom 19. November 1992, GVBl. II, S. 726

fachkundiger behördlicher Datenschutzbeauftragter sicherlich ein geeignetes Mittel zu sachgerechten Aufgabenerfüllung wäre. Dies sollte vom Gesetzgeber durch eine entsprechende Regelung im Brandenburgischen Datenschutzgesetz klargestellt werden.

1.2.3 Besondere Beziehung zum Land Berlin

Im Berichtszeitraum sind weitere Staatsverträge zwischen den Ländern Berlin und Brandenburg in Kraft getreten. Die rechtsfähigen Anstalten des öffentlichen Rechts "Feuersozietät Berlin Brandenburg" und "Öffentliche Lebensversicherung Berlin Brandenburg"[12] haben ihren Sitz in Berlin und Potsdam. Dagegen ist der Sitz der "Zentralen Adoptionsstelle Berlin-Brandenburg"[13] in Oranienburg bzw. der "Akademie der Künste" (bereits 1992 gegründet) in Berlin. Die zugrundeliegenden Staatsverträge enthalten keine datenschutzrechtlichen Regelungen in bezug auf den Geltungsbereich von Gesetzen und Kontrollzuständigkeiten. Damit kein rechtsfreier Raum entsteht, werden deshalb die Datenschutzkontrollen in den genannten öffentlichen Einrichtungen in enger Abstimmung mit dem Berliner Datenschutzbeauftragten erfolgen.

Hinzuweisen ist ferner auf den im Oktober 1993 vorgelegten Zwischenbericht zum Staatsvertrag der Länder Berlin und Brandenburg über die Bildung eines gemeinsamen Bundeslandes (Neugliederungsstaatsvertrag). Danach gehört das Datenschutzrecht zu den Rechtsvorschriften, die vorrangig in beiden Ländern harmonisiert werden sollen. Unabhängig davon, ob eine Vereinigung der beiden Länder zustande kommt, hätte dies bereits praktische Bedeutung für die oben angeführten und zusätzlich geplanten gemeinsamen Zweiländereinrichtungen sowie länderübergreifenden Datensammlungen.

1.3 Schaffung einzelgesetzlicher Datenschutzregelungen im Land Brandenburg

Die Entwicklung des Datenschutzes läßt sich sehr genau an den im Berichtszeitraum in Kraft getretenen oder im Entwurf vorliegenden bereichsspezifischen Datenschutzregelungen ablesen. Das Brandenburgische Datenschutzgesetz schreibt in § 27 vor, daß dies in jedem Tätigkeitsbericht "in einem gesonderten Teil" zu geschehen hat.

Eine Gewichtung der einzelgesetzlichen Datenschutzregelungen halte ich an dieser Stelle nicht für erforderlich; derzeit stellt die Verabschiedung eines jeden Gesetzes für die noch immer im Aufbau befindliche Verwaltung im Land Brandenburg eine große Hilfestellung dar. Die nachfolgende Auflistung der Einzelgesetze erfolgt nach dem Ressortprinzip:

- Personalausweisgesetz (s. unter 3.4.2),
- Entwurf eines Statistikgesetzes (s. unter 3.9.3),
- Entwurf eines Katastrophenschutzgesetzes (s. unter 3.10),
- Archivgesetz (s. unter 6.1),
- Entwurf eines Landesgleichstellungsgesetzes (s. unter 7.1),
- Entwurf eines Gesundheitsdienstgesetzes (s. unter 7.2.2.1),
- Landeskrankenhausgesetz (s. unter 7.2.3.1),
- Entwurf eines Psychisch-Kranken-Gesetzes (s. unter 7.2.3.2) und
- Hebammengesetz (s. unter 7.2.5).

Auch in Brandenburg werden unter der Zielvorgabe, möglichst "schlanke Einzelgesetze" zu

---

12

13 vom 16. Juni 1993, GVBl. I, S. 216
vom 18. März 1994, GVBl. I, S. 79

verabschieden, die Mehrheit der spezialgesetzlichen Datenschutzregelungen auf die Ebene von Rechtsverordnungen verlagert bzw. anstelle der erforderlichen materiell-rechtlichen Regelungen bloße Verwaltungsvorschriften erlassen bzw. vorgelegt. Dabei handelt es sich u. a. um folgende Vorschriften:

- Rundschreiben des MdI zur weiteren Verwendung von Daten der ehemaligen DDR-Volkspolizeikreisämter (VPKA) Bereich Meldewesen (s. unter 3.1.3),
- Erste Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (s. unter 3.4.1),
- Errichtunganordnungen gem. § 48 VGPolGBbg (s. unter 3.6.2.3),
- Entwurf einer Verwaltungsvorschrift über die Aufnahme von Schülern und Schülerinnen in die Grundschule (s. unter 5.1.1),
- Entwurf einer Verwaltungsvorschrift über die Bestellung und Tätigkeit von Beratungslehrerinnen und Beratungslehrer (s. unter 5.1.2),
- Entwurf einer Verwaltungsvorschrift über die Schulpsychologische Beratung (s. unter 5.1.3),
- Entwurf einer Verwaltungsvorschrift über wissenschaftliche Untersuchungen in Schulen (s. unter 5.1.4),
- Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen (s. unter 5.1.5),
- Weitere Verwaltungsvorschriften im Schulbereich (s. unter 5.1.6),
- Runderlaß zu Hinweisen zur Meldung, Aufbewahrung und Nutzung von Unterlagen, Zentralkarteien, Zentralregistern und Zentraldateien mit patientenbezogenem (medizinischem) Inhalt aus ehemaligen Gesundheitseinrichtungen der DDR (s. unter 7.2.1),
- Berufsordnung der Landesärztekammer Brandenburg (s. unter 7.2.4),
- Berufsordnung für Hebammen und Entbindungspfleger (s. unter 7.2.6),
- Entwurf einer Datenschutzverordnung für den Bereich Immissionsschutz (s. unter 8.3),
- Verordnung über Beiträge an die Tierseuchenkasse des Landes Brandenburg (s. unter 9.2),
- Pflanzenschutzsachkundeverordnung (s. unter 9.4) und
- Erlaß einer Verwaltungsvorschrift über die Errichtung und Benutzung von dienstlichen Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg (s. unter 11.1).

Diese aufgezeigte Entwicklung erscheint im Hinblick auf § 41 Abs. 2 Bbg DSG nicht unproblematisch. Denn dieser bezweckt mit der Forderung nach bereichsspezifischen Regelungen die konkrete Ausformung des Grundrechts auf informationelle Selbstbestimmung durch den Gesetzgeber selbst. Durch die derzeitige Vorgehensweise wird es der Verwaltung praktisch ermöglicht, ohne Einschaltung des Parlaments datenschutzrechtliche Maßstäbe zu setzen und diese jederzeit selbst abzuändern.

1.4 Datenschutz vor dem Hintergrund rasanter technisch-organisatorischer Entwicklungen

Um meine Beratungsaufgabe gem. § 23 Abs. 2 Bbg DSG gegenüber der öffentlichen Verwaltung durch Empfehlungen und Hinweise zur Verbesserung des Datenschutzes rechtzeitig erfüllen zu können, ist es unerläßlich, die neuesten informationstechnischen Entwicklungstendenzen hinsichtlich der Folgen für die Gewährleistung des Datenschutzes aufmerksam zu verfolgen. Was heute in den technischen Labors entwickelt oder bereits in Feldversuchen erprobt wird, kann morgen schon zu Beschaffungsmaßnahmen bei öffentlichen Stellen führen und Risiken für das Recht auf informationelle Selbstbestimmung hervorrufen, denen durch gesetzliche Regelungen oder geeignete technisch-organisatorische Maßnahmen entgegengewirkt werden muß.

Die bekannten Entwicklungstendenzen in der Informationstechnik schreiten seit mehreren

Jahren mit unvermindertem Tempo voran. Sie sind besonders durch folgende Trends gekennzeichnet:

- Die zunehmende Miniaturisierung der Hardware hat dazu geführt, daß tragbare Computer (Laptops) heute Leistungsparameter erreichen, die vor wenigen Jahren noch Großrechnern vorbehalten waren. Kleine Notebook-Computer ermöglichen die Mitnahme automatisiert geführter Datenbanken in der Hand- oder Westentasche. Damit ist die Datenverarbeitung heute längst nicht mehr ortsgebunden und mit neuen Gefahren für den Datenschutz und die Sicherheit der Daten verbunden (s. Anlage 1).

- Die laufende Verbesserung des Preis-Leistungs-Verhältnisses bei Hard- und Software ermöglicht ihre Anwendung für immer mehr Einsatzgebiete. Nicht nur die meisten Behörden sind heute finanziell in der Lage, sich Computer mit erstaunlicher Leistungsfähigkeit zu kaufen, sondern auch in vielen Privathaushalten gehören sie bereits zur Standardausstattung. Dabei werden diese Privatcomputer durchaus nicht nur zur privaten Lebensführung genutzt, sondern öffentlich Bedienstete versuchen auch Teile ihrer dienstlichen Aufgaben auf ihren häuslichen Computer zu verlagern. Gefahren für den Datenschutz liegen hier besonders darin, daß sich dieser Personenkreis sowohl einer effektiven Kontrolle durch ihre Dienststelle als auch durch meine Behörde entzieht.

- Die Vernetzung von Personalcomputern zu lokalen Netzen (LAN), um gemeinsame Ressourcen zu nutzen, Ausfälle zu überbrücken oder zusätzliche Kommunikationsmöglichkeiten zu erschließen, ist heute zur Selbstverständlichkeit geworden. Lokale Netze werden ihrerseits über größere Entfernungen hinweg zu Weitverkehrsnetzen (WAN) verknüpft. Das für das Land Brandenburg konzipierte Datenvermittlungssystem und der beabsichtigte Datenaustausch über den Telekommunikationsverbund der obersten Landesbehörden sind typische Beispiele dafür. Mit der zunehmenden Ausbreitung solcher Netze entstehen zusätzliche datenschutzrelevante Risiken für ihre Verfügbarkeit und Integrität; die Sicherheit dieser Systeme gewinnt angesichts ihrer besonderen Verletzlichkeit erhöhte Bedeutung. Die im Zusammenhang mit der Vernetzung aus Rationalisierungsgründen neu aufgetretenen Fragen der Fernwartung von Hard- und Software werden von unüberschaubaren Risiken für die Vertraulichkeit und Integrität der Systeme und Daten begleitet.

- Mit leistungsfähigen Generierungswerkzeugen und neuartigen Programmiersprachen werden heute immer komplexere und preisgünstigere Standardsoftwaresysteme erstellt, die die höheren Rechengeschwindigkeiten und fast unbegrenzten Speichermöglichkeiten für neue Anwendungen erschließen. Oft werden dabei aus der Sicht des Datenschutzes dringend erforderliche Sicherheitsfunktionen nicht vorgesehen und müssen nachträglich teuer hinzugekauft werden.

- Chipkarten ermöglichen es heute, technisch auf kleinstem Raum komplette Computer mit umfangreichen Speichermöglichkeiten unterzubringen und darauf beispielsweise die gesamte Krankengeschichte eines Patienten einzutragen. Gravierend sind die Gefahren für das Recht auf informationelle Selbstbestimmung besonders dann, wenn es sich um personenbezogene Daten handelt, die gem. § 203 Strafgesetzbuch (StGB)[14] einem Berufs- oder besonderen Amtsgeheimnis unterliegen (s. Anlage 16).

- In modernen ISDN-Telekommunikationsanlagen übernehmen heute Computersysteme die Vermittlung und Registrierung der Gespräche. Sie können aber neben der erforderlichen Gebührenerfassung auch äußerst kritische Leistungsmerkmale realisieren und das gesamte

---

14 i. d. Fassung der Bekanntmachung vom 10. März 1987, BGBl. I, S. 945, ber. S. 1160

Kommunikationsverhalten der Gesprächsteilnehmer überwachen. Die neuen technischen Möglichkeiten beinhalten damit neben ihren Vorteilen auch erhebliche Gefahren für das Fernmeldegeheimnis (s. Anlage 6).

1.4.1 ISDN-Telefonanlagen

1.4.1.1 Bestandsaufnahme der gegenwärtigen Situation

Im Berichtszeitraum ersetzten viele öffentliche Stellen ihre meist veralteten analogen internen Telefonanlagen durch neue digitale ISDN-Telefonanlagen. Diese computergesteuerten Systeme bieten mit ihren neuen Leistungsmerkmalen dem Nutzer jedoch nicht nur schnelle effektive und komfortable Kommunikationsmöglichkeiten, sondern bergen auch ungeahnte und oft unterschätzte Risiken für die Rechte des einzelnen, die seine Privatsphäre und sein Sozialverhalten erheblich beeinträchtigen können. Die durch Software bestimmten Leistungsmerkmale lassen sich schnell und vom Nutzer unbemerkt bis auf die einzelnen Arbeitsplätze genau festlegen und so den spezifischen Kommunikationsforderungen anpassen. Dadurch entstehen komplexe technologische Systeme, deren volles Leistungspotential meist nur noch Systemspezialisten bekannt ist und deren Eigenschaften innerhalb kürzester Zeit dauerhaft oder temporär grundlegend verändert werden können, wobei in der Regel davon auszugehen ist, daß dabei auch unrechtmäßige Konfigurationen und Aktionen möglich sind.

In den Vermittlungs- und Gebührencomputern können umfangreiche Sammlungen sensibler personenbezogener Daten entstehen, die sich auch zur Verhaltens- und Leistungskontrolle der Mitarbeiter eignen und Hinweise auf das Kommunikationsverhalten der Gesprächsteilnehmer geben können. Davon werden nicht nur die Grundrechte der Beschäftigten selbst berührt, sondern auch die Rechte Dritter, die anrufen oder angerufen werden. Unter den Schutz des Fernmeldegeheimnisses fallen nicht nur die Inhalte der geführten Gespräche, sondern auch die näheren Umstände des Fernmeldeverkehrs, insbesondere wer wann mit wem mittels welchen Mediums kommuniziert hat. Unter diesem Gesichtspunkt und in Anbetracht der Tatsache, daß von dienstlichen Telefonapparaten auch private Gespräche mit Zustimmung der Dienststelle geführt werden, sind die Verbindungsdaten, falls sie über das Gesprächsende hinaus für Zwecke der Kontrolle und Gebührenerfassung gespeichert werden sollen, als besonders sensibel einzustufen.

1.4.1.2 Eigenschaften von ISDN-Anlagen

Im folgenden soll aus der Sicht des Datenschutzes auf einige kritische Leistungsmerkmale von ISDN-Telefonanlagen eingegangen werden (s. Anlage 6):

- *Rufnummernanzeige*

  Die Rufnummer des Anrufers, bei manchen internen Anlagen auch dessen Name, wird im Display des Angerufenen bereits vor Gesprächsbeginn und ggf. während des gesamten Gespräches angezeigt. So kann einerseits die Annahme des Gespräches davon abhängig gemacht werden, andererseits besteht die Gefahr, daß unbeteiligte Dritte über die Anzeige erfahren, mit wem telefoniert wird. Die fehlende Anonymität des Anrufers beeinflußt die Vertraulichkeit voraussetzende Tätigkeit bestimmter Behörden. Besonders betroffen sind davon Beratungsstellen, Sozialämter, Personalräte und behördliche Datenschutzbeauftragte. Nach der EURO-ISDN erhält deshalb der Anrufer durch eine einfache technische Vorrichtungen die Möglichkeit, für jedes einzelne Gespräch zu entscheiden, ob er seine Rufnummer beim Angerufenen anzeigen lassen will oder nicht.

- *Frei sprechen und laut hören*

  In Telefonapparaten mit Freisprecheinrichtung sind ein Mikrofon und ein Lautsprecher

eingebaut. Ohne den Hörer zu benutzen, kann man so den Kommunikationspartner im gesamten Raum hören und über das Mikrofon direkt mit ihm sprechen. Die Nutzung dieser Einrichtung kann dazu führen, daß ohne das Wissen der Kommunikationspartner andere Personen im Raum - ggf. auch in den Nebenräumen oder auf den Fluren - Zeugen von Gesprächen werden. Der Gesprächspartner sollte deshalb vor jeder Nutzung der Freisprecheinrichtung grundsätzlich darauf hingewiesen werden. Darüber hinaus sollten interne Anlagen so gestaltet sein, daß sie dem anderen Partner die Nutzung der Freisprecheinrichtung in geeigneter Form signalisieren.

- *Anrufumleitung und Nachziehen*

Vorübergehend können alle Gespräche für eine Nebenstelle direkt auf eine andere umgeleitet werden. Die Umleitung kann von der eigenen, von einer fremden Nebenstelle oder vom Vermittlungsplatz aus eingeleitet werden. Zusätzlich besteht die Möglichkeit, die eigene Nebenstelle für das Nachziehen freizugeben, dann die Umleitung von der Zielnebenstelle zu aktivieren sowie bei einem erneuten Platzwechsel auch an eine dritte Nebenstelle weiterzugeben und so alle ankommenden Gespräche nachzuziehen. Die Nutzung dieser Einrichtung bringt für den Anrufer den Nachteil, daß er stets damit rechnen muß, mit beliebigen anderen Teilnehmern als den gewünschten verbunden zu werden. Dadurch können Regelungen zur innerbehördlichen Abschottung durchbrochen und vertrauliche Gesprächskontakte Dritten bekannt werden. Es besteht auch die Gefahr, daß sich ein Anrufer plötzlich ohne sein Wissen in eine bestehende Konferenzschaltung begibt. Daher sollte die Weiterleitung eines Anrufes an einen anderen als den gewählten Anschluß dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau noch abbrechen kann.

- *Konferenzschaltung*

Hierbei können herstellerabhängig eine variable Anzahl von - auch externen - Teilnehmern gleichzeitig miteinander kommunizieren. Einen besonderen Status besitzt der Teilnehmer, der die Konferenz einberuft, der sogenannte Konferenzleiter. Er kann sich selbst zeitweise auskoppeln, die Konferenzleiterschaft weitergeben und Teilnehmer zu- bzw. abschalten. Dabei besteht die Gefahr, daß ein externer Teilnehmer gegen seinen Willen oder sein Wissen in eine bestehende Konferenz einbezogen wird, ohne daß er die Identität und die Anzahl der Konferenzteilnehmer kennt. Für die sich bereits in einer Konferenzschaltung befindlichen Personen besteht die Gefahr, daß sie die Hinzunahme weiterer Teilnehmer nicht bemerken bzw. gegen ihren Willen nicht erfahren. So ist z. B. die Zuschaltung eines "anonymen Zeugen", der dann, ohne echter Konferenzteilnehmer zu sein, den Gesprächsverlauf verfolgen kann, denkbar und stellt eine besondere Gefährdung für die Vertraulichkeit der Kommunikation dar. Konferenzschaltungen sollten deshalb für außenstehende Dritte immer angekündigt werden, bevor sie an der Konferenz teilnehmen. Sie können sich dann darauf einstellen und ggf. die Teilnahme an einer Konferenzschaltung ablehnen. Auch den bereits an einer Konferenzschaltung Beteiligten muß die Hinzunahme weiterer Personen angekündigt werden, und der Konferenzleiter sollte die neuen Teilnehmer erst dann zuschalten, wenn kein Veto vorliegt. Die Abmeldung aus einer bestehenden Konferenzschaltung sollte für jeden Teilnehmer zu jeder Zeit möglich sein und den verbleibenden Konferenzteilnehmern mitgeteilt werden.

- *Automatischer Rückruf und Anrufliste*

Kommt ein gewünschtes Gespräch wegen besetzter Nebenstelle ("Besetztfall") oder weil der gewünschte Partner nicht abhebt ("Freifall") nicht zustande, so kann der Anrufer einen automatischen Rückruf veranlassen. Im Besetztfall wird dann der Verbindungsaufbau automatisch eingeleitet, sobald der gewünschte Teilnehmer das vorherige Gespräch beendet hat. Im Freifall wird die Verbindung hergestellt, sobald das System erkennt, daß der Teilnehmer nun wieder erreichbar ist.

Dadurch, daß mehrere Rückrufe auf eine Nebenstelle gerichtet sein können und die Anlage die Verbindungen beim automatischen Rückruf selbständig herstellt, kann ein Teilnehmer gegen seinen Willen dazu gezwungen sein, längere Zeit Rückrufe abzuarbeiten. Der Rückruf im Besetztfall kann zur Kontrolle des Kommunikationsverhaltens mißbraucht werden (Dauer von Gesprächen ermitteln). Wesentlich bedenklicher ist jedoch der Rückruf im Freifall, der wirksame Anwesenheitskontrollen ermöglicht. Dies kann besonders zu morgendlichen Arbeitsbeginnkontrollen verwendet werden, falls man die Rückrufwünsche am Vorabend kurz nach Arbeitsende einträgt.

Eine vernünftige Alternative zum automatischen Rückruf stellt die Anrufliste dar. Ein Anrufer kann beim Angerufenen auf eigenen Wunsch einen Eintrag in dessen Anrufliste vornehmen und der Angerufene kann dann über Notwendigkeit und Zeitpunkt eines Rückrufes selbst entscheiden.

- *Aufschalten*

Das Aufschalten war früher hauptsächlich für Vermittlungsplätze üblich, wo es zur Ankündigung dringender Gespräche genutzt wurde. Heute besteht bei den meisten Anlagen dagegen die Möglichkeit, daß diese Funktion vom Systemadministrator für jeden Telefonapparat freigegeben wird. Für Teilnehmer einer bestehenden Kommunikationsverbindung besteht die Gefahr, daß gegen ihren Willen die Vertraulichkeit ihrer Verbindung durch das Aufschalten gestört wird. Das gilt auch für den Fall, daß das Aufschalten einer dritten Person durch einen warnenden Aufschaltton den Gesprächsteilnehmern signalisiert wird. Das Aufschalten sollte nur für Vermittlungsplätze freigegeben werden. Es stellt sich die Frage, ob durch die sinnvolle Verwendung des Anklopfens das Aufschalten nicht überflüssig wird. Das Anklopfen ließe dem Betroffenen die Wahl, ob er überhaupt ein weiteres Gespräch entgegennehmen möchte. Über das Makeln in Verbindung mit dem Anklopfen bliebe auch die Vertraulichkeit des bestehenden Gesprächs gewährleistet.

- *Direktansprechen*

Durch Nutzung des Direktansprechens kann ein Angerufener, der über einen Apparat mit Lauthören und Freisprechen verfügt, wie bei einer Gegensprechanlage direkt angesprochen werden, ohne daß er das Gespräch erst annehmen muß. Dabei werden Mikrophon und Lautsprecher der Freisprechanlage des Angerufenen vom Anrufer aktiviert. Das Direktansprechen eignet sich zum Abhören von Räumen und sollte deshalb vermieden werden. Trotz des in der Regel realisierten Ansprechtones ist die Gefahr des Abhörens eines Raumes, beispielsweise in Großraumbüros, gegeben, besonders dann, wenn der Angerufene sich im Augenblick des Ansprechens nicht in unmittelbarer Nähe seines Telefonapparates befindet oder der Ton, z. B. aufgrund der Geräuschkulisse, nicht wahrgenommen wird. Wird dieses Leistungsmerkmal eingesetzt, muß sich jeder auf Knopfdruck gegen das Direktansprechen schützen können (Direktansprechschutz). Beide Teilnehmer sollten für die Dauer der Verbindung optisch oder akustisch auf das eingeschaltete Mikrophon und auf den eingeschalteten Lautsprecher hingewiesen werden.

- *Drohanrufaufzeichnung*

Bei Drohanrufen handelt es sich um eine telefonische Androhung von Gewalt gegen Personen oder Sachen. Die Aufzeichnungsmöglichkeit von Drohanrufen wird mitunter in öffentlichen Einrichtungen gefordert, um über die Analyse der Stimme eines Anrufers nachträglich die Personenidentifizierung vornehmen zu können. Dabei wird von einem erhöhten Schutzbedürfnis - besonders bei exponierten Dienststellen - ausgegangen. Das technische Verfahren beruht darauf, daß der gesamte Wortlaut aller an den Abfrageplätzen ankommenden externen Gespräche vorsichtshalber für einige Minuten in digitalen Speichern aufgezeichnet wird. Läßt sich ein Gespräch nach einer gewissen Zeit als

Drohanruf erkennen, kann durch Tastendruck der Vermittlungskraft das gerade anstehende Gespräch ab Gesprächsbeginn auf einen magnetischen Tonträger übertragen und damit gespeichert werden. Nach Beendigung eines Drohanrufes könnte unter Beachtung besonderer Sicherheitsmaßnahmen der Tonträger mit dem Gesprächsinhalt entnommen und den betreffenden Strafverfolgungsbehörden übergeben werden. Die bei diesen Verfahren praktizierte präventive Registrierung aller ankommenden Telefongespräche ist datenschutzrechtlich als bedenklich anzusehen. Eine Registrierung auf Knopfdruck im Einzelfall, d. h. wenn ein Anruf bereits als Drohanruf erkannt wurde, ist hingegen zulässig.

Die Zuweisung der geforderten Leistungsmerkmale auf die einzelnen Nebenstellen erfolgt bei kleineren Anlagen in der Regel mit der Inbetriebnahme durch einen Systemverantwortlichen der Lieferfirma. Nutzer größerer Anlagen verfügen dagegen meist über eigene Systemverantwortliche, die bei Bedarf eine Aktualisierung der Leistungsmerkmale vornehmen können. Durch geeignete technische und organisatorische Maßnahmen sind unberechtigte Veränderungen an den Systemparametern und den Leistungsmerkmalen der Telekommunikationsanlage zu verhindern. Eine Zwangsprotokollierung aller Aktivitäten des Systemadministrators erscheint unbedingt erforderlich. Ebenso wichtig ist, daß die Veränderung der Leistungsmerkmale nur von zwei genau bestimmten Personen vorgenommen werden kann (sog. Vier-Augen-Prinzip), um Fehlfunktionen weitestgehend auszuschließen.

Die zweifellos erforderliche, korrekte Zuordnung der Telefongebühren für von Dienstapparaten aus geführte Privatgespräche und die Verteilung der Kosten für die Dienstgespräche auf einzelne Kostenstellen führt häufig zu Auseinandersetzungen innerhalb der Behörden. Das hängt vor allem mit der gewählten Methode der Gebührendatenverarbeitung zusammen sowie damit, daß dabei mitunter umfangreiche sehr sensible Datenbestände über lange Zeiträume bei relativ geringen technischen Sicherheitsmöglichkeiten gespeichert werden. Verwaltungen, die zur Gebührenermittlung über längere Zeiträume alle Verbindungsdaten, d.h. detaillierte Angaben darüber, wer zu welcher Zeit mit welcher Zielrufnummer telefoniert hat, speichern, verletzen das Prinzip der Erforderlichkeit bei der Erhebung personenbezogener Daten. Sie verfügen damit über umfangreiche Datenbestände, die außer zur Gebührenabrechnung und Kostenkontrolle auch zur individuellen Leistungs- und Verhaltenskontrolle der Mitarbeiter genutzt werden können. Vorrangig sollte deshalb ein bei den meisten Herstellern von Telekommunikationsanlagen realisiertes sehr variables zweistufiges Verfahren zur Gebührenabrechnung zum Einsatz kommen. Bei diesem Verfahren werden in einer ersten Stufe die Verbindungsdaten am Gesprächsende kurzzeitig in einem Zwischenspeicher des Vermittlungscomputers abgelegt. In einem zweiten Schritt werden sie dann - in der Regel täglich - an den Gebührencomputer übermittelt und können in vielfältiger Weise selektiert und ergänzt werden. Die ursprünglich im Zwischenspeicher enthaltenen Verbindungsdaten sind nach der Übernahme in den Gebührencomputer zu löschen. Die Selektion der Daten ist so variabel, daß für jede einzelne Nebenstelle festgelegt werden kann, welche Daten in den Gebührencomputer übernommen werden sollen und welche nicht. Auch eine getrennte Behandlung von Dienst- und Privatgesprächen ist problemlos möglich.

Für Dienstgespräche sollten jeweils Gruppen von Nebenstellen (Abteilungen, Bereiche) einer gemeinsamen Kostenstelle zugeordnet werden, für die dann nur die Gebühreneinheiten zu speichern und fortlaufend zu addieren sind. So ist aber z.B. auch die Speicherung der kompletten Verbindungsdaten nur für besonders kostenintensive Gespräche denkbar. Grundsätzlich dürfen jedoch zum Zweck der Kostenkontrolle Daten nur soweit gespeichert werden, wie solche Kontrollen auch tatsächlich erforderlich sind. Falls überhaupt eine stichprobenartige Kontrolle von Dienstgesprächen als notwendig erachtet wird, so dürfen auch nur die Verbindungsdaten dieser Stichproben gespeichert werden. Dies erfordert allerdings, daß die Kriterien für die Stichproben z. B. durch einen Zufallsgenerator bereits im voraus (beispielsweise an jedem Monatsanfang) festgelegt werden. Für Privatgespräche sollten - je Nebenstelle frei wählbar - nur die Gesamtgebühren (spätere Reklamationen sind

dann nicht möglich) oder alle Verbindungsdaten mit der um die letzten drei Ziffern verkürzten Zielrufnummer gespeichert werden.

Da Telekommunikationsanlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren und häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Behörden Mitbestimmungsrechte der Personalräte gem. § 65 Nr. 2 Landespersonalvertretungsgesetz (PersVG)[15] aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, wie die Gebührendatenerfassung bei Dienst- und Privatgesprächen erfolgt, welche Daten gespeichert und wie und von wen sie ausgewertet werden dürfen.

1.4.2 Die Chipkarte - nicht mehr wegzudenken

1.4.2.1 Technologische Innovationen der Chipkarte

Auf dem Gebiet der Kartensysteme (z.B.: Kreditkarten, ec-Karten usw.) sind revolutionäre Entwicklungen im Gange. Eine neue Generation dieser Karten sind die sogenannten Chipkarten. Diese Karten sind teilweise mit modernsten Prozessorsystemen ausgestattet. Es werden folgende Chipkarten-Produktsegmente unterschieden:

- Karten mit Speicherchips
- Karten mit Mikroprozessoren
- Karten mit Krypto-Controllern

Chipkarten mit Speicherchips werden heute schon bei den Krankenversicherten-Karten und den Telefonkarten verwendet. Diese Art der Karten ermöglicht das Lesen und Schreiben von bestimmten Daten auf der Chipkarte. Mikroprozessor-Karten werden im Bereich der Telekommunikation, z.B. in Mobilfunkgeräten der C- und D-Netze, eingesetzt. Es ist weiterhin geplant, die eurocheque-Karten in Zukunft auf Chip-Technik umzustellen. Karten mit Krypto-Controllern beinhalten bestimmte Sicherheitsalgorithmen, die in besonders sensiblen Bereichen Verwendung finden.

Ein weiteres Unterscheidungsmerkmal dieser Chipkarten ist ihre Funktionalität. Es besteht die Möglichkeit, entweder nur eine (monofunktionale Chipkarte) oder mehrere Anwendungen (multifunktionale Chipkarte) auf einer Karte zu implementieren. Auf den ersten Blick ist die Integration von mehreren Anwendungen auf einer Chipkarte sehr verführerisch, da nur noch eine Karte zum Telefonieren, Geldabheben oder Fahren mit dem öffentlichen Verkehrsmittel benötigt wird. Weiterhin könnte man die komplette Krankenakte auf diesem Datenträger ablegen. Doch welcher Bürger könnte noch transparent nachvollziehen, welche Daten auf seiner Chipkarte gespeichert sind, welche Stellen welche Daten liest, schreibt oder ändert? Was geschieht beim Verlust einer solchen multifunktionalen Chipkarte? All diese Fragen müssen in Zukunft sehr kritisch und mit größter Aufmerksamkeit betrachtet werden.

Auch in der Art der Benutzung dieser Chipkarten gibt es zum Teil sehr unterschiedliche Lösungsansätze. Man unterscheidet zwischen kontaktbehafteten und kontaktlosen Chipkarten. Während bei den kontaktbehafteten Karten bei der Datenverarbeitung ein direkter Kontakt zwischen der Chipkarte und dem Lesegerät bestehen muß, ermöglichen kontaktlose Chipkarten eine Datenübertragung bis zu einigen Metern, wodurch die Gefahr des Abhörens und des unbemerkten Datentransfers besteht.

1.4.2.2 Chipkarten im Zahlungsverkehr

---

15 vom 15. September 1993, GVBl. I, S. 358

Im Bereich des Zahlungsverkehrs liegt eine der Hauptanwendungen der Chipkarte. Zwei unterschiedliche Kartensysteme stehen in diesem Zusammenhang zur Verfügung: die personenbezogene Buchungskarte (z.B. die zukünftige ec-Karte) und die anonyme Wertkarte (z. B. die Telefonkarte). Bei den anonymen Wertkarten, die auch als Prepaid-Cards bezeichnet werden, wird die Chipkarte mit einem bestimmten Wert "aufgetankt" und erst dann die entsprechende Dienstleistung in Anspruch genommen. Dieses Verfahren wird heute schon bei der Telefonkarte realisiert. Die Telefonkarte ist im Vergleich zu zukünftigen Wertkarten nicht wieder aufladbar. Wertkarten haben gegenüber den personenbezogenen Buchungskarten bedeutende Vorteile. Einerseits wird die Anonymität des Verbrauchers gewahrt, es können keine Bewegungsprofile erstellt werden, andererseits wird bei der Verwendung der Karte keine Bonität des Nutzers vorausgesetzt, da die Wertkarte im voraus bezahlt wird. Der Nutzer sollte zwischen dem Einsatz von Pre- und Postpaid-Cards frei wählen können, und nicht durch eine gezielte Verteuerung der Prepaid-Cards einseitig auf die weniger datenschutzfreundliche Lösung der Postpaid-Cards verwiesen werden.

1.4.2.3 Chipkarten im Gesundheitswesen

Im Bereich der Krankenkassen werden derzeit bundesweit Chipkarten eingeführt. In Brandenburg wird bis Anfang 1995 jedem gesetzlich Krankenversicherten eine Krankenversichertenkarte (KVK) gem. § 291 Abs. 1 SGB V[16] ausgehändigt werden. Sie ist eine einfache Speicherkarte (s. unter 1.4.2.1), die gem. § 291 Abs. 2 SGB V neben der Unterschrift des Versicherten ausschließlich folgende Angaben enthalten darf:

- Bezeichnung der ausstellenden Krankenkasse,
- Familienname und Vorname des Versicherten,
- Geburtsdatum,
- Anschrift,
- Krankenversichertennummer,
- Versicherungsstatus,
- Tag des Beginns des Versicherungsschutzes und
- bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Die KVK darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie für die Abrechnung mit den Leistungsträgern verwendet werden. Durch Lesegeräte bei den behandelnden Ärzten werden die auf ihr gespeicherten Informationen ausgelesen und auf maschinell auswertbare Abrechnungsunterlagen und Vordrucke übertragen. Mit der Verwendung der KVK und dieser Formulare werden den Kassenärztlichen Vereinigungen und den Krankenkassen sowohl arzt- als auch patientenbezogene Daten übermittelt, die bei diesen Stellen selbst maschinell ausgewertet werden können. Die datenschutzrechtlichen Fragen betreffen somit weniger den Einsatz der KVK selbst als die Speicherung und Weiterverwendung der Versichertendaten bei den genannten Stellen. Eine vergleichbare Transparenz des Leistungsgeschehens im Gesundheitswesen war unter Verwendung des herkömmlichen Krankenscheins unmöglich.

Um Manipulationen an Versichertendaten zu verhindern, werden nur speziell vom Bundesamt für Sicherheit geprüfte Chipkartenleser in den Arztpraxen zugelassen. Diese Leser dürfen keine Schreibfunktion besitzen. Der Inhaber kann sich beim Aussteller kostenlos vergewissern, welche Angaben auf seiner KVK stehen.

Für die Zukunft sind aber bereits weitere medizinische Anwendungen der Chipkarte geplant,

---

16 Sozialgesetzbuch (SGB) 5. Buch (V), vom 20. Dezember 1988, BGBl. I, S. 2477, zuletzt geänd. am 26. Februar 1993, BGBl. I, S. 278

bei denen der Datenschutz vor völlig neuen Dimensionen stehen wird. Während die KVK nur eine Speicherkapazität von 256 Bytes besitzt, ist es technisch gesehen heute kein Problem mehr, auf eine Chipkarte mit 20 MB die komplette Krankengeschichte eines Menschen einschließlich Röntgenbildern, EKG usw. zu speichern. Vor diesem Hintergrund wird mit der Einführung der KVK weiterhin eine technische (Grund-) Infrastruktur geschaffen, auf deren Basis durch Aufstockung der Weg bereitet wird für den Einsatz von umfassenden Patientenkarten.

Bereits jetzt werden in laufenden Projekten ganz unterschiedliche Zwecke mit dem Einsatz derartiger Patientenkarten verfolgt. Zum einen handelt es sich lediglich um Verweiskarten, auf denen die Arztbesuche des Patienten und indirekt damit auch die Aufbewahrungsorte seiner jeweiligen Krankheitsdaten gespeichert sind. Als Alternative dazu werden in den Dokumentationskarten echte medizinische Daten gespeichert. Dies kann sich auf eine schnelle und einfache Verfügbarkeit von Notfalldaten (Blutgruppe, Rhesusfaktor, Allergien, Impfungen, Einwilligung in Organtransplantation usw.) beschränken oder - wie im Falle der Hochschule Hannover bei Patienten mit Herzschrittmacher bzw. des Deutschen Krebsforschungszentrums bei Krebspatienten - alle für eine intensive Nachsorge erforderlichen Daten einschließen.

Aus Sicht des Datenschutzes muß in jedem Fall die Freiwilligkeit einer Nutzung solcher Chipkarten im Gesundheitswesen gewährleistet bleiben. Bereits jetzt gibt es aber Hinweise dafür, daß dieser datenschutzrechtliche Grundsatz von einzelnen Anbietern unterwandert wird (s. Anlage 16).

1.4.2.4 Chipkarten im öffentlichen Verkehr

Weitere Einsatzorte der Chipkarte sind im öffentlichen Nahverkehr geplant. Auch in diesem Bereich gibt es verschiedene Ansatzpunkte. Diskutiert wird momentan die Verwendung einer vorbezahlten Wertkarte und die Verwendung einer personenbezogenen Verkehrskarte. Die Nutzung einer im voraus bezahlten Wertkarte stellt - wie oben schon erwähnt - kein datenschutzrechtliches Problem dar. Mit dieser Karte kann im gesamten öffentlichen Nahverkehr anonym "bezahlt" werden.

Die zweite Art der Nutzung der Verkehrskarte ist kritisch zu hinterfragen. Bei diesem Prinzip werden die Bewegungsdaten der Nutzer zentral gespeichert, um daraus entsprechende Rabatte für den Benutzer ableiten zu können. In diesem Fall ergibt sich die Frage nach der datenschutzrechtlichen Zulässigkeit dieser personenbezogenen Speicherung von Daten. Der schon so oft zitierte "gläserne Bürger" rückt dann wieder ein Stück näher. Denn es müßten alle Informationen gespeichert werden, z.B. wann ist der Bürger von A nach B gefahren, und welches Verkehrsmittel hat er benutzt. Im öffentlichen Nahverkehr ist der Verwendung von anonymen Wertkarten unbedingt der Vorrang zu gewähren.

In einigen Städten ist die Einführung einer sogenannten City-Card (als Prepaid-Card) vorgesehen. Mit dieser Karte können dann mehrere Dienstleistungen im bargeldlosen Zahlungsverkehr in Anspruch genommen werden, so z. B. für öffentliche Verkehrsmittel, Museen, Schwimmbäder oder Parkuhren. Bei den Verkehrsbetrieben in Kiel befindet sich derzeit das Pilotprojekt "Busfahren mit Telefonkarte" in Erprobung. Diese Wertkartenlösung erfordert keinerlei Speicherung personenbezogener Daten (s. Anlage 13).

1.4.3 Elektronische Autobahnmaut - Vorbereitungen in vollem Gange

Da eine weitere Erhöhung der Mineralölsteuer für eine Finanzierung der Erhaltung und des Ausbaus des Autobahn- und Straßennetzes politisch als inopportun gilt, ist damit zu rechnen, daß spätestens ab 1998 das Befahren deutscher Autobahnen gebührenpflichtig sein wird. Auf einem Teilstück der A 555 zwischen Köln und Bonn läuft bereits ein Feldversuch, womit das Bundesverkehrsministerium die verschiedenen Anbietersysteme auf ihre Eignung für die

Einführung einer Autobahngebühr vergleichend prüfen läßt.

Da das Bundesverkehrsministerium davon ausgeht, daß sich durch eine Autobahngebühr auch eine Steuerung des Verkehrs erreichen läßt, soll die Gebührenerhebung u.a. gestaffelt nach Tageszeit, Wochentag und zurückgelegter Wegstrecke bei ungebremst fließendem Verkehr erfolgen. Dies ist durchaus realisierbar. Voraussetzung ist dazu, daß mit Hilfe eines Datenaustausches per Funk, der zwischen einem im Kraftfahrzeug installierten Bordsystem und an der Straße aufgestellten Feststationen oder im Weltall stationierten Satelliten erfolgt, ein bargeldloser Zahlungsvorgang initiiert oder sofort vollzogen wird. Datenschutzrechtlich bedeutsam ist dabei, ob und in welchem Ausmaße hierbei eine Speicherung von personenbezogenen Daten geschieht.

Grundsätzlich stellt jedes elektronische Maut-System, dem sich kein Verkehrsteilnehmer entziehen kann, eine Herausforderung für den Datenschutz dar, denn das Grundrecht auf freie Entfaltung der Persönlichkeit beinhaltet auch das Recht, sich möglichst frei und unbeobachtet zu bewegen. In dieses Recht greift ein, wer registriert, wann wer und wo mit seinem Auto gefahren ist. Bei dem nachfolgend dargestellten Post- und Prepaid-Verfahren ist dies sehr unterschiedlich der Fall.

1.4.3.1 Postpaid-Verfahren - Erst fahren, dann bezahlen!

Das Fahrzeug verfügt über eine elektronische Plakette, in der die Daten zur Identifizierung, vor allem Name, Anschrift und Kfz-Kennzeichen, gespeichert vorliegen. Sobald das Fahrzeug in einen Gebührenbereich gelangt, werden automatisch die Identifikationsdaten von der elektronischen Plakette abgerufen und an einen Zentralrechner weitergegeben. Dieser stellt für einen bestimmten Abrechnungszeitraum, z. B. monatlich, dem Fahrzeughalter die angefallenen Gebühren in Rechnung. Dazu wird zumindest im Zentralrechner bis zur Bezahlung der Gebühr und darüber hinaus für eine angemessene Reklamationsfrist gespeichert, wann welches Fahrzeug welchen Straßenabschnitt befahren hat. Damit entstehen riesige Datenbestände, mit denen sich ggf. exakte Bewegungsprofile einzelner Verkehrsteilnehmer erstellen lassen.

1.4.3.2 Prepaid-Verfahren - Erst bezahlen, dann fahren!

Bei diesem Verfahren bezahlt der Fahrer im voraus einen (variablen oder Mindest-) Betrag, der auf einer wiederaufladbaren Chipkarte verbucht wird. Gelangt ein Fahrzeug in einen Gebührenbereich, so wird während der Fahrt über Funk dem im Auto montierten Abbuchungsgerät das Kommando gegeben, das Guthaben auf der Chipkarte automatisch um einen bestimmten Betrag zu reduzieren.

Dieses Verfahren erscheint auf den ersten Blick datenschutzfreundlicher, da für die Abbuchung des Betrages weder die Identität des Fahrers noch die des Fahrzeuges erforderlich sind und somit die Speicherung personenbezogener Daten entfällt. Das trifft aber nur zu, solange die Abbuchung ohne Komplikationen verläuft. Was ist aber, wenn der Restbetrag auf der Chipkarte nicht ausreicht oder das Abbuchungsgerät einen Defekt aufweist und damit eine automatische Gebührenabbuchung unmöglich wird?

Für diese und andere Fälle sollen nach Meinung von Verkehrsexperten vorbeugend flächendeckend Videokameras installiert werden, die alle vorbeifahrenden Fahrzeuge fotografieren. Dagegen sind - wie oben dargestellt - grundsätzliche Bedenken aus datenschutzrechtlicher Sicht zu erheben. Diese Bedenken können auch nicht mit dem Argument ausgeräumt werden, daß die Aufnahmen der Fahrzeuge, bei denen die Gebührenabbuchung komplikationslos verlief, unmittelbar danach gelöscht werden. Vielmehr ist auf die potentielle Gefahr aufmerksam zu machen, die ein so aufwendiges und teures Kontrollsystem darstellt. Von ihm wird früher oder später die Versuchung ausgehen, es auch

für andere Zwecke zu nutzen oder gar zu mißbrauchen. Dies ist bereits verschiedentlich geäußert worden.

Dagegen wäre ein stichprobenartiges Kontrollsystem - ähnlich wie bei Geschwindigkeitsüberprüfungen - durchaus vorstellbar. Dafür müßte vom Abbuchungsgerät lediglich ein zusätzliches Signal über die ordnungsgemäße Funktion gesendet werden.

Ich hoffe, daß es bei der letztendlichen Entscheidung über die Einführung einer elektronischen Autobahnmaut zu einer gründlichen Abwägung aller Optionen auch unter datenschutzrechtlichen Gesichtspunkten kommt. In welcher Form auch immer die Erfassung der Autobahngebühren gestaltet werden soll, in jedem Fall wird dafür ein Gesetz erforderlich sein, in dem nicht zuletzt auch und gerade die Datenerhebung und -verarbeitung detailliert geregelt werden muß.

1.4.4 Leichtfertiger Umgang mit Telefax

Telefaxgeräte haben in den Behörden als schnelles Kommunikationsmittel in großem Maße Einzug gehalten, nicht zuletzt weil Telekopien in vielen Fällen billiger als der Briefversand sind. Obwohl auch Telefaxgeräte zu den Fernmeldeanlagen gehören und alle Telekopien und Übermittlungsprotokolle dem Fernmeldegeheimnis nach Art. 10 Abs. 1 Grundgesetz unterliegen, ist die Gefährdung des Datenschutzes bei den üblichen Standardfaxgeräten jedoch größer als beim Briefversand. Telekopien kommen beim Empfänger ohne Umschlag an. Wenn sie einen falschen Adressaten erreichen, dann werden sie zwangsläufig unbefugt gelesen. Beim Briefverkehr wird der falsch zugestellte Brief dagegen normalerweise ungeöffnet zurückgeschickt.

Darüber hinaus sind Telefax-Geräte kleine Rechner, die personenbezogene Daten automatisiert verarbeiten. Sie speichern in jedem Fall die Verbindungsdaten der abgesandten Telekopien in einem besonderen Protokollbereich. Nur ein Teil der Geräte speichert auch die ankommenden und die abzusendenden Inhalte der Telekopien. Zur Wahrung des Rechts auf informationelle Selbstbestimmung sind deshalb bei ihrem Einsatz technische und organisatorische Maßnahmen gem. § 10 Bbg DSG bzw. gem. § 9 Bundesdatenschutzgesetz (BDSG) zu treffen. Aufgrund der bestehenden Risiken für die Einhaltung der Vertraulichkeit bei der Übermittlung von Daten mittels Fax sollten deshalb Regeln speziell vom Absender eines Telefax eingehalten werden, wie sie in Anlage 2 beschrieben sind.

Die vorstehend empfohlenen Regelungen zum datenschutzgerechten Gebrauch von Faxgeräten gelten nur eingeschränkt bei der Übermittlung von Patientendaten in "echten" Notfällen, beispielsweise für Notaufnahmestationen in Krankenhäusern. Die dort tätigen Ärzte sind zur Einschätzung des akuten Krankheitsgeschehen dringend auf frühere Krankheitsdaten ohne Zeitverzug angewiesen. Ist im konkreten Fall eine Übermittlung dieser Daten nur durch ein in der Verwaltung der angegangenen Institution aufgestelltes Telefaxgerät möglich oder kann das Fax mit den Befunden nur in der Verwaltung des anfordernden Krankenhauses empfangen werden, können die beteiligten Ärzte grundsätzlich von einer mutmaßlichen Einwilligung des Betroffenen ausgehen.

Eine größere Gewährleistung des Datenschutzes bieten Fax-Personalcomputer oder PC mit Faxeinrichtung, wenn man die üblichen Sicherheitsanforderungen bei PC realisiert hat. Günstig ist auch, daß Fax-PC, die nicht ständig empfangsbereit sind, an das öffentliche Netz angeschlossen werden dürfen. Dabei müssen die eingehenden Telefaxe, die im PC abgespeichert werden, nicht unbedingt ausgedruckt werden. Dadurch wird die Gefahr des unbefugten Lesens von Telekopien deutlich eingeschränkt. Weitere Sicherungen sind denkbar: die Verschlüsselung der Telekopien für die Übermittlung und eine sicherere Adressierung des Empfängers etwa durch automatischen Rückruf und Überprüfung der Fax-Nummer des Empfängers im Fax-PC des Absenders.

1.4.5 Anrufbeantworter mit Fernabfrage

In der heutigen Kommunikationsgesellschaft stellen Telefonanrufbeantworter keine Besonderheit mehr dar. Anrufbeantworter werden heute schon sehr preisgünstig angeboten. Die datenschutzrechtlichen Gefahren, die von dieser Technik ausgehen, werden aber noch zu wenig berücksichtigt. Viele Anrufbeantworter sind mit einer sog. Fernabfrage ausgestattet. Es besteht damit die Möglichkeit, den Anrufbeantworter von einem beliebigen Telefon aus fernzusteuern.

Folgende Fernsteuerungsmöglichkeiten stehen typischerweise zur Verfügung:

- Abfrage von aufgezeichneten Gesprächen,
- Löschen sämtlicher aufgezeichneten Gespräche,
- schneller Vor- und Rücklauf des Bandes,
- Raumüberwachung.

Kritische Punkte aus der Sicht des Datenschutzes sind die Raumüberwachung und Abfrage von aufgezeichneten Gesprächen. Bei Nutzung der Raumüberwachungsfunktion kann der Anrufer die Gespräche in unmittelbarer Nähe des Anrufbeantworters mithören.

Nach Start der Fernabfrage muß eine Geheimzahl am Fernabfragesender eingegeben werden. Diese Geheimzahl ist in den meisten Fällen zwei- oder dreistellig. Die Länge der Geheimzahl ist als völlig unzureichend anzusehen. Empirisch läßt sich relativ schnell diese Nummer ermitteln. Bei zweistelligen Geheimzahlen ergeben sich sogar nur 100 verschiedene Möglichkeiten, die in kurzer Zeit ausprobiert werden können. Der Schutz der persönlichen Daten des Anrufers und des Angerufenen sind dadurch extrem gefährdet. In öffentlichen Behörden sollte deshalb auf Verwendung eines solchen Anrufbeantworters mit Fernabfrage generell verzichtet werden.

2 Zusammenarbeit mit Landtag und Landesregierung

2.1 Landtag

2.1.1 Kontrollmöglichkeiten

Im Zusammenhang mit der parlamentarischen Tätigkeit des Landtags wurden datenschutzrechtliche Fragestellungen an mich herangetragen, bei deren Bearbeitung jeweils zunächst die folgende Problematik der gesetzlichen Regelung im Brandenburgischen Datenschutzgesetz im Vordergrund stand:

Als unabhängiges Verfassungsorgan und Repräsentant der freien Willensbildung des Volkes kann der Landtag in seiner parlamentarischen Tätigkeit nicht einer faktisch administrativen Kontrolle unterliegen, und zwar auch dann nicht, wenn die Kontrollinstanz, wie es bei meinem Amt der Fall ist, vom Parlament berufen ist. Die Einhaltung der verfassungsrechtlichen und einfachgesetzlichen Begrenzungen der parlamentarischen Tätigkeit kann nach den der demokratischen Rechtsordnung zugrunde liegenden Prinzipien der Gewaltenteilung grundsätzlich nur von der rechtsprechenden Gewalt überwacht werden. Deshalb können von Verfassungs wegen meinem Amt im Hinblick auf die parlamentarische Tätigkeit des Landtags keine Kontrollbefugnisse zustehen.

Zu Recht hat der Gesetzgeber mein Amt auch nicht als Instrument der Selbstkontrolle des Parlaments konzipiert, sondern mir lediglich die Aufgabe zugewiesen, den Landtag auf eine entsprechende Bitte hin in datenschutzrechtlichen Fragen zu seiner parlamentarischen Tätigkeit sachverständig zu beraten. Dadurch wird ausgeschlossen, daß die ausschließliche

Verantwortlichkeit des Parlaments als der Summe seiner vom Volk frei gewählten Mitglieder für die Rechtmäßigkeit der eigenen parlamentarischen Tätigkeit - und d. h. in einer Demokratie für die Verfassungsgemäßheit der Repräsentation des Volkes - auf eine dem Wähler selbst nicht unmittelbar verantwortliche Kontrollinstanz abgeschoben werden kann. Bei diesem Verständnis der verfassungsrechtlichen Ausgangslage sehe ich meine wesentliche Aufgabe darin, im parlamentarischen Entscheidungsprozeß entscheidungsrelevante datenschutzrechtliche Kriterien darzustellen und zu erläutern.

Nicht für überzeugend halte ich es, daß nach dem Willen des Gesetzgebers für die parlamentarische Tätigkeit des Landtags lediglich die sich unmittelbar aus der Verfassung ergebenden datenschutzrechtlichen Kriterien gelten sollen, das Parlament sich jedoch in § 2 Abs. 1 Satz 2 Bbg DSG von einer Anwendung der in diesem Gesetz getroffenen allgemeinen Regelung über die Verarbeitung personenbezogener Daten ausgenommen hat. Dieser Ausschluß des einfachgesetzlichen datenschutzrechtlichen Maßstabs für die parlamentarische Tätigkeit des Landtags scheint mir auch im Hinblick auf die in Art. 12 Abs. 1 Verfassung des Landes Brandenburg[17] betonte Gleichheit aller vor dem Gesetz nicht gerechtfertigt zu sein. Ferner ergibt sich daraus für Stellungnahmen meines Amtes zu datenschutzrechtlichen Fragen im Zusammenhang mit der parlamentarischen Tätigkeit des Landtags eine weitere Beschränkung insofern, als dabei eben auf die für meine sonstige Tätigkeit maßgeblichen rechtlichen Kriterien des Brandenburgischen Datenschutzgesetzes nicht Bezug genommen werden kann. Ich würde es deshalb begrüßen, wenn anläßlich einer Novellierung des Brandenburgischen Datenschutzgesetzes die problematische gesetzliche Verpflichtung zum Messen mit zweierlei Maß vom Gesetzgeber noch einmal überdacht würde.

Hinzuweisen ist dabei auch auf ein weiteres Problem der gesetzlichen Regelung in § 23 Abs. 4 Bbg DSG. Danach kann mich der Landtag mit Stellungnahmen zu Datenschutzfragen betrauen. Da in § 23 Abs. 3 und 5 Bbg DSG deutlich unterschieden wird zwischen dem Landtag einerseits und seinen Ausschüssen andererseits, gehe ich grundsätzlich davon aus, daß der Begriff des Landtags in § 23 Abs. 4 Bbg DSG dort ebenso als auf die Gesamtheit, d. h. das Plenum des Parlaments bezogen zu verstehen ist, wie meines Erachtens der Begriff der dort ebenfalls genannten Landesregierung im Hinblick auf die ausdrückliche Unterscheidung in § 23 Abs. 2 Bbg DSG nur auf die Gesamtheit ihrer im Kabinett vertretenen Mitglieder zu beziehen ist und nicht auch die einzelnen Ministerien meint. Jedoch ist keine der mir seitens des Landtags vorgelegten datenschutzrechtlichen Fragestellungen vom Plenum an mich herangetragen worden. Vielmehr handelte es sich um Anfragen einer Fraktion sowie des Petitions-, des Haupt- und eines Untersuchungsausschusses. Vor diesem Hintergrund scheint mir eine gesetzliche Klarstellung dazu erforderlich zu sein, ob das in § 23 Abs. 4 Bbg DSG nach Wortlaut und Systematik der Regelung dem Plenum des Landtags vorbehaltene Recht, mein Amt mit Stellungnahmen zu datenschutzrechtlichen Fragen zu betrauen, auch den Ausschüssen des Landtags und gegebenenfalls weiteren in der Geschäftsordnung des Landtags mit eigenen Rechten ausgestatteten Beteiligten zustehen soll oder nicht.

2.1.2 Einzelfragen

Im Fall der Anfrage der *Fraktion*, die sich auf die Rechtmäßigkeit der Weitergabe personenbezogener Daten aus dem Bereich eines Untersuchungsausschusses heraus bezog, habe ich eine Stellungnahme unter Hinweis auf die bestehende Rechtslage abgelehnt.

Bei der Anfrage des *Petitionsausschusses* handelte es sich der Sache nach um eine Angelegenheit, die meinen Aufgabenbereich unmittelbar betraf. Der Petitionsausschuß hätte mich deshalb - vorzugsweise mit Einwilligung der Petentin - gem. § 23 Abs. 3 Bbg DSG

---

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

ersuchen können, der Eingabe der Petentin in eigener Zuständigkeit nachzugehen. Die Anfrage beschränkte sich jedoch auf die Bitte, den in der Eingabe vorgetragenen Sachverhalt datenschutzrechtlich zu bewerten und so den Petitionsausschuß bei seiner eigenen Tätigkeit zu beraten. Im gegebenen Fall konnte die Frage der Vereinbarkeit dieses Vorgehens mit der gesetzlichen Regelung in § 23 Abs. 3 und 4 Bbg DSG dahinstehen, da bereits der mir mitgeteilte Sachverhalt eine rechtliche Beurteilung nicht zuließ und ich mich in meiner Antwort an den Petitionsausschuß auf einen abstrakten Hinweis zum Brandenburgischen Datenschutzgesetz beschränken konnte.

Zu den Anfragen des *Haupt- und des Untersuchungsausschusses* habe ich - mit den aufgezeigten Beschränkungen - trotz der dargestellten Bedenken in der Sache Stellung genommen. Dabei habe ich gleichsam eine entsprechende Bevollmächtigung der Ausschüsse durch das Plenum des Landtags stillschweigend unterstellt. Dies schien mir in beiden Fällen der Sache nach gerechtfertigt zu sein. Gleichwohl meine ich, daß eine solche Einzelfallpraxis eine normenklare gesetzliche Regelung nicht entbehrlich macht.

Der *Hauptausschuß* hatte mich um eine datenschutzrechtliche Beurteilung der beabsichtigten Immunitätsrichtlinien des Landtags gebeten. Dabei ging es im wesentlichen um die in § 1 des Entwurfs der Immunitätsrichtlinien vorgesehenen Mitteilungen des Justizministeriums an den Präsidenten des Landtags über einen Abgeordneten betreffende Strafverfolgungsmaßnahmen.

Die nach dem Entwurf vorgesehene Anzeige solcher Strafverfolgungsmaßnahmen beim Präsidenten des Landtags habe ich für geeignet und erforderlich gehalten, um der durch die Maßnahmen gegebenenfalls drohenden Beeinträchtigung der parlamentarischen Arbeit gem. Art. 58 der Landesverfassung zu begegnen. Insbesondere habe ich sie auch aus datenschutzrechtlicher Sicht für verhältnismäßig gehalten. Bei dieser Beurteilung war das in Art. 58 Landesverfassung garantierte Recht des Parlaments gegen das Grundrecht der betroffenen Abgeordneten auf informationelle Selbstbestimmung abzuwägen. Dabei war davon auszugehen, daß das Grundrecht auf informationelle Selbstbestimmung den Abgeordneten nur in den verfassungsimmanenten Schranken des Art. 58 der Landesverfassung zusteht. Im Hinblick auf die Bedeutung, die der freien und unbeeinträchtigten Willensbildung des Parlaments in einer freiheitlichen parlamentarischen Demokratie zukommt, bin ich zu der Auffassung gelangt, daß auch aus datenschutzrechtlicher Sicht keine durchgreifenden Bedenken dagegen zu begründen sind, das Grundrecht der Abgeordneten auf informationelle Selbstbestimmung hinter dem Verfassungsrecht des Parlaments auf Wahrung seiner unbeeinträchtigten Arbeitsfähigkeit zurücktreten zu lassen.

Die in § 1 Abs. 1 des Entwurfs aufgeführten Strafverfolgungsmaßnahmen sind grundsätzlich dazu geeignet, die durch Art. 58 der Landesverfassung geschützte freie politische Willensbildung und Beschlußfassung des Parlaments zu beeinflussen, da durch sie stets ein gewisser Druck auf die Abgeordneten ausgeübt wird. Dem Parlament muß deswegen grundsätzlich das Recht und die Möglichkeit eingeräumt werden, auch gegen den Willen des betroffenen Abgeordneten die Frage zu prüfen, ob durch die Strafverfolgungsmaßnahmen sein eigenes Verfassungsrecht beeinträchtigt wird, um eine solche Beeinträchtigung gegebenenfalls gem. Art. 58 der Landesverfassung abwehren zu können. Zu berücksichtigen war bei der Beurteilung schließlich auch, daß die Übernahme eines Abgeordnetenmandats auf der freien Entschließung des Betroffenen beruht. Ich habe deshalb dem Hauptausschuß im Ergebnis lediglich eine Konkretisierung zum Inhalt der Mitteilungen des Justizministeriums empfohlen.

In der Anfrage des *Untersuchungsausschusses* war ich um eine Empfehlung dazu gebeten worden, in welchem Umfang eine Anonymisierung der personenbezogenen Daten erforderlich sei, die in den Dokumenten enthalten sind, die als Anlage zum Schlußbericht des Untersuchungsausschusses veröffentlicht werden sollen.

In meiner Stellungnahme bin ich davon ausgegangen, daß das Recht der parlamentarischen Untersuchungsausschüsse auf Beweiserhebung nach Maßgabe der dafür geltenden Verfahrensregelungen die Veröffentlichung des Beweismaterials grundsätzlich mit einschließt, da diese in einer parlamentarischen Demokratie gleichsam Bestandteil einer wirksamen Kontrolle der Regierung durch das Parlament ist.

Soweit jedoch mit einer Veröffentlichung des Beweismaterials zugleich das Grundrecht des Betroffenen auf informationelle Selbstbestimmung berührt ist, ist zu beachten, daß grundsätzlich von Verfassungs wegen jede Grundrechtsbeeinträchtigung für den jeweiligen Zweck geeignet, erforderlich und verhältnismäßig sein muß. Es muß also vom Untersuchungsausschuß jeweils konkret geprüft werden, ob der verfassungsrechtliche Auftrag des parlamentarischen Untersuchungsausschusses die Veröffentlichung der jeweiligen personenbezogenen Daten erfordert oder auch auf andere Weise sachgerecht erfüllt werden kann. Dabei ist auch das mit der Veröffentlichung verfolgte Ziel des dem Untersuchungsausschuß erteilten Auftrags gegen die Schutzwürdigkeit und -bedürftigkeit der jeweiligen personenbezogenen Daten abzuwägen. Personenbezogene Daten, deren Weitergabe wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist und auf die sich deshalb bereits das Beweiserhebungsrecht des Untersuchungsausschusses nicht erstreckt, dürfen nicht veröffentlicht werden. Im übrigen ist der Abwägung die herausragende Bedeutung zugrunde zu legen, die das Kontrollrecht des Parlaments sowohl für die parlamentarische Demokratie als auch für das Ansehen des Staates hat. Eine Verkürzung der Rechte des parlamentarischen Untersuchungsausschusses zugunsten des Rechts des einzelnen auf informationelle Selbstbestimmung dürfte danach nur bei gravierenden Beeinträchtigungen der individuellen Grundrechtsposition in Betracht kommen.

Nach Maßgabe dieser grundsätzlichen Erwägungen habe ich die Auffassung vertreten, daß eine Veröffentlichung der Anschriften für Zwecke des Untersuchungsausschusses nur unter besonderen Umständen erforderlich sein dürfte, und insbesondere empfohlen, die Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung bei Unterlagen mit Personalaktendatenqualität besonders sorgfältig zu prüfen. Soweit es sich bei den für die Veröffentlichung vorgesehenen Dokumenten um Unterlagen handelt, die dem Untersuchungsausschuß von dem Bundesbeauftragten für die Stasi-Unterlagen nach Maßgabe des Stasi-Unterlagengesetzes (StUG)[18] zur Verfügung gestellt wurden, habe ich vorgeschlagen, der Regelung des § 32 Abs. 3 StUG entsprechend zu verfahren, durch die der Bundesgesetzgeber den Maßstab für einen Ausgleich vergleichbarer Interessen gesetzt hat. Ich habe ferner angeregt, insoweit gegebenenfalls auch den Bundesbeauftragten für die Stasi-Unterlagen um eine sachverständige Stellungnahme zu bitten.

2.2 Landesregierung

Auf einzelne Aspekte und Beispiele zur konkreten Zusammenarbeit mit den Ministerien werde ich in meinem Bericht aus den Geschäftsbereichen näher eingehen. An dieser Stelle hervorzuheben ist lediglich die für die Erfüllung meiner Aufgaben unerläßliche Beteiligung meines Amtes beim Erlaß von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen oder eine solche zwingend voraussetzen, sowie bei Maßnahmen von erheblicher datenschutzrechtlicher Bedeutung.

Ich habe insoweit bereits in einer Stellungnahme gegenüber dem Innenausschuß empfohlen, im Brandenburgischen Datenschutzgesetz ausdrücklich klarzustellen, daß ich in diesen Fällen vor dem Erlaß der Vorschriften bzw. vor der Durchführung der Maßnahmen zu hören bin. Derzeit erfahre ich leider noch immer von datenschutzrelevanten Regelungen erst durch die

---

18 vom 20. Dezember 1991, BGBl. I, S. 2272

Veröffentlichung im Amtsblatt bzw. im Gesetz- und Verordnungsblatt. Dies ist aus meiner Sicht mit der verfassungsrechtlichen Verpflichtung zum Datenschutz nicht zu vereinbaren, denn es wird so bereits verfahrensmäßig ausgeschlossen, daß ich schon im Vorfeld beabsichtigter Regelungen und Maßnahmen auf die sich aus ihnen möglicherweise ergebenden Beeinträchtigungen des Grundrechts auf informationelle Selbstbestimmung hinweisen kann. Damit geht meinem Amt jedoch die Qualität einer rechtzeitigen verfahrensrechtlichen Schutzvorkehrung verloren, die das Bundesverfassungsgericht der Beteiligung unabhängiger Datenschutzbeauftragter ausdrücklich zugemessen hat[19]. Auch die nur begrenzten personellen Kapazitäten meines Amtes machen es erforderlich, mich möglichst frühzeitig zu beteiligen.

In diesem Zusammenhang hat der Innenausschuß des Landtags festgestellt[20], daß die Sensibilität für die Aufgaben des Datenschutzes auf allen Ebenen der Verwaltung und der Politik im Land Brandenburg deutlich erhöht werden muß, und sich dafür ausgesprochen, im Brandenburgischen Datenschutzgesetz die Stellung des Landesbeauftragten für den Datenschutz zu stärken und die frühzeitige und umfassende Einbeziehung meines Amtes bei allen erheblichen datenschutzrechtlichen Fragen sicherzustellen. Dazu liegen dem Landtag inzwischen konkrete Vorschläge für eine Novellierung des Brandenburgischen Datenschutzgesetzes vor.

19

20 vgl. BVerfGE 65, 1 (46)

Beschlußempfehlung u. Bericht d. Ausschusses für Inneres, Landtags-Drs. 1/2698 vom 13. Januar 1994

3 Inneres

3.1 Altdaten auch weiterhin aktuell

3.1.1 Meldepflicht von Altdaten

Öffentliche und nicht-öffentliche Stellen sowie Personen, die im Besitz sind von personenbezogenen Daten aus sog. "ehemaligen Einrichtungen" (staatliche oder wirtschaftsleitende Organe, Kombinate, Betriebe und Einrichtungen sowie gesellschaftliche Organisationen der ehem. DDR), hatten darüber - soweit sie diese Daten nicht in den Verwaltungsvollzug übernommen haben - gem. § 34 Abs. 3 Bbg DSG bis zum 01. Juli 1992 entsprechend § 8 Abs. 1 Bbg DSG ein Verzeichnis zu erstellen und dem Ministerium des Innern vorzulegen. Zur möglichst effektiven Umsetzung dieser Übergangsregelung hat sich das Ministerium des Innern (MdI) in Abstimmung mit mir mit einem Rundschreiben[21] an die Verwaltungen gewandt, in dem die wesentlichen ehemaligen Einrichtungen zusammengestellt und die Meldepflicht sowie die Verantwortlichkeiten nach § 34 Abs. 3 Bbg DSG erläutert wurden.

In unregelmäßigen Abständen bin ich bisher über den Stand der eingegangenen Meldungen seitens des MdI informiert worden. Trotz des erwähnten Rundschreibens liegen dem Ministerium mit Stand Ende März 1994 nur insgesamt 30 Meldungen von Landratsämtern bzw. kreisfreien Städten (darunter auch Mehrfachmeldungen) vor; weitere 9 betreffen Altdatenbestände des Bereiches Polizei, die vom Inhalt her nicht unter diese Regelung fallen (s. unter 3.1.3). Bezüglich der weiteren Verwendung bzw. Aufbewahrung dieser Altakten hat das Ministerium des Innern in der Regel andere Ministerien konsultiert. Grundsätzlich war dabei zu beachten, daß Daten aus ehemaligen Einrichtungen gem. § 37 Abs. 1 Bbg DSG bis zum Inkrafttreten eines Brandenburgischen Archivgesetzes gesperrt sind (d. h. sie durften weder verwendet, übermittelt, genutzt oder gelöscht werden).

Die Anzahl der eingegangenen Meldungen repräsentieren nicht den tatsächlichen Bestand an Altdaten im Lande, deshalb werden "Zufallsfunde" in Zukunft nicht ausbleiben. Mir sind im Berichtszeitraum zwei derartige Fälle angezeigt worden:

- Ein Petent beschwerte sich, daß seine Karteikarte über die abgelegte Meisterprüfung einschließlich deren Benotung auf dem Hof der zuständigen Handwerkskammer neben den Müllbehältern gefunden wurde. Auf meine Nachfrage räumte die Handwerkskammer ein, daß Kinder in das angrenzende und nicht bewachte Objekt eingebrochen waren, dabei auf Altakten u. a. von der bis 1972 an die DDR-Handwerkskammer angegliederten Bereichsakademie gestoßen waren und große Teile anschließend auf dem Hof der Handwerkskammer sowie auf die anliegende Straße verstreut hatten.

  Nach Darstellung der Handwerkskammer sind diese Altakten, soweit sie noch vorhanden waren, sofort durch eigene Kräfte "beräumt" und "aufgeräumt" worden. Erst auf erneute Nachfrage teilte die Handwerkskammer mit, daß sie diese Akten dabei auch gleich vernichtet hätte. Begründet wurde diese Vorgehensweise damit, daß diese Akten bereits nach den Bestimmungen der DDR-Gesetzgebung längst hätten vernichtet sein müssen. Von dem seit Januar 1992 geltenden Brandenburgischen Datenschutzgesetz hatte die Handwerkskammer keine Kenntnis.

- Ein Landratsamt zeigte mir an, daß Mitte Januar 1994 durch die untere Naturschutzbehörde Aktenbestände auf einer eigentlich stillgelegten Müllkippe aufgefunden worden waren. Dabei handelte es sich um Bauakten aus dem Jahre 1908 und

---

21 vom 16. März 1992, ABl., S. 363

um Bauakten mit DDR-Bauzustandsanalysen zweier Gemeinden. Beide Funde sind nach Auskunft des zuständigen Amtes bei einer Sperrmüllaktion versehentlich "mit verkippt" worden. Ich habe diese Umgangsweise mit Akten beanstandet. Die aufgefundenen Aktenbestände sind zwischenzeitlich dem zuständen kommunalen Archiv zugestellt worden.

3.1.2 Unterlagen aus Pionierlagern

Aufgefunden wurden auch Unterlagen aus den Krankenstationen ehemaliger Zentraler Pionierlager. Ambulant behandelte Lagerteilnehmer sind hier listenmäßig mit Name, Adresse, Symptom, Diagnose und Therapie erfaßt worden; darüber hinaus sind darin Krankengeschichten und ärztliche Abschlußberichte von stationär behandelten Patienten dokumentiert. Ich habe dem Vorschlag des Landesamtes für Soziales und Versorgung zugestimmt, daß diese Unterlagen von insgesamt 6 Lagern zur ordnungsgemäßen Archivierung an die Gesundheitsämter der Kreise übergeben werden, in denen sich diese Einrichtungen befanden.

3.1.3 Daten der ehemaligen Volkspolizeikreisämter - Bereich Meldewesen -

Die Zuständigkeit für das Paß- und Meldewesen in der DDR lag nach § 7 Gesetz über die Aufgaben und Befugnisse der Deutschen Volkspolizei[22] bei der Polizei und wurde im wesentlichen von den Volkspolizeikreisämtern (VPKÄ) wahrgenommen (s. 1. Tätigkeitsbericht unter 5.6 ff.). Den neuen Bundesländern wurde deshalb eine Überleitungsregelung im Einigungsvertrag[23] eingeräumt, das Meldewesen innerhalb von einem Jahr nach Wirksamwerden des Beitritts nach den Vorschriften des Melderechtsrahmengesetzes zu gestalten. Dazu hat das brandenburgische Innenministerium als ersten Schritt per Erlaß vom 13.12.1990 festgelegt, daß ab 01.01.1991 die Oberbürgermeister und Landräte als Kreisordnungsbehörden die Aufgaben des Meldewesens, der Personalausweis- und Paßangelegenheiten sowie des Ausländer- und Asylrechts wahrzunehmen haben. Gleichzeitig wurde bestimmt, daß bis dahin verwendete Unterlagen und Datenträger bis zu einer endgültigen Entscheidung bei den VPKÄ verbleiben und getrennt von anderen Dienstvorgängen sicher aufzubewahren sind.

Nachdem ich das Ministerium des Innern wiederholt auf diese Akten angesprochen hatte, begrüße ich es ausdrücklich, daß das Ministerium meine Hinweise aufgegriffen und nach Abstimmung mit mir ein Rundschreiben zur weiteren Verwendung von Daten der ehemaligen Volkspolizeikreisämter (VPKA) Bereich Meldewesen[24] erlassen hat. Danach sind

- Kataloge der Personenkennzahl,
- Anträge auf Ausstellung von Personalausweisen,
- Anzeigen von Verlusten von Personalausweisen,
- Anträge auf Ein- und Ausreisen,
- Mikrofilme,
- Stellungnahmen der Abschnittsbevollmächtigten sowie des jeweiligen Betriebes zum Reiseantrag,
- Anträge auf Fremdenpässe,
- Ausreiseanträge für Übersiedler und

22

23 vom 11. Juni 1968, GBl. d. DDR I, S. 232

vom 31. August 1990, BGBl. II, S. 889, zuletzt geänd. am 20. August 1992, BGBl. I, S. 1546, in Anl. I Kap. II Sachgeb. C

24 Abschn. III Nr. 4 Buchst. a

vom 9. Dezember 1993, ABl., S. 1750

- Hotelmeldescheine

möglichst bis zum 30.06.1994 zu vernichten.

Schwierig war zu entscheiden, ob die Unterlagen möglicherweise Angaben enthalten, die von Betroffenen noch für die Durchsetzung von Restitutions- und Rehabilitierungsansprüchen benötigt werden könnten. Ursprünglich sollten dies nach Meinung des Innenministeriums die zuständigen Stellen nach Durchsicht selbst entscheiden. Dies hätte jedoch die gebotene Vernichtung unnötig hinausgeschoben. Ausdrücklich enthält deshalb Nr. 2.4. des Rundschreibens die Befugnis auf eine vorherige Einsichtnahme in diese Akten durch den Betroffenen. Darauf sind die Bürger mindestens in allgemeiner (ortsüblicher) Form hinzuweisen. Aus der Presse konnte ich hierzu bisher keine Hinweise entnehmen.

Weiterhin aufbewahrt werden müssen bei den Personalausweisbehörden Nachweise über die Ausstellung von Personalausweisen und Nebenkarteien. Dies ist erforderlich, weil die Personalausweise der ehemaligen DDR bis zum 31. Dezember 1995 gültig sind[25] bzw. weil § 11 Abs. 4 Brandenburgisches Meldegesetz[26] vorschreibt, die Daten von verzogenen bzw. verstorbenen Personen 50 Jahre zu speichern.

3.1.4 Weiternutzung des reduzierten DDR-Meldedatensatzes

Grundsätzlich habe ich dem Gesetzentwurf zur Änderung des Stasi-Unterlagen-Gesetzes (StUÄndG)[27] begrüßt, weil damit endlich die im Einigungsvertrag[28] nicht vorgesehene - über den 31.12.1992 hinausgehende - Weiteraufbewahrung und -nutzung des reduzierten Meldedatenbestandes des Zentralen Einwohnerregisters der ehemaligen DDR durch die Behörde des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und durch die Zentrale Ermittlungskommission für Regierungs- und Vereinigungskriminalität (ZERV) gesetzlich geregelt wird.

Die Gesetzesänderung setzt den Schlußpunkt unter eine lange Diskussion über die Frage, ob dazu überhaupt eine gesetzliche Grundlage erforderlich sei. Begonnen hatte sie Ende 1992 mit der Auflösung des Zentralen Einwohnerregisters (ZER) in Berlin-Biesdorf. Die Innenminister der fünf neuen Bundesländer und Berlins sowie die Datenschutzbeauftragten waren sich einig, daß ein auf

- Name, Vorname,
- Geburtsname, sonstige Namen,
- Geburtsort,
- Personenkennzeichen (PKZ),
- letzte Anschrift DDR,
- Merkmal "Verstorben"

reduzierter Datensatz jedes Einwohners (Stand Oktober 1992) von der Vernichtung ausgenommen werden solle. Sie waren sich ebenfalls einig, daß zur Datennutzung gesetzliche Regelungen nötig seien. Bundesstellen vertraten demgegenüber die Auffassung, daß das

---

[25] vom 31. August 1990, BGBl. II, S. 889 in Anl. I Kap. II Sachgeb. B Abschn. III Nr. 2 Ziff. 8

[26] vom 25. Juni 1992, GVBl. I, S. 236

[27] BT-Drs. 12/5775

[28] vom 31. August 1990, BGBl. II, S. 889 in Anl. I Kap. II Sachgeb. C Abschn. III

StUG in seiner damaligen Fassung als gesetzliche Grundlage ausreiche, da der reduzierte Meldedatenbestand keine Meldedaten im Sinne des gültigen Melderechts enthalte, sondern den Stasi-Unterlagen zuzurechnen sei.

Im Gegensatz zu den Datenschutzbeauftragten sind die Innenminister im Laufe des Jahres 1993 von ihrer ursprünglichen Auffassung abgerückt. Im Zuge dieses Sinneswandels beabsichtigte das MdI Brandenburg schließlich, die unterdessen aufbereitete Datei ohne weiteres an das Bundesministerium des Innern (BMI) zu übergeben. Dies hat der Landtag Brandenburg durch Beschluß vom 17.06.1993[29] verhindert. In der mündlichen Verhandlung einer einstweiligen Verfügung, die ein Abgeordneter beim Potsdamer Verwaltungsgericht beantragt hatte, um die Übergabe zu stoppen, hat das Gericht die Auffassung der Datenschutzbeauftragten bestätigt, daß es sich bei den fraglichen Daten um Meldedaten der ehemaligen DDR handle, deren Weiternutzung einer gesetzlichen Grundlage bedürfe[30].

Abgeordnete verschiedener Bundestagsfraktionen legten im September mit einem Änderungsantrag für das StUG die für die Weiternutzung erforderliche gesetzliche Regelung vor. Die Datenschutzbeauftragten der fünf neuen Bundesländer und Berlins haben dieser Gesetzesinitiative mit einigen Verbesserungsvorschlägen zugestimmt. Anfang Oktober ist der Änderungsantrag im Innenausschuß des Deutschen Bundestages verabschiedet worden und an den Rechtsausschuß mit der Empfehlung, ihm zuzustimmen, weitergeleitet worden. Die Mitglieder des Rechtsausschusses sind dem jedoch nicht gefolgt. In einer Bundesratsempfehlung gewähren sie vielmehr auch den Gerichten und Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben die Nutzungsbefugnis für den Datenbestand. Damit haben sie einen Beschluß ihrer Amtsvorgänger aus dem Jahre 1976 für die Bürger der ehemaligen DDR außer Kraft gesetzt. Damals hatte der Rechtsausschuß des Deutschen Bundestages befunden, daß sich die zentrale Registrierung aller Bürger und die Abrufbarkeit ihrer Daten nicht mit einer demokratischen Gesellschaftsordnung vertragen.

Der Bundesrat ist der Empfehlung des Rechtsausschusses gefolgt, so daß mit dem vorgesehenen StUÄndG nicht nur der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und die Zentrale Ermittlungsstelle von Regierungs- und Vereinigungskriminalität (ZERV) der reduzierte Meldedatenbestand der ehemaligen DDR zu ihrer Aufgabenerfüllung zur Verfügung steht, sondern auch den Gerichten und Strafverfolgungsbehörden. Daß Gerichte und Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben auf Meldedaten angewiesen sind, ist unbestritten. Dazu haben sie jedoch - den gesetzlichen Vorschriften entsprechend - in den neuen ebenso wie in den alten Bundesländern Zugriff auf die Melderegister der Gemeinden. Ein zentrales Melderegister sowie eine PKZ sind verfassungswidrig.

Die ursprüngliche von den Datenschutzbeauftragten der fünf neuen Bundesländer und Berlins mitgetragene Absicht, einen reduzierten Meldedatenbestand von der Vernichtung auszunehmen, damit nur der BStU und die ZERV ihn im engen und zeitlich befristeten Rahmen ihrer Aufgabenerfüllung nutzen können, ist durch die verabschiedete Regelung aufgehoben.

Die so nun u. a. auch für die Bürger der ehemaligen DDR geltende Sonderregelung ist nicht mehr mit der besonderen geschichtlichen Situation des Einigungsprozesses zu begründen, da sie nur für die Verfolgung zukünftiger Straftaten wirksam wird. Ich halte dies auch im Hinblick auf den schwierigen Einigungsprozeß, der einheitliche rechtliche Bedingungen für alle Bürger voraussetzt, für bedenklich.

29

30 LT-Drs. 1/2074

Protokoll der mündlichen Verhandlung vom 19. August 1993

3.1.5 Das Widerspruchsrecht des Betroffenen

Anläßlich der Eingabe eines Bürgers hatte ich festzustellen, daß bei der Schulabgangsuntersuchung seiner minderjährigen Tochter ein psychologisches Gutachten von Anfang 1989 verwendet worden war. Dieses Gutachten war dem damals zuständigen Jugend- und Gesundheitsschutzamt übermittelt worden und von dort an das Jugendamt des Landkreises gelangt.

Die Verwendung des Gutachtens erfolgte offensichtlich in Unkenntnis der Bestimmungen der §§ 35 und 36 Bbg DSG. Nach § 35 Abs. 1 Nr. 3 setzt eine weitere Nutzung personenbezogener Daten aus ehemaligen Einrichtungen zwingend voraus, daß der Betroffene der Verarbeitung nicht widersprochen hat. Er ist deshalb vor einer weiteren Verarbeitung seiner Daten gem. § 36 Abs. 2 Bbg DSG über deren Herkunft, die Art der ursprünglichen Verwendung, die Art und den Umfang der beabsichtigten weiteren Verarbeitung, die nunmehr zuständige datenverarbeitende Stelle sowie über das ihm zustehende Widerspruchsrecht zu unterrichten. Macht der Betroffene von seinem Widerspruchsrecht Gebrauch, so sind die Unterlagen mit den auf ihn bezogenen Daten aus ehemaligen Einrichtungen gem. § 37 Abs.1 Bbg DSG in Verbindung mit § 4 Abs. 1 und Abs. 2 Nr. 2 Brandenburgisches Archivgesetz[31] dem jeweils zuständigen öffentlichen Archiv anzubieten und bei einer Verneinung der Archivwürdigkeit (§ 5 Abs. 3 Bbg ArchivG) zu löschen. Letzteres gilt nicht für medizinische Unterlagen, da diese gem. Runderlaß (s. unter 7.2.1) 10 Jahre aufbewahrt werden müssen.

Macht der Betroffene von seinem Widerspruchsrecht keinen Gebrauch, so ist die weitere Verwendung von personenbezogenen Daten aus ehemaligen Einrichtungen gleichwohl nur insoweit zulässig, als die Kenntnis der Daten zur rechtmäßigen Erfüllung einer in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgabe erforderlich ist und die erneute Erhebung der Daten einen unverhältnismäßig hohen Aufwand darstellen würde (§ 35 Abs. 1 Nr. 1 und 2 Bbg DSG). Ferner muß die Zuständigkeit und Verantwortlichkeit der datenverarbeitenden Stelle eindeutig bestimmt sein (§ 35 Abs. 1 Nr. 4 Bbg DSG).

Die der Regelung im Brandenburgischen Datenschutzgesetz entsprechende Unterrichtung des Petenten wurde "nachgeholt". Der Landkreis hat mir versichert, daß die Mitarbeiter des Gesundheitsamtes aufgrund des Vorfalls ausführlich über die gesetzlichen Bestimmungen informiert worden seien. Da ich somit davon ausgehen konnte, daß sich ein vergleichbarer Verstoß gegen den Datenschutz bei dem betreffenden Gesundheitsamt nicht wiederholen wird, habe ich von einer Beanstandung abgesehen.

3.2 Personaldaten

3.2.1 Übergabe von Personalakten nach Übergang der Trägerschaft

Mit Übergang der Berufsfeuerwehr eines Landkreises in die Trägerschaft einer kreisfreien Stadt war die Stadt auch als neuer öffentlicher Arbeitgeber in die bestehenden Arbeitsverhältnisse eingetreten. Der Bürgermeister dieser Stadt fragte bei mir an, ob bei dieser Betriebsübernahme entsprechend den Bestimmungen des Bürgerlichen Gesetzbuches (BGB) auch die bislang beim Landkreis geführten Personalakten der Mitarbeiter der Berufsfeuerwehr an die Stadt übergeben werden müssen.

In meiner Antwort stellte ich darauf ab, daß der Übergang der Trägerschaft aufgrund einer materiell-rechtlichen Vorschrift, zumindest aber ordnungsgemäß auf der Grundlage einer

---

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

Verwaltungsvereinbarung mit Übergabeprotokoll erfolgt ist und damit nicht nur die Übernahme von Betriebsmitteln, sondern auch die Übernahme des Personals unter Fortführung der bestehenden Arbeitsverhältnisse verbunden war. Nach § 613a BGB gehen mit Übergang eines Betriebes gleichzeitig die Rechte und Pflichten aus den im Zeitpunkt des Übergangs bestehenden Arbeitsverhältnissen auf den neuen Inhaber über. Dies trifft auch für juristische Personen des öffentlichen Rechts zu.

Mit dem Übergang der Rechte und Pflichten an den bestehenden Arbeitsverhältnissen war auch die aus § 13 BAT-O[32] zu schließende Verpflichtung des Arbeitgebers, die Personalakten zu führen, auf die Stadt übergegangen.

In Ermangelung allgemeinverbindlicher Spezialnormen zum Arbeitnehmerdatenschutz könnte man möglicherweise zu einem anderen Ergebnis kommen, wenn die Arbeitsverhältnisse zuvor aufgelöst und von der Stadt neu begründet worden wären. Da sich aus der Sicht der Mitarbeiter an den Arbeitsverhältnissen jedoch nichts geändert hatte und Spezialvorschriften im Arbeitnehmerbereich zur Behandlung von Personalakten nicht vorliegen, greifen die allgemeinen Bestimmungen des § 29 Bbg DSG zur Datenverarbeitung bei Dienst- und Arbeitsverhältnissen. Hiernach sind die Personalakten in der Weise zu führen, daß dies u. a. zur Durchführung und Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Da ich im vorliegenden Fall davon ausgegangen bin, daß die Personalakten der Mitarbeiter der Berufsfeuerwehr auch bei der Personalverwaltung ihres bisherigen öffentlichen Arbeitgebers, des Landkreises, nur solche Teile enthielten, die eben zu der genannten Aufgabenerfüllung erforderlich waren, konnte darauf geschlossen werden, daß sie auch für die Fortführung der ordnungsgemäßen Aufgabenerfüllung beim neuen öffentlichen Arbeitgeber, der Stadt, unabdingbar sein werden. Insoweit war die uneingeschränkte Fortführung der Personalakten bei der Personalstelle des neuen Arbeitgebers, der Stadt, als gerechtfertigt zu beurteilen. Dabei ist auch in vergleichbaren Fällen die Einwilligung der betroffenen Arbeitnehmer entsprechend § 29 Abs. 1 Satz 3 Bbg DSG nicht erforderlich, da hier lediglich die Übermittlung an künftige Arbeitgeber, also im Zusammenhang mit dem Eingehen neuer Arbeitsverhältnisse,
angesprochen sind.

Im übrigen wäre im geschilderten Fall ein Verbleib der Personalakten beim Landkreis gemäß § 29 Abs. 1 Satz 1 Bbg DSG unzulässig gewesen, da dies nicht mehr zur "Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder einer Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht". Sofern in vergleichbaren Fällen bei Übergang der Trägerschaft auch beamtete Mitarbeiter betroffen sind, würde sich ein Pflicht zur Fortführung der Personalakten durch den neuen Dienstherrn ohne ausdrückliche Zustimmung des Betroffenen aus § 91 Landesbeamtengesetz (LBG) und §128 Abs. 1 Beamtenrechtsrahmengesetz (BRRG)[33] i. V. m. §§ 57 ff. LBG ergeben.

3.2.2 Einsichtnahme in Personalakten vor Trägerwechsel

Im Zusammenhang mit der beabsichtigten Übernahme eines Feierabend- und Pflegeheimes

---

[32] Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften - (BAT-O) vom 10. Dezember 1990, GMBl. 1991, S. 234, zuletzt geänd. am 4. November 1992, GMBl. 1993, S. 63

[33] i.d. Fassung der Bekanntmachung vom 27.Februar 1985, BGBl. III 2030-1

durch die Innere Mission aus der Trägerschaft eines Landkreises hatte das Landratsamt die Heimleitung gebeten, der Inneren Mission zur Vorbereitung der Übernahme und der Gehaltszahlung sowie zur Anpassung der Einstufung Einsichtnahme in die Personalakten zu gewähren. Unter Hinweis darauf, daß anderenfalls die Gehaltszahlungen nach Trägerwechsel vorerst nur als Abschlagszahlung erfolgen könnten, bat das Landratsamt, zuvor die schriftliche Zustimmung der Mitarbeiter zur Einsichtnahme in ihre Personalakte einzuholen. Die Heimleitung hatte datenschutzrechtliche Bedenken, dieses Verfahren durchzuführen, und bat mich um meine Beurteilung.

Nach § 29 Bbg DSG ist eine Datenübermittlung, also auch die Einsichtnahme in Personaldaten, an einen künftigen Dienstherrn oder Arbeitgeber nur mit Einwilligung der Betroffenen zulässig. Insoweit war gegen das vorgeschlagene Verfahren grundsätzlich nichts einzuwenden. Da situationsbezogen über die Mitarbeiter ein faktischer Zwang ausgeübt worden wäre, habe ich die Heimleitung darauf hingewiesen, daß auch bei grundsätzlicher Zulässigkeit das Erforderlichkeitsprinzip zu beachten sei. Danach konnte es genügen, zunächst eine tabellarische Aufstellung lediglich der personenbezogenen Daten vorzunehmen, die zur Zahlbarmachung der Gehälter erforderlich wären, wobei sich der Umfang der insoweit benötigten Daten exakt festlegen ließe.

3.2.3 Erlaubte Weitergabe der privaten Anschrift von Mitarbeitern des öffentlichen Dienstes

Auch Mitarbeiter des öffentlichen Dienstes haben regelmäßig einen grundsätzlichen Anspruch darauf, in ihrer Privatsphäre insoweit geschützt zu sein, daß von ihrem öffentlichen Arbeitgeber bzw. Dienstherrn ihre privaten Anschriften und Telefonnummern nicht weitergegeben werden dürfen. Es gibt jedoch Ausnahmen:

In einer Eingabe beklagte der Hausmeister einer Schule, daß die dortige Direktorin seine Anschrift an Dritte weitergegeben habe. Darüber hinaus habe das zuständige Schulamt ihm gegenüber sogar die Auffassung vertreten, es dürfe seine Adresse sogar öffentlich in dem Schulgebäude ausgehängt werden. Der Petent sah sich dadurch in seiner Privatsphäre verletzt und war der Meinung, daß ihm im übrigen von seinem öffentlichen Arbeitgeber ein Diensttelefon zur Verfügung gestellt werden müsse.

Hintergrund des Sachverhalts war, daß der Petent nicht in der Schule selbst, sondern in einiger Entfernung von seinem Arbeitsplatz wohnt. Die Frage, ob es sich dabei um eine vom Arbeitgeber gestellte Dienstwohnung oder um eine Privatwohnung handelt, war im Ergebnis meiner datenschutzrechtlichen Prüfung ohne Belang. Bei dem Namen, der Anschrift und beruflichen Stellung einer/eines Bediensteten handelt es sich um Einzelangaben über deren/ dessen persönliche und sachliche Verhältnisse und somit um personenbezogene Daten i.S.v. § 3 Abs.1 Bbg DSG. Solche Daten dürfen bei Beschäftigten gem. § 29 Abs. 1 Bbg DSG nur verarbeitet werden, wenn dies u.a. zur Durchführung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Eine Übermittlung solcher Daten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat (§ 29 Abs. 1 Satz 2 Bbg DSG).

Ich mußte den Petenten darauf hinweisen, daß er die Weitergabe seiner Anschrift durch die Direktorin an private Dritte im Zusammenhang mit seinen Aufgaben als Schulhausmeister sehen müsse. Aus meiner Sicht erfordert es der Beruf eines Hausmeisters, daß dieser, soweit es um Belange geht, die das Schulgebäude betreffen, für Dritte erreichbar sein muß. Insoweit sah ich es als Inhalt des Arbeitsverhältnisses an, daß - im Hinblick auf seine Stellung - die Privatanschrift zugleich auch seine Dienstanschrift ist, auch wenn es sich um keine Dienstwohnung handeln sollte. Deshalb war aus datenschutzrechtlicher Sicht nicht zu beanstanden, daß die Anschrift des Petenten im Schulgebäude so ausgehängt war, daß er in Not- und Alarmfällen von Personen, die sich in der Schule aufhalten, so erreicht werden

kann, wie man es auch bei einer Dienstwohnung erwarten würde.

Dies muß auch für eine Mitteilung der Anschrift eines Schulhausmeisters an dritte Personen gelten, wenn die Mitteilung in unmittelbarem Bezug zu den Aufgaben eines Hausmeisters erfolgt. Nur wenn nachweislich ein dienstlicher Zusammenhang mit telefonischen Auskünften nicht bestehen sollte, wären diesbezügliche Informationsweitergaben an Dritte durch datenschutzrechtliche Bestimmungen nicht gedeckt. Da aber in jedem Fall im einzelnen Auskünfte nur gegeben werden dürfen, wenn die zuvor genannten Voraussetzungen eines dienstlichen Zusammenhangs bestehen, habe ich dem Petenten mitgeteilt, daß aus datenschutzrechtlicher Sicht nicht gefordert werden kann, daß ihm von der Schulverwaltung ein Diensttelefon im privaten Bereich installiert wird.

3.2.4 Überprüfung von Beschäftigten

In zunehmendem Maße beschweren sich Bedienstete der öffentlichen Verwaltung des Landes bei mir, daß sie durch eine Anfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) überprüft werden sollen, obwohl sie aus den alten Bundesländern stammen. Bereits im Vorjahr hatte ich berichtet (s. 1. Tätigkeitsbericht unter 5.3.1 und 5.3.3), daß hierfür tatsächlich keine ausreichende Rechtsgrundlage gegeben ist. Dieser Auffassung konnte sich die Landesregierung in ihrer Stellungnahme zu meinem letzten Tätigkeitsbericht zwar noch nicht anschließen, jedoch muß ich uneingeschränkt an meiner Rechtsauffassung festhalten. Sie wird vom Grundsatz her auch von meinen Kollegen in den anderen neuen Bundesländern einschließlich Berlin geteilt.

Das datenschutzrechtliche Anliegen ist es nicht, eine durchaus wünschenswerte Gleichbehandlung von Mitarbeitern aus den neuen und alten Bundesländern zu verhindern. Es geht allein darum, daß die Verfahren entsprechend den datenschutzrechtlichen Erfordernissen auf eine eindeutige Rechtsgrundlage gestellt werden.

Eine solche ist im Einigungsvertrag[34] jedoch nur für die Überprüfung einer eventuellen Zusammenarbeit mit dem Ministerium für Staatssicherheit bei solchen Mitarbeitern und Bewerbern gegeben, die innerhalb der letzten zwei Jahre vor dem Vereinigungstag ihren Wohnsitz oder gewöhnlichen Aufenthaltsort im Betrittsgebiet hatten. Bei diesem Personenkreis wird die Anfrage nicht auf die Einwilligung der Betroffenen abgestellt.

Für den übrigen Personenkreis fehlt eine gesetzliche Regelung. Irrig ist anzunehmen, daß die fehlende Befugnisnorm durch Einwilligungserklärungen der Betroffenen ersetzt werden kann. Das Stasi-Unterlagen-Gesetz (StUG)[35] enthält zwar Vorschriften darüber, für welche Zwecke Informationen von der "Gauck-Behörde" aus den Stasi-Unterlagen verwendet und an wen sie übermittelt werden dürfen. Es enthält jedoch keine Regelungen darüber, in welchen Fällen öffentlich Bedienstete durch eine dortige Anfrage überprüft werden dürfen. Insoweit ist die Abfrageberechtigung für den nicht über den Einigungsvertrag erfaßten Personenkreis rechtlich nicht hinreichend geregelt. § 21 Abs. 1 Nr. 6 StUG sieht Überprüfungen bei dort nachfolgend genannten Personen nur nach Maßgabe "der dafür geltenden Vorschriften" vor. Damit setzt das StUG Datenerhebungsbefugnisse voraus, die die Vorschrift selbst nicht enthält. Solche Befugnisse lassen sich normenklar aber auch weder aus allgemeinen Grundsätzen des Beamtenrechts ableiten, noch aus § 8 Bundesangestelltentarifvertrag

---

[34] vom 31. August 1990, BGBl. II, S. 889 in Anl. I Kap. XVIV Sachgeb. A Abschn. III

[35] vom 20. Dezember 1991, BGBl. I, S. 2272

(BAT)[36] oder § 9 Landesbeamtengesetz (LBG)[37], wonach Betroffene sich zur freiheitlich-demokratischen Grundordnung zu bekennen bzw. die Gewähr dafür zu bieten haben, sich jederzeit für diese einzusetzen. Auch sind die in § 13 Abs. 2 Nr. 2 Bundesdatenschutzgesetz (BDSG)[38] alternativ genannten Voraussetzungen nicht erfüllt.

Im übrigen führt ein Appell an den betroffenen Personenkreis zu keiner datenschutzgerechten Lösung, da die Betroffenen Benachteiligungen befürchten könnten. Außerdem kann eine Einwilligung die Befugnis zur beabsichtigten Datenverarbeitung nicht ersetzen. Aus genannten Gründen ist der Gesetzgeber aufgerufen, hier eine geeignete landesweit greifende Befugnisnorm zu schaffen.

---

[36] vom 23. Februar 1961, GMBl., S. 137, zuletzt geänd. durch Tarifvertrag vom 12. Februar 1993, GMBl., S. 317

[37] vom 24. Dezember 1992, GVBl. I, S. 506

[38] vom 20. Dezember 1990, BGBl. I, S. 2954

3.3 Landespersonalvertretungsgesetz

Das Landespersonalvertretungsgesetz (PersVG)[39] enthält keine normenklare Rechtsvorschrift für die Verarbeitung personenbezogener Daten durch den Personalrat und den Wahlvorstand für die Personalratswahl. Bereichsspezifische Einschränkungen ergeben sich für den Personalrat jedoch insbesondere aus §§ 60 Abs. 3 bis 4, 62 Abs. 4 und 5 sowie 94 Abs. 3 PersVG. So können Personalaktendaten vom Personalrat nur mit Zustimmung des Betroffenen verarbeitet werden (§ 60 Abs. 3 Satz 2 und 3 PersVG) und dürfen ihm bei Einstellungen die Bewerbungsunterlagen nur in dem für die Wahrnehmung seiner Beteiligungsrechte erforderlichen Umfang zur Verfügung gestellt werden (§ 60 Abs. 2 PersVG). Personenbezogene Daten, die beim Personalrat bei der Erfüllung seiner Aufgaben anfallen, sind zu löschen, sobald sie zur Aufgabenerfüllung nicht mehr erforderlich sind (§ 94 Abs. 3 Pers VG).

Der Mitbestimmung des Personalrats unterliegen gem. § 65 Nr. 1 und 2 PersVG die Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung sowohl von automatisierten Verarbeitungen personenbezogener Daten der Beschäftigten - soweit es sich nicht um Besoldungs-, Vergütungs-, Lohn- und Versorgungsleistungen oder Beihilfen handelt - als auch von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.

Dem von der Dienststellenleitung bestellten behördlichen Datenschutzbeauftragten werden gegenüber dem Personalrat dieselben Kontrollbefugnisse eingeräumt, wie sie gegenüber der Dienststelle bestehen (§ 94 Abs. 1 PersVG); zur Wahrung der personalvertretungsrechtlichen Autonomie gegenüber der Dienststellenleitung sieht § 66 Nr. 6 PersVG "im Gegenzug" vor, daß der Personalrat bei der Bestellung des behördlichen Datenschutzbeauftragten mitbestimmt, so daß in seinem Bereich die datenschutzrechtliche Kontrolle nur durch einen Beschäftigten der Diensstelle ausgeübt werden kann, der auch das Vertrauen der Personalvertretung genießt.

In § 94 Abs. 2 PersVG wird klargestellt, daß der Personalrat das Recht hat, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden.

Obgleich auf Empfehlung des Innenausschusses die von mir in einer ersten Stellungnahme angesprochenen Punkte bei der Endfassung des Gesetzestextes berücksichtigt wurden, ergibt eine Überprüfung der Regelungen zur Datenverarbeitung durch den Personalrat insbesondere im Hinblick auf § 41 Abs. 2 Bbg DSG einen datenschutzrechtlichen Nachbesserungsbedarf.

3.4 Meldewesen

3.4.1 Erste Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden

Im Berichtszeitraum ist mir der Entwurf der 1. Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörde (1.MeldDÜÄV)[40] mit der Bitte um Stellungnahme zugegangen. Unter Nummer 8 ist der § 14 in die MeldDÜÄV aufgenommen worden, gegen den sich nicht nur datenschutzrechtliche, sondern auch verfassungsrechtliche Bedenken erheben.

39

40 vom 15. September 1993, GVBl. I, S. 358
vom 8. Dezember 1993, GVBl. II, S. 776

Die Vorschrift soll allen Ämtern derselben Verwaltungseinheit Zugriff auf das gesamte Melderegister ermöglichen. Im einzelnen sind das die in § 3 Abs. 1 Meldegesetz (BbgMeldeG)[41] enthaltenen und über den Datensatz des § 28 Abs. 1 BbgMeldeG, der die Übermittlungen an andere Behörden und öffentliche Stellen regelt, hinausgehenden Merkmale, wie z. B.

- erwerbstätig/nicht erwerbstätig,

- gesetzliche Vertreter (Vor- und Familienname, akademische Grade, Anschrift, Tag der Geburt),

- Zugehörigkeit zu einer Religionsgemeinschaft,

- Ehegatte (Vor- und Familienname, akademische Grade, Anschrift, Tag der Geburt, Sterbetag),

- minderjährige Kinder (Vor- und Familienname, Tag der Geburt, Sterbetag),

- Ausstellungsbehörde, -datum, Gültigkeitsdauer des Personalausweises/-passes.

Vom Ministerium des Innern (MdI) wurde dies so interpretiert, daß sie damit allen Verwaltungsbereichen einer Kommune - von der Wohngeldstelle über das Liegenschaftsamt bis zur Kämmerei - zur Verfügung stehen. Ausgenommen sind nur diejenigen Bestandteile des Datensatzes, die die Meldebehörden für die in § 3 Abs. 2 BbgMeldeG aufgezählten Zwecke speichert. Hier wird der Zugriff mit Verweis auf die Regelungen des § 28 Abs. 2 BbgMeldeG beschränkt. Eingegrenzt wird die Übermittlung weiterhin durch den Verweis auf die Erforderlichkeit, die als Voraussetzung für die Übermittlung in § 28 Abs. 1 BbgMeldeG normiert ist.

Es ist fraglich, ob diese Interpretation dem funktionalen Behördenbegriff noch Rechnung trägt, der nach allgemein herrschender Rechtsauffassung die Informationsbeziehungen innerhalb einer Verwaltungseinheit kennzeichnet und sowohl im Brandenburgischen Datenschutz- als auch im Meldegesetz ausformuliert ist. Der Begriff "Verwaltungseinheit" ist umfassender als der der "speichernden Stelle". Keinesfalls kann darunter jedoch die gesamte Verwaltung einer Kommune verstanden werden. "Speichernde Stelle" im Sinne des Datenschutzgesetzes ist nicht die Verwaltungseinheit, der die Meldebehörde angehört, sondern die Meldebehörde selbst, die zu ihrer Aufgabenerfüllung Daten zweckgebunden erhebt und speichert. Die zur Aufgabenerfüllung erforderlichen Datenübermittlungen - also die Durchbrechung der Zweckbindung - sind nur im Rahmen des Meldegesetzes gestattet.

Ebenso ist zu fragen, ob die vorliegende Regelung nicht Art. 80 Grundgesetz verletzt, indem sie über den im Gesetz festgelegten Inhalt und das Ausmaß der Rechtsverordnungsermächtigung hinausgeht. Das MdI ist jedoch als Verordnungsgeber an die Gesetze und inbesondere auch an die Beschränkungen, die die gesetzliche Ermächtigung aufstellt, gebunden.

§ 29 Abs. 2 BbgMeldeG, den die vorliegende 1.MeldDÜÄV als Ermächtigungsregelung zitiert, legt fest, daß das MdI eine Rechtsverordnung zur regelmäßigen Datenübermittlung nur im Rahmen des § 28 Abs. 1 und 2 BbgMeldeG erlassen kann, die darüber hinaus Anlaß, Zweck und die jeweils zu übermittelnden Daten festlegen muß.

Mit dem vorliegenden Entwurf der 1.MeldeDÜÄV wird den Intentionen des Gesetzgebers

---

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

nicht mehr Rechnung getragen. Dieser sah in dem einschlägigen § 28 BbgMeldeG vor, daß anderen Behörden oder öffentlichen Stellen - vorausgesetzt dies ist zur Aufgabenerfüllung erforderlich - im Regelfall nur ein gegenüber § 3 Abs. 1 BbgMeldeG um die oben aufgeführten Merkmale reduzierter Datensatz übermittelt wird. Die in § 28 Abs. 2 BbgMeldeG unter bestimmten Voraussetzungen gestatteten Ausnahmen werden nun ohne die erforderlichen Festlegungen zum Regelfall für alle Behörden der Verwaltungseinheit.

Das Ministerium hat die von mir erhobenen Bedenken übernommen und die 1.MeldDÜÄV entsprechend geändert. Durch die Novellierung des Melderechtsrahmengesetzes (s. unter 3.4.3) ist unterdessen allerdings eine Ermächtigungsgrundlage für den § 14 geschaffen, vorausgesetzt der brandenburgische Gesetzgeber übernimmt die Ermächtigung in das BbgMeldeG. Damit wären zwar die verfassungsrechtlichen Bedenken gegen das Regelungsverfahren ausgeräumt. Die Regelung entspricht aber dessen ungeachtet datenschutzrechtlichen Anforderungen nicht. Da ihr jedoch bislang weder das BbgMeldeG noch die 1.MeldDÜÄV angepaßt wurden und mir auch eine entsprechende Absicht des MdI nicht bekannt ist, wird an dieser Stelle darauf nicht eingegangen. Nach derzeitiger Rechtslage kann die brandenburgische Verwaltung mit den Meldedaten auf keinen Fall so verfahren, als wäre die Verwaltungseinheit, der die Meldestelle angehört, in ihrer Gesamtheit "speichernde Stelle" des Melderegisters.

3.4.2 Personalausweisgesetz

Der von der Landesregierung im Berichtszeitraum vorgelegte Entwurf eines Personalausweisgesetzes für das Land Brandenburg (BbgPAuswG-E) entsprach in seinen datenschutzrechtlichen Regelungen im allgemeinen dem bundesweiten Standard. Das Gesetz ergänzt die bundesrechtliche Regelung des Gesetzes über die Personalausweise[42]. Für § 4 Abs. 5 Satz 3 Bbg PauswGE gilt dies aber nicht.

Diese brandenburgische Sonderregelung in § 4 Abs. 5 Satz 3 BbgPAuswG-E hatte ich kritisiert. Sie ist eine Auffangvorschrift für die aus dem Einigungsprozeß herrührenden Besonderheiten des Personalausweiswesens im Land Brandenburg. Damit erhalten die Personalausweisbehörden die Befugnis, bei Beantragung eines Personalausweises immer dann die Vorlage weiterer geeigneter Unterlagen verlangen zu können, wenn Zweifel an der Richtigkeit der im Personalausweisregister gespeicherten Daten bestehen. Die Begründung führt dazu aus, daß damit die unterschiedlichen melderechtlichen Vorschriften der ehemaligen DDR und der alten Bundesländer ausgeglichen werden, die u. a. zur Folge haben, daß im Personalausweisregister bestimmte Daten (z. B. weitere Vornamen) fehlen.

Die Personalausweisgesetze der anderen Bundesländer bzw. die bundesrechtliche Vorschrift verlangen die Vorlage weiterer geeigneter Unterlagen nur, wenn Zweifel an der Identität des Antragstellers bestehen. Nur der brandenburgische Antragsteller muß, ohne daß diese zum Nachweis seiner Identität erforderlich wären, immer auch dann der Verwaltung mehr Daten liefern - und tiefere Eingriffe in seine Persönlichkeitsrechte hinnehmen - , wenn ohne sein Verschulden die Datensammlungen der Verwaltung nicht in Ordnung sind.

Ich habe dagegen angeführt, daß Vorschriften, die nur auf die besondere Situation in den neuen Bundesländern zurückzuführen sind und die eine Schlechterstellung der Betroffenen gegenüber den Einwohnern der Altbundesländer bewirken, nicht auf Dauer gelten können. Um die Personalausweisregister an den Standard der Altbundesländer anzugleichen, sind vom brandenburgischen Bürger tiefere Eingriffe in das Recht auf informationelle Selbstbestimmung nur für eine bestimmte Übergangsfrist hinnehmbar. Ich habe dafür

---

42 i. d. Fassung der Bekanntmachung vom 21. April 1986, BGBl. I, S. 548

entsprechend den Regelungen des Einigungsvertrags[43] den Zeitraum bis 31.12.1995 vorgeschlagen. Bis dahin sollte die Verwaltung in der Lage sein, sowohl die Melderegister als auch die Personalausweisregister an den bundesdeutschen Standard anzupassen, und so zur Gleichbehandlung der Bürger in beiden Teilen Deutschlands beitragen. Der Gesetzgeber ist meinen Vorschlägen nicht gefolgt.

3.4.3 1. Gesetz zur Änderung des Melderechtsrahmengesetzes

Zwischenzeitlich ist das 1. Gesetz zur Änderung des Melderechtsrahmengesetzes (MRRG)[44] in Kraft getreten. Dieses Gesetz zeichnet sich zunächst dadurch aus, daß mit ihm die aus datenschutzrechtlicher Sicht nicht erforderliche sog. Hotelmeldepflicht (§ 16 Abs. 2 MRRG) nicht abgeschafft wurde. Ferner wurde mit der Änderung des § 22 Abs.1 MRRG die Erteilung einer einfachen Melderegisterauskunft an Parteien und Wählergruppen im Zusammenhang mit Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament nicht, wie aus datenschutzrechtlicher Sicht zu fordern war, von einer ausdrücklichen Zustimmung der Betroffenen abhängig gemacht; vielmehr sieht die gesetzliche Neuregelung lediglich ein Widerspruchsrecht vor. Dem entspricht bereits die Regelung in § 33 Abs. 1 des Brandenburgischen Meldegesetzes (s. unter 3.4.4.1).

Von besonderer Bedeutung für das Land Brandenburg ist die in das MRRG eingefügte Bestimmung des § 24 MRRG. Dadurch wird es den neuen Bundesländern erlaubt, soweit die nach den Meldegesetzen zulässigen Datenübermittlungen an andere öffentliche Stellen wegen der besonderen Art der Speicherung im Melderegister nicht oder nur mit unverhältnismäßig hohem Aufwand möglich sind, für die Zeit bis zum 31. Dezember 1996 durch Landesgesetz zu bestimmen, daß die für den Polizeivollzugsdienst zuständigen Behörden befugt sind, bei Vorliegen der sonstigen Übermittlungsvoraussetzungen Einsicht in die bei den Meldebehörden gespeicherten Daten zu nehmen (sog. "Schlüssellösung", s. unter 3.6.3).

Dies ist im Klartext so zu verstehen, daß das Rahmenrecht des Bundes es auch dem brandenburgischen Gesetzgeber freistellt, es dem jeweils zuständigen Polizeibeamten rechtlich zu ermöglichen, sich vom Pförtner den Schlüssel zur Meldestelle aushändigen zu lassen und außerhalb der normalen Dienstzeit Einsicht in das Melderegister zu nehmen.

Will man nicht bereits den bloßen Hinweis auf die angeblich besonderen Bedingungen in den neuen Bundesländern als Begründung genügen lassen, so bleibt diese den Datenschutz der Bürgerinnen und Bürger in den neuen Bundesländern gegenüber dem Standard im alten Bundesgebiet herabsetzende bundesrechtliche Regelung ihre sachliche Rechtfertigung aus datenschutzrechtlicher Sicht letztlich schuldig. Zwar ermöglicht sie es, eine bekanntermaßen bereits längst geübte Praxis gesetzlich zu legitimieren. Eben diese Praxis ist jedoch in den neuen Bundesländern grundsätzlich ebensowenig erforderlich wie in den alten Bundesländern und sollte daher vom Gesetzgeber auch nicht (mehr) gestattet werden.

3.4.4 Vorbereitung der Kommunalwahlen

3.4.4.1 Handhabung des Widerspruchsrechts

§ 33 Abs. 1 Meldegesetz (BbgMeldeG) befugt die Meldebehörden, den Parteien, Wählergemeinschaften und Einzelbewerbern im Zusammenhang mit Wahlen zum Deutschen

---

43 vom 31. August 1990, BGBl. II, S. 889: Anl. 1 Kap. 2 Sachgeb. B Abschn. III Nr. 8, EVertr. zuletzt geänd. am 20. August 1992, BGBl. I, S. 1546

44 vom 11. März 1994, BGBl. I, S. 569

Bundestag, zum Europäischen Parlament und zu Landtags- und Kommunalwahlen sechs Monate vor der Wahl

- Familiennamen,
- Vornamen,
- akademische Grade und
- gegenwärtige Anschriften

der wahlberechtigten Bürger zu übermitteln. Gem. § 33 Abs.1 BbgMeldeG haben die Bürger das Recht, dieser Datenweitergabe zu widersprechen. Die Meldestellen sollen die Bürger bei der Anmeldung auf ihr Recht hinweisen.

Rechtzeitig vor der für den 05.12.1993 festgesetzten Kommunalwahl hat das Ministerium des Innern (MdI) die Gemeinden auf die am 04.06.1993 ablaufende Widerspruchsfrist hingewiesen und sie aufgefordert, die Bürger durch öffentliche Bekanntmachung über ihr Widerspruchsrecht und den Fristablauf zu informieren.

Im Zusammenhang damit haben sich mehrere Bürger an mich gewandt, weil die zuständige Meldestelle ihr Widerspruchsrecht auf zwei Jahre befriste. Für dieses Vorgehen gibt es jedoch keine Rechtsgrundlage. Vielmehr regelt § 33 Abs. 1 BbgMeldeG Datenweitergabe und Widerspruchsrecht der Bürger folgendermaßen:

- In den Sätzen 1-3 ist festgelegt, daß Parteien, Wählergemeinschaften usw. die o. a. Daten der wahlberechtigten Bürger geordnet nach Altersgruppen zur Verfügung gestellt werden können.

- Satz 4 regelt das Widerspruchsrecht der Bürger und bestimmt, daß die Meldebehörde das Widerspruchsrecht nur insoweit befristen darf, als sie einen Zeitpunkt festlegt, bis zu dem erstmalig eingelegte Widersprüche für eine bestimmte Wahl berücksichtigt werden.

- Satz 5 und Satz 6 regelt die Pflichten, die den Parteien, Wählergemeinschaften usw. für den Umgang mit den sog. Wählerlisten auferlegt werden.

- Satz 7 befugt die Meldebehörde, die Herausgabe der Wählerlisten mit zusätzlichen Auflagen zu versehen. Und nur in diesem Zusammenhang ist auch die Frist von zwei Jahren zu verstehen, die sich aus § 32 Abs. 6, auf den in § 33 Abs. 1 Satz 8 BbgMeldeG verwiesen wird, ergibt.

- § 32 Abs. 6 BbgMeldeG regelt, wie mit Auskunftssperren zu verfahren ist, wenn von einem Dritten eine Melderegisterauskunft über einen Betroffenen verlangt wird, der eine Auskunftssperre nach § 32 Abs. 5 BbgMeldeG beantragt und erhalten hat. Diese Auskunftssperren sind auf zwei Jahre befristet und können nur auf Antrag verlängert werden.

- § 33 Abs.1 Satz 8 BbgMeldeG macht durch den Paragraphenverweis darauf aufmerksam, daß Auskunftssperren bei der Erstellung von Wählerlisten zu berücksichtigen sind, d. h. sie dürfen grundsätzlich nicht mit aufgenommen werden.

Die Regelungsabfolge macht deutlich, daß sich die Zweijahresfirst nicht auch auf die Widersprüche der Bürger erstreckt. Da Wahlen üblicherweise alle vier Jahr stattfinden, wäre dies auch die logische Frist für Widersprüche, wenn denn der Gesetzgeber beabsichtigt hätte, die Widersprüche der Bürger zu befristen.

Um die Handhabung des Widerspruchrechts durch die Meldestellen zu überprüfen, habe ich alle Meldestellen des Landes angeschrieben, und sie gebeten, mir das von ihnen gewählte Bekanntmachungsverfahren und die Anzahl der eingelegten Widersprüche mitzuteilen sowie

mir eine Kopie ihrer öffentlichen Bekanntmachung und eine Kopie des Widerspruchsformulars zuzusenden.

In überwiegender Mehrzahl sind die Gemeinden meiner Bitte nachgekommen und haben mir die gewünschten Unterlagen zugesandt. So gut wie alle Gemeinden haben ihre Bürger in öffentlichen Aushängen und durch ihr Gemeindeblatt über das Widerspruchsrecht und den Fristablauf informiert. Worauf die in manchen Gemeinden erstaunlich hohe Anzahl von Widersprüchen (z. B. 84 in einer Kleinstadt) zurückzuführen ist, ließ sich anhand der Unterlagen nicht festmachen.

3.4.4.2 Abgleich mit dem Bundeszentralregister

In Vorbereitung der Kommunalwahlen 1993 hatten die Meldebehörden zur Feststellung eines Ausschlusses vom Wahlrecht oder von der Wählbarkeit bei den als Wahlberechtigte in Betracht kommenden Personen Behördenführungszeugnisse gem. § 31 Bundeszentralregistergesetz (BZRG)[45] beim Bundeszentralregister (BZR) angefordert. In der Folge übermittelte das BZR den Meldebehörden sämtliche sog. Positivauskünfte aus dem Register, d.h. das beantragte Behördenführungszeugnis wurde in allen Fällen erteilt, in denen Eintragungen im BZR vorlagen; nach einer groben Schätzung aus den alten Bundesländern betrifft dies ca. 1 % der Anfragen. Eine Vorprüfung der Eintragungen auf eine etwaige Wahlrechtsrelevanz konnte programmtechnisch nicht vorgenommen werden, so daß sich die Übermittlungen z.B. auch auf Eintragungen zu Entscheidungen von Ordnungsbehörden und zu Wehrerfassungen bezogen. Eine sog. Negativauskunft wurde nicht ausdrücklich erteilt; sie ergab sich jedoch für die Meldebehörden jeweils zwangsläufig aus der Tatsache, daß eine Positivauskunft nicht erteilt wurde. Aufgrund der Anfragen beim BZR ergaben sich für 1.094.400 Einwohner über 18 Jahre 265 Ausschlüsse von der Wählbarkeit und 2 Ausschlüsse vom aktiven Wahlrecht.

Aus datenschutzrechtlicher Sicht war zu diesem Sachverhalt, der in der Öffentlichkeit zu Recht große Beachtung gefunden hat, festzustellen, daß das Vorgehen der Meldebehörden durch die geltenden Rechtsvorschriften nicht gedeckt und deshalb rechtswidrig war. Dies ist inzwischen auch durch die Übergangsregelung im 3. Gesetz zur Änderung des Bundeszentralregistergesetzes (s. unter 3.4.5) bestätigt worden, mit der der Gesetzgeber dem grundsätzlich berechtigten Anliegen, die Rechtmäßigkeit der Wahlen in den neuen Bundesländern sicherzustellen, Rechnung getragen und die für eine Auskunfsterteilung durch das BZR erforderlichen Befugnisnormen in das BZRG aufgenommen hat. Dazu hat nicht zuletzt auch die Unterstützung des datenschutzrechtlichen Anliegens durch die Berichterstattung in den Medien beigetragen, die deutlich gemacht hat, daß die Bürger Brandenburgs nicht mehr bereit sind, gravierende Verletzungen ihres Grundrechts auf informationelle Selbstbestimmung widerspruchslos hinzunehmen. Ich habe zum Wahlabgleich zahlreiche Eingaben besorgter Bürger erhalten.

Ferner war zu beanstanden, daß ich über die beabsichtigte Handhabung der Überprüfung der Wahlberechtigten nicht informiert worden war und so keine Gelegenheit zu einer datenschutzrechtlichen Stellungnahme bereits im Vorfeld der Maßnahme hatte. Vor dem Hintergrund dieser Erfahrung hat der Innenausschuß des Landtags deshalb empfohlen, die Verpflichtungen zur Information und Beteiligung meines Amtes nach dem Brandenburgischen Datenschutzgesetz im Gesetz klarstellend zu präzisieren.

Nachdem den Betroffenen Gelegenheit zur Einsichtnahme gegeben worden war, wurden die

---

45 i. d. Fassung der Bekanntmachung vom 21. September 1984, BGBl. I, S. 1229, ber. 1985 I, S. 195, zuletzt geänd. am 29. Oktober 1992, BGBl. I, S. 1814

vom BZR erteilten Behördenführungszeugnisse zwischenzeitlich von den Meldebehörden vernichtet.

3.4.5 Bundeszentralregisteränderungsgesetz

In den neuen Bundesländern sind in den Melderegistern der Gemeinden Ausschlüsse vom Wahlrecht oder der Wählbarkeit nicht oder nur unvollständig vermerkt, da das in den alten Bundesländern gem. Nr. 12 a der Anordnung über die Mitteilungen in Strafsachen (MiStra)[46] praktizierte Verfahren in den neuen Bundesländern bisher nur in wenigen Fällen angewendet wurde und Entscheidungen vor dem 3. Oktober 1990 von ihm ohnehin nicht erfaßt werden. Um eine ordnungsgemäße Vorbereitung der im Jahr 1994 anstehenden Wahlen zu gewährleisten und insbesondere zur Verminderung des Risikos von Wahlanfechtungen und gegebenenfalls Wahlwiederholungen wegen Teilnahme nicht wahlberechtigter oder nicht wählbarer Personen wollte deshalb der Gesetzgeber die notwendige Aktualisierung der Melderegister in den neuen Bundesländern ermöglichen. Für den dazu erforderlichen Datenabgleich mit dem Bundeszentralregister (BZR) bot das Bundeszentralregistergesetz (BZRG) keine ausreichende Rechtsgrundlage. Durch das 3. Gesetz zur Änderung des Bundeszentralregistergesetzes (3.BZRÄG)[47] sollte die notwendige Rechtsgrundlage in Form einer Übergangsregelung geschaffen werden.

Der Gesetzentwurf der Bundesregierung sah zunächst vor, den Innenministerien der neuen Länder Behördenführungszeugnisse aller volljährigen Bürger ihres Landes zugehen zu lassen. Die Millionenzahl der den Innenministerien danach zu erteilenden und zudem vollständigen Registerauskünfte hätte in keinem Verhältnis zu der nur kleinen Zahl von zu erwartenden Auskünften mit Wahlrechtsrelevanz gestanden (s. unter 3.4.4.2).

Im Einklang mit den Datenschutzbeauftragten des Bundes und der neuen Bundesländer habe ich mich deshalb nachdrücklich sowohl bei der Landesregierung als auch dem Landtag gegen eine solche Regelung ausgesprochen und dabei insbesondere gefordert, daß die Informationen mit Wahlrechtsbezug bereits im BZR herauszufiltern zu seien und Auskünfte über einen Ausschluß des Wahlrechts durch das BZR unmittelbar den zuständigen Meldebehörden übermittelt werden müßten. Eine Filterfunktion der Innenministerien konnte nur für den Fall von Auskünften über Eintragungen akzeptiert werden, die zum Ausschluß der Wählbarkeit führen könnten. Insoweit bestand bislang nämlich beim BZR programmtechnisch keine Möglichkeit, Eintragungen, die sich nur auf die Wählbarkeit beziehen, lückenlos im Registerbestand zu erkennen. Allerdings mußte ausgeschlossen werden, daß die Innenministerien den zuständigen Meldebehörden andere Eintragungen mitteilen können als die, aus denen sich der Ausschluß von der Wählbarkeit ergibt oder ergeben kann. Ferner war eine strikte Begrenzung der Regelung auf die Wahlen im Jahre 1994 zu fordern.

Im Gesetzgebungsverfahren hat sich schließlich ein Formulierungsvorschlag des Bundesbeauftragten für den Datenschutz durchgesetzt. Danach erteilt das BZR gem. §§ 69, 70 BZRG n.F. zur Feststellung eines Ausschlusses vom Wahlrecht auf Antrag Auskunft über die in den neuen Bundesländern bei den Wahlen 1994 wahlberechtigten Personen. Die Anträge sind von den zuständigen Meldebehörden über das jeweilige Innenministerium zu stellen. Die Auskunft wird vom BZR unmittelbar an die zuständigen Meldebehörden erteilt und darf nur solche Eintragungen enthalten, aus denen sich ein Ausschluß der betroffenen Person vom Wahlrecht ergibt. Soweit das Register keine oder andere Eintragungen enthält, wird eine Auskunft nicht erteilt. Eine Verwendung der übermittelten Daten zu anderen Zwecken als dem der Feststellung von Wahlausschlußgründen ist unzulässig.

---

[46]

[47] vom 15. März 1985, BAnz. Nr. 60
vom 9. März 1994, BT-Drs. 190/94

Wird der Antrag beim BZR zur Feststellung eines Ausschlusses der Wählbarkeit gestellt, so wird dem jeweiligen Innenministerium ein sogenanntes Behördenführungszeugnis gem. §§ 31, 32 Abs. 3 BZRG erteilt. Enthält das Register keine Eintragung, die in ein Führungszeugnis für Behörden aufzunehmen ist, teilt das BZR nur dies dem Innenministerium mit. Ein Führungszeugnis wird in diesem Fall nicht erteilt. Anderenfalls prüft das Innenministerium, ob sich aus den in ihm enthaltenen Eintragungen ein Ausschluß von der Wählbarkeit ergibt oder ergeben kann. Ist dies der Fall, so teilt das Innenministerium diese Eintragungen der zuständigen Meldebehörde mit. Andere Eintragungen dürfen nicht mitgeteilt werde. Eine Weiterleitung der Führungszeugnisse ist unzulässig. Wird dem Innenministerium ein Führungszeugnis nicht erteilt oder stellt es fest, daß die Eintragungen im Führungszeugnis einen Ausschluß von der Wählbarkeit nicht ergeben und auch nicht ergeben können, so teilt das Innenministerium der zuständigen Meldebehörde nur mit, daß das Führungszeugnis keine Eintragung im Hinblick auf den Ausschluß von der Wählbarkeit enthält.

Diese schließlich gefundene Regelung ist als praktisch nur durchsetzbarer Ausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung und dem verfassungsrechtlichen Interesse an der Rechtmäßigkeit demokratischer Wahlen zwar auch aus datenschutzrechtlicher Sicht hinnehmbar. Es ist jedoch grundsätzlich bedenklich, daß der Gesetzgeber weiterhin Sonderregelungen für die neuen Bundesländer festschreibt. Angesichts der Gefahr einer weiteren Ungleichbehandlung der Bürgerinnen und Bürger in den neuen Bundesländern durch den Gesetzgeber muß in jedem Einzelfall besonders kritisch geprüft werden, ob dies sachlich wirklich gerechtfertigt ist. Da die Änderung des BZRG all diejenigen Fälle nicht erfaßt, in denen Bürger aus den neuen Bundesländern ihren Wohnsitz in das Gebiet der alten Bundesländer verlegt haben, erscheint mir die sachliche Rechtfertigung für die Ungleichbehandlung durch das 3. Gesetz zur Änderung des BZRG durchaus fragwürdig zu sein. Ich werde vor diesem Hintergrund auch in Zukunft dafür eintreten, daß die aus dem Einigungsprozeß herrührenden und zum Aufbau der Verwaltungen in den neuen Bundesländern zunächst erforderlichen Sonderregelungen, mit denen ein gegenüber dem Niveau in den alten Bundesländern reduzierter Datenschutzstandard in Kauf genommen wurde, nicht festgeschrieben, sondern zur gleichberechtigten Verwirklichung des Grundrechts auf informationelle Selbstbestimmung so bald wie möglich abgebaut werden.

3.4.6 Eingaben

3.4.6.1 Das Blaue Adreßbuch - eine problematische Veröffentlichung

Wie schon im vergangenen haben mich auch in diesem Berichtszeitraum wieder mehrere Eingaben von Bürgern erreicht, die sich darüber beschwerten, daß ihre Anschrift trotz eingelegten Widerspruchs in das Blaue Adreßbuch ihres Wohnorts aufgenommen worden war.

Gem. § 33 Abs. 3 Bbg MeldeG darf die Meldebehörde einem Adreßverlag Familienname, Vorname, akademischer Grad und gegenwärtige Anschrift der Einwohner für die Erstellung eines "Blauen Adreßbuches" zur Verfügung stellen. Ausgenommen sind Einwohner, die das 18. Lebensjahr noch nicht vollendet haben, sowie Insassen von Justizvollzugsanstalten, Krankenhäusern und vergleichbaren Einrichtungen sowie Hotelgäste. Ebenfalls nicht übermittelt werden dürfen die Daten derjenigen Einwohner, die der Weitergabe widersprochen haben (s. 1. Tätigkeitsbericht unter 7.2).

Im Zusammenhang mit dem Blauen Adreßbuch stellte sich die Frage, ob dazu Daten aus dem Gewerberegister einer Stadt an einen Adreßbuchverlag übermittelt werden dürfen. Die Gewerbeämter sind öffentliche Dienststellen des Landes Brandenburg, für die das Bbg DSG gilt, soweit diese personenbezogene Daten in oder aus Dateien oder Akten verarbeiten. Da nach § 3 Bbg DSG personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind, sind hier nur die

Daten derjenigen Gewerbetreibenden problematisch, die unter ihrem natürlichen Namen firmieren (z. B. Heinrich Mustermann OHG).

Für diese Daten kommt § 16 Abs. 1 Buchst. d Bbg DSG als Rechtsgrundlage für die Übermittlung in Frage. Danach ist eine Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs zulässig, wenn sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat. Unstrittig ist, daß eine Veröffentlichung der Gewerbetreibenden im öffentliche Interesse liegt. Entscheidend für die Übermittlung ist allerdings, daß die Betroffenen der Datenverarbeitung nicht widersprochen haben.

In dem an mich herangetragenen Fall vertrat das Ordnungsamt die Auffassung, daß die Datensätze der Gewerbetreibenden, die einer Weitergabe ihrer Daten widersprochen hatten, vor einer Zweitauflage des Adreßbuches aus dem Datenbestand entfernt werden müßten. Bei der Erstauflage des Blauen Adreßbuches hatte die Gemeinde entgegen der Rechtslage einen Datenbestand zur Verfügung gestellt, der auch die Adressen derjenigen Gewerbetreibenden enthielt, die dagegen Widerspruch eingelegt hatten. Sie hatte es dem Verlag überlassen, diese Adressen aus dem zur Veröffentlichung vorgesehenen Bestand herauszufiltern. Dabei waren dem Adreßbuchverlag Fehler unterlaufen. In einem Gespräch mit dem Adreßbuchverlag wurde vereinbart, daß der Verlag dem ihm bereits vorliegenden Altdatenbestand des Gewerbeamtes für eine Zweitauflage - verändert um die eigenen Korrekturen nach Herausgabe der ersten Auflage und unter Berücksichtigung der aufgrund der ersten Auflage dort direkt eingegangenen Widersprüche und Reklamationen - wiederverwenden kann. Eine Briefaktion, in der die Datenaktualität dieser Firmen überprüft wird, kann vom Verlag selbst durchgeführt werden. Da dem Verlag für die Erstauflage entgegen der Rechtslage auch die Datensätze übermittelt wurden, zu denen ein Widerspruch vorlag, muß die genannte Briefaktion auch der nochmaligen Abfrage der Widersprechenden dienen, die mit Hilfe der Bestätigung ihres Widerspruchs eine Veröffentlichung in der zweiten Auflage unterbinden können. Da die Datenübermittlung der Widerspruchsfälle unzulässig war, ist ihre Speicherung und Wiederverwendung bei der Verlagsgesellschaft ebenfalls unzulässig mit der Konsequenz, daß sie gem. § 35 BDSG gelöscht werden müßten. In § 19 Abs. 5 Bbg DSG wird die Pflicht der Behörde zur Unterrichtung der empfangenden privaten Stellen über einen Rechtsmangel davon abhängig gemacht, daß die Unterrichtung keinen erheblichen Aufwand erfordern würde und keine nachteiligen Folgen für die Betroffenen zu befürchten sind. Ich habe es deshalb für vertretbar gehalten, daß von einer Löschung der Daten abgesehen wird. Durch die Abfrageaktion des Verlages werden mögliche Rechtsmängel, die nachteilige Folgen für die Betroffenen haben könnten, geheilt.

Der Verlag ist jedoch gehalten, bei seiner Briefaktion in allen Fällen darauf hinzuweisen, daß

- bei der Erstauflage irrtümlich auch Datensätze des Gewerbeamtes genutzt worden waren, für die dem Gewerbeamt ein Widerspruch vorlag und

- bei der zweiten Auflage nicht nur die hier beim Verlag eingegangenen Widersprüche, sondern auch jeder weitere Widerspruch berücksichtigt wird.

Dies ist bei der Zweitauflage des Blauen Adreßbuches so umgesetzt worden.

3.4.6.2 Gratulation trotz Widerspruchs

Ein Bürger hat sich an mich gewandt, weil ihm in der Regionalzeitung zu einem Jubiläum gratuliert worden war. Die zur Gratulation erforderlichen Angaben hatte die Zeitung von der Meldestelle erhalten. § 33 Abs. 2 Bbg MeldeG befugt die Meldebehörden über Alters- oder Ehejubiläen der Einwohner Auskunft zu erteilen, wenn der Betroffene vor Auskunftserteilung nicht widersprochen hat. Dies hatte der Petent jedoch getan, so daß die Weitergabe seiner Daten an die Zeitung unrechtmäßig war.

Die Gemeinde hat sich bei dem Petenten entschuldigt, nachdem dieser sie auf den Verstoß hingewiesen und mich nachträglich in Kenntnis gesetzt hatte. Weiteres war von mir nicht mehr zu veranlassen

3.4.6.3 Personalausweis mit falscher Hausnummer

Ein Bürger, auf dessen neu ausgestellten Personalausweis eine falsche Hausnummer vermerkt war, bat mich um Unterstützung bei seinen Korrekturbemühungen.

Die Bundesdruckerei nutzt beim Herstellungsverfahren die von den Gemeinden mit den Anträgen zur Erstellung der Personalausweise beigefügten Adreßangaben. Diese Daten werden aus dem aktuellen Meldedatensatz herausgezogen. Auch wenn die Angaben im Meldedatensatz korrekt gespeichert sind, kann es bei der Übertragung auf den Antrag zur Erstellung eines Personalausweises zu Übertragungsfehlern kommen. Gem. § 5 i. V. m. § 18 Bbg DSG ist die Personalausweisstelle verpflichtet, die falschen Angaben zu korrigieren und ggf. zu erläutern, wie es zu der fehlerhaften Eintragung gekommen ist. Ggf. muß auch eine Neuausstellung in Betracht gezogen werden. Gebühren für diese Neuausstellung sollten dem Bürger allerdings nicht in Rechnung gestellt werden.

3.5 Verfassungsschutz

Im Berichtszeitraum habe ich mich in einigen wenigen Bereichen mit der Datenverarbeitung durch die Verfassungsschutzbehörde Brandenburgs befaßt.

3.5.1 Zusammenarbeit mit den Jugendbehörden

So erfuhr ich, daß auf Länderebene geprüft werde, inwieweit eine engere Zusammenarbeit bis hin zur Weitergabe von Informationen über Jugendliche, die der rechten bzw. Skinheadszene zugerechnet werden, zwischen der Verfassungsschutzbehörde und den Jugendbehörden anzustreben sei.

Auf Anfrage teilte die Verfassungsschutzbehörde mit, daß eine regelmäßige und enge Zusammenarbeit mit Jugend- und Sozialbehörden bei der Bekämpfung extremistischer Bestrebungen beabsichtigt sei. In diesem Rahmen sollen auch Informationen über Schwerpunktgebiete, Treffpunkte usw. dieses Personenkreises an die Jugend- und Sozialbehörden weitergegeben werden.

Da die Verfassungsschutzbehörde ausdrücklich betont hat, daß keine personenbezogenen Daten ausgetauscht werden, bestehen gegen die Zusammenarbeit der Verfassungsschutzbehörde mit Jugend- und Sozialbehörden keine datenschutzrechtlichen Bedenken.

3.5.2 Identitätsnachweis bei Anträgen von Bürgern auf Auskunft bzw. Akteneinsicht über die zu ihrer Person gespeicherten Daten

Die Verfassungsschutzbehörde hat sich mit der Frage an mich gewandt, in welcher Weise sie sicherstellen könne, daß tatsächlich nur dem Antragsteller Auskunft über die bei der Behörde zu seiner Person gespeicherten Informationen erteilt wird. Neben besonderen Postzustellungsformen, wie z. B. Einschreiben mit Rückschein oder Postzustellungsurkunde, hat sie dabei auch in Erwägung gezogen, den Antragsteller vor Auskunftserteilung um eine Kopie seines Personalausweises zu bitten.

Letzteres habe ich aus datenschutzrechtlichen Gründen abgelehnt, da es fraglich ist, ob die Verfassungsschutzbehörde, der keine Exekutivbefugnisse zustehen, eine zur Prüfung der

Personalien ermächtigte Behörde gem. § 1 Abs. 1 Personalausweisgesetz[48] ist. Sie kann demnach auch den in § 12 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[49] geregelten Anspruch des Betroffenen auf Aktenauskunft nicht ablehnen, wenn dieser die Bedingung nicht erfüllt, einen Personalausweis vorzulegen, im übrigen aber einen ihm zuordenbaren Antrag stellt. Des weiteren halte ich die Verpflichtung des Antragstellers, der Verfassungsschutzbehörde eine Kopie seines Personalausweises zu überlassen, für eine nicht geeignete und damit auch nicht erforderliche Datenerhebung.

Da das BbgVerfSchG im einschlägigen § 12 keine näheren Regelungen bezüglich des Antrages auf Aktenauskunft gibt und Informationsverarbeitung im übrigen nur in den in § 3 BbgVerfSchG geregelten Fällen zur Erfüllung des Auftrags der Verfassungsschutzbehörde gestattet, kommt für die Informationsverarbeitung bei der Aktenauskunft das Bbg DSG in Frage.

§ 12 Abs. 1 Bbg DSG knüpft die Zulässigkeit der Datenerhebung daran, daß die Kenntnis der Information zur Aufgabenerfüllung erforderlich und für den Zweck geeignet sein muß. Die Kopie des Personalausweises enthält eine Reihe von Angaben (Seriennummer, ausstellende Behörde, Gültigkeitsdatum), deren Kenntnis zur Auskunftserteilung nicht erforderlich ist. Das Schwärzen dieser nicht erforderlichen Angaben bedeutet einen zusätzlichen Verwaltungsaufwand, den die Verfassungsschutzbehörde immer dann erbringen muß, wenn der Antragsteller dies nicht selbst tut. Gem. § 4 Bbg DSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Bbg DSG oder ein anderes Gesetz sie erlaubt oder der Betroffene schriftlich eingewilligt hat. Wollte die Verfassungsschutzbehörde also die o. a. nicht erforderlichen Daten verarbeiten (hier: speichern), bedürfte dies der schriftlichen Einwilligung des Betroffenen.

Die vom Antragsteller zu machenden Personenangaben wie Name, Vorname, Geburtsdatum, Geburtsort, Anschrift reichen aus, um eine Person in manuellen bzw. automatisierten Datensammlungen zu identifizieren und so eine Personenverwechslung zum Nachteil des Antragstellers oder einer anderen Person auszuschließen. Die Gefahr, daß ein Dritter sich unter Verwendung der Personalien eines Betroffenen Auskunft über Informationen erschleichen könnte, die die Verfassungsschutzbehörde über den Betroffenen speichert, lassen sich durch die besonderen Postzustellungsformen vermeiden. Eine zusätzliche Identitätsprüfung des Antragstellers mittels einer Kopie seines Personalausweises wird weder vom Bundesamt für Verfassungsschutz (BfV) noch von den Landesämtern (LfV) vorgenommen.

3.5.3 Mitwirkung im Einbürgerungsverfahren

Im Berichtszeitraum ist durch den Bundesbeauftragten für den Datenschutz die Frage an mich herangetragen worden, inwieweit die Brandenburgische Verfassungsschutzbehörde am Einbürgerungsverfahren beteiligt ist. Dazu hat das Ministerium des Innern mitgeteilt, daß im Land Brandenburg die sog. Regelanfrage an die Verfassungsschutzbehörde "bewußt nicht eingeführt" wurde.

Die Verfassungsschutzbehörde wird nur dann eingeschaltet, wenn das zuständige MdI bei der Bearbeitung eines Einbürgerungsantrags Hinweise erhält, daß der Antragsteller Bestrebungen i.S.d. § 3 Abs. 1 BbgVerfSchG verfolgen könnte. Dies ist in § 16 Abs. 1 BbgVerfSchG geregelt.

---

[48] i.d. Fassung der Bekanntmachung vom 21. April 1986, BGBl. I, 548

[49] vom 5. April 1993, GVBl. I, S. 78

Dagegen habe ich aus datenschutzrechtlicher Sicht keine Einwände erhoben.

3.5.4 Zuverlässigkeitsüberprüfungen nach Luftverkehrsgesetz

Es stellte sich die Frage, wie im Land Brandenburg bei den Zuverlässigkeitsüberprüfungen nach § 29 d Luftverkehrsgesetz (LuftVG)[50] verfahren wird. Dazu hat das zuständige Ministerium für Stadtentwicklung, Wohnen und Verkehr Brandenburg mitgeteilt, daß die Aufgabe der Zuverlässigkeitsüberprüfungen vom Land Brandenburg noch nicht wahrgenommen wird. Im Einigungsvertrag[51] wird das Bundesministerium für Verkehr ermächtigt, Aufgaben nach § 29 Abs. 2 LuftVG für einen Zeitraum von drei Jahren für die neuen Bundesländern auf andere Behörden zu übertragen. Die Zuverlässigkeitsüberprüfung nach § 29 d LuftVG ist dem Bundesministerium des Innern (BMI) übertragen worden. Das Land Brandenburg hat das BMI gebeten, diese Aufgabe bis Ende 1994 an seiner Stelle wahrzunehmen.

Mit dieser Aufgabe ist der Bundesgrenzschutz (BGS) betraut. Diejenigen Personen, für die die Zugangsberechtigung zum Sicherheitsbereich des Flughafens Berlin Schönefeld beantragt worden ist, werden durch INPOL-Fahndungsabgleich auf ihre Zuverlässigkeit überprüft. Dabei wirkt weder die Brandenburgische Verfassungsschutzbehörde mit, noch erfolgt eine Anfrage beim BstU.

3.5.5 G 10-Gesetz

Zu dem Entwurf eines Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz im Land Brandenburg (BbgAG G 10) habe ich in meiner Stellungnahme ausgeführt, daß das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 GG - G 10) die Verarbeitung der personenbezogenen Daten regelt, die der Verfassungsschutz durch Abhörmaßnahmen bzw. durch Eingriffe in das Brief- und Postgeheimnis erlangt. Für abweichende materiell-rechtliche Landesregelungen im Ausführungsgesetz zu G 10 bleibt kein Raum. Für Regelungsbereiche, die, wie z. B. bei der Verantwortung für die Datenübermittlung oder bei der Berichtigung, Löschung und Sperrung von Daten, nicht erfaßt sind, ist das Bbg DSG anwendbar. Darüber hinaus 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 hat. Um dem Gebot in Art. 74 Verfassung des Landes Brandenburg Rechnung zu tragen, sollte im Brandenburgischen Ausführungsgesetz zu G 10 klargestellt werden, daß auch dem Landesbeauftragten für den Datenschutz die Kontrolle von Maßnahmen nach G 10 nach Maßgabe des Bbg DSG und anderer Vorschriften über den Datenschutz obliegt.

Nach dem Gesetzentwurf hat die G 10 - Kommission die Entscheidung darüber zu treffen, ob eine Beschränkung des Brief-, Post- und Fernmeldegeheimnisses durchgeführt wird. Der Vollzug der Beschränkungsmaßnahme ist an die vorherige Zustimmung der Kommission geknüpft. Aus diesem Grund muß die Kommission grundsätzlich vor Vollzug der Maßnahme unterrichtet werden. Um dieser Aufgabe gerecht zu werden, bedarf die Kommission der Möglichkeit, den Sachverhalt zu prüfen. Der Entwurf sollte daher Regelungen enthalten, die klarstellen, daß die Kommission dazu auch bestimmte Eingriffsbefugnisse hat.

---

50 vom 1. August 1922, RGBl. I, S. 681, i.d.F. der Bekanntmachung vom 14. Januar 1981, BGBl. I, S. 61, zuletzt geänd. am 2. Januar 1984, BGBl. II, S. 69

51 vom 31. August 1990, BGBl. II, S. 889: Anl. I Kap. XI Sachgeb. C Abschn. III Nr. 1 b EVertr.

Weiterhin ist geregelt, daß die Kommission erst innerhalb von drei Monaten nach Einstellung einer Beschränkungsmaßnahme über die Mitteilung an den Betroffenen unterrichtet wird. Ich habe vorgeschlagen, im Gesetz zu bestimmen, daß die Kommission monatlich Kenntnis erhalten muß über die Mitteilungen an Betroffene oder über die Gründe, die einer Mitteilung entgegenstehen. Damit soll zum einen der Kommission eine bessere Kontrolle ermöglicht werden. Zum anderen gewährleistet dies dem Betroffenen einen besseren Grundrechtsschutz.

Der Entwurf sieht vor, daß die Parlamentarische Kontrollkommission (PKK), die die Aufgabenerfüllung der Verfassungsschutzbehörde des Landes Brandenburg kontrolliert, von den angeordneten Beschränkungsmaßnahmen sowie über die Mitteilungen an Betroffene, oder über die Gründe, die einer Mitteilung entgegenstehen, unterrichtet wird. Ich habe vorgeschlagen, daß die Kommission dies selbst tun sollte.

3.6 Polizei

Die schon im 1. Tätigkeitsbericht für andere Verwaltungen beschriebenen Verwaltungsstrukturen der ehemaligen DDR und die daraus resultierende Problematik finden sich auch bei der Polizei. Und wie dort gilt es, die zentralistische Verwaltungsorganisation der Volkspolizei der ehemaligen DDR und ihre Informationssammlungen so umzugestalten, daß sie in die dezentralisierte Verwaltung des Landes Brandenburg passen. Dies ist immer noch nicht abgeschlossen.

3.6.1 Organisation

3.6.1.1 Verwaltungsaufbau der ehemaligen Volkspolizei

Die Volkspolizei unterstand dem Ministerium des Innern. Streng hierarchisch aufgebaut, bildete die als Abteilung in das Ministerium des Innern eingegliederte Hauptverwaltung der Deutschen Volkspolizei die oberste Verwaltungsebene.

Diese Abteilung betrieb mit der Personendatenbank (PDB) als zentrale Datensammlung der Schutz- und Sicherheitsbehörden im Rechenzentrum in Berlin-Biesdorf eines der Großrechnerverfahren der DDR (s. 1. Tätigkeitsbericht Anlage 3). In der PDB waren die Daten zu unterschiedlichen Bereichen, wie Strafregister, Sozialversicherung, Rentenzahlungen, Kader- und Personalverwaltung bis hin zur Nationalen Volksarmee sowie die Daten des Zentralen Melderegisters (ZER), erfaßt. Ein Teilbestand der PDB - Das Dialogorientierte Recherche- und Auskunftssystem (DORA) - diente ausschließlich kriminalpolizeilichen Zwecken.

Auf der mittleren Verwaltungsebene war den 15 Bezirksdirektionen und den ihnen unterstellten Volkspolizeikreisämtern die tatsächliche schutz- und kriminalpolizeiliche Sach- und Einzelvorgangsbearbeitung zugewiesen. Bei den Bezirkskriminalämtern wurde der gesamte Kriminalaktenbestand eines Bezirkes geführt.

Die Inspektionen als die unterste Verwaltungsebene nahmen einfache schutzpolizeiliche Aufgaben wahr.

3.6.1.2 Das Gemeinsame Landeskriminalamt der fünf neuen Länder

Die im Januar 1990 vom Runden Tisch erzwungene Auflösung der Staatssicherheit blieb nicht ohne Auswirkung auf die Polizei. Am 5. Februar 1990 erließ die Regierung Modrow den Befehl Nr. 0104/90 zur Gründung eines Zentralen Kriminalamtes (ZKA) und leitete damit die Umstrukturierung der ehemaligen Volkspolizei ein.

Im wesentlichen bestand das ZKA aus der Hauptabteilung Kriminalpolizei des Ministeriums

des Innern. Diese Abteilung war bis zur Wende zuständig für zentrale Aufgaben der Kriminalitätsvorbeugung und -bekämpfung. Ihr unterstanden die Kriminalabteilungen der Volkspolizei auf Bezirks- und Kreisebene sowie das kriminalistische Institut und die Zentralstelle für kriminalistische Registrierung in Berlin-Biesdorf.

Der Aufbau des ZKA war im wesentlichen der Organisationsstruktur des Bundeskriminalamtes (BKA) der Bundesrepublik Deutschland angeglichen. § 18 des Ländereinführungsgesetzes[52], mit dem u. a. die Wiedervereinigung der beiden deutschen Staaten vorbereitet wurde, legte fest, daß das ZKA übergangsweise in der zentralen Zuständigkeit des Ministeriums des Innern verblieb. Das Gesetz über die Aufgaben und Befugnisse der Polizei (Poli-zeiaufgabengesetz)[53] sah vor, daß das ZKA als Gemeinsames Landeskriminalamt (GLKA) der fünf neuen Bundesländer weitergeführt wird, "solange und soweit diese keine Länderkriminalämter errichtet haben". § 83 des Polizeiaufgabengesetzes befugte die Länder, "durch Vereinbarung Sitz-, Dienst- und Fachaufsicht sowie Kostenübertragung" für das GLKA zu regeln und bis zur Verabschiedung solcher Vereinbarungen das GLKA vorübergehend dem Land Brandenburg anzugliedern.

Weder der Einigungsvertrag noch das Polizeiaufgabengesetz der ehemaligen DDR, das in den fünf neuen Bundesländern solange gültig ist, bis die Länder eigene Gesetze verabschiedet haben (in Brandenburg ist das noch nicht geschehen), regelten Aufgaben und Zuständigkeiten des GLKA. In einer vorläufigen Vereinbarung der fünf neuen Bundesländer vom 16.10.1990 ist festgelegt, daß das GLKA vor allem für Staatsschutzdelikte (Hochverrat, Friedensverrat u. ä.), aber auch für die Verfolgung und Aufklärung von Kernenergie- und Strahlungsverbrechen zuständig sein sollte. Diese Vereinbarung ist jedoch nie in Kraft getreten, da das Land Thüringen sie nicht unterschrieben hat. Die polizeiliche Zusammenarbeit, inklusive Datenaustausch und Angleichung der dazu erforderlichen technischen Systeme, zwischen den Altbundesländern und den fünf neuen Bundesländern erfolgte auf der Grundlage eines Beschlusses der Konferenz der Innenminister des Bundes und der Länder (IMK), die im Mai 1990 auf dem Gebiet der damals noch bestehenden DDR tagte.

Das GLKA übernahm DORA und bereinigte es in mehreren Schritten um die gröbsten Verstöße gegen die nunmehr geltenden Rechtsvorschriften. Am 3. Oktober 1990 waren in DORA ca. 400.000 Personendatensätze von Beschuldigten und Tätern gespeichert, von denen ca. die Hälfte personenbezogene Hinweise, wie Fertigkeiten, Spezialkenntnisse, Motivation, Personenbeschreibungen nach 36 Merkmalsgruppen und modus-operandi-Beschreibungen nach 120 Merkmalsgruppen gegliedert, enthielten. Erst mit der Auflösung des GLKA (Herbst 1991) ist der Betrieb eingestellt worden. Die LKÄ der fünf neuen Bundesländer erhielten den jeweils auf sie entfallenden Teil der nunmehr ca. 430.000 Personendatensätze.

Der "inaktive Datenbestand" (Datensätze, die eigentlich zu löschen waren, sind in einen sog. inaktiven Bestand überführt worden) verblieb in der Obhut des Zentralen Einwohnerregisters (ZER) in Berlin-Biesdorf. Im Januar 1992 hat das Ministerium des Innern (MdI) Brandenburg in einem Schreiben an das GLKA verfügt, daß dieser Bestand im Landeskriminalamt (LKA) Brandenburg archiviert werden solle. Das ZER hat jedoch den inaktiven Bestand nie an das LKA übergeben, so daß davon auszugehen ist, daß er zusammen mit den anderen Datenträgern bei der Auflösung des ZER 1993 vernichtet worden ist.

3.6.1.3 Ausgangssituation im Land Brandenburg

Das Gesetz über die Organisation und die Zuständigkeit der Polizei im Land Brandenburg

---

52

53 vom 22. Juli 1992, GBl. d. DDR I, S. 995
vom 13. September 1990, GBl. d. DDR I, S. 1489

(Polizeiorganisationsgesetz - POG/Brbg)[54] legt in § 1 fest, daß Polizeibehörden des Landes die Polizeipräsidien und das Landeskriminalamt (LKA) sind, die das Ministerium des Innern - nach vorheriger Anhörung im Landtag - durch Rechtsverordnung gem. § 2 einrichtet.

Mit der Verordnung über die Polizeipräsidien des Landes Brandenburg (VO PP)[55] entstanden mit Wirkung vom 01.11.1991 die 5 Polizeipräsidien Cottbus, Eberswalde-Finow, Frankfurt/Oder, Oranienburg, Potsdam sowie das Polizeipräsidium der Wasserschutzpolizei. Je nach Größe des Einzugsgebiets wurden in den Polizeipräsidien bis zu sechs Schutzbereiche mit untergeordneten Wachen und Posten gebildet, in denen Schutz- und Kriminalpolizei unter einer Führung zusammenarbeiten. Zuständig für die jeweilige polizeiliche Aufgabe ist im allgemeinen die Polizeidienststelle, in deren Einzugsbereich sie anfällt. Darüber hinaus ist den Polizeipräsidien die Überwachung des Straßenverkehrs sowie das Versammlungs-, Waffen-, Munitions- und Sprengstoffwesen übertragen.

Das LKA ist als zentrale Dienststelle der Kriminalpolizei des Landes Brandenburg zuständig für den Informationsaustausch mit dem Bundeskriminalamt (BKA). Es unterhält Einrichtungen für kriminaltechnische und erkennungsdienstliche Untersuchungen und Forschungen sowie diejenigen Informationssammlungen, die von landesweiter Bedeutung sind.

Als kriminalaktenführende Stelle erhielten die Polizeipräsidien und das LKA die ihnen zuzuordnenden Kriminalakten aus dem Kriminalaktenbestand der ehemaligen DDR. Diesen Altbestand (zwischen 3.000 bis ca. 10.000 Akten pro Polizeipräsidium) gilt es zu sichten, und ggf. entsprechend der neuen Rechtslage zu bereinigen oder aber zu archivieren.

Vom GLKA übernahmen LKA und Polizeipräsidien jeweils einen identischen DORA-Bestand, der aber nur noch als "Findex"-Datei, d. h. zum Auffinden einer bestimmten Kriminalakte aus dem Altaktenbestand, genutzt wird.

3.6.2 Prüfung der Datenverarbeitung im Landeskriminalamt und in den Polizeipräsidien

Im Berichtszeitraum habe ich eine Querschnittsprüfung der Datenverarbeitung im LKA und in den Polizeipräsidien durchgeführt. Den Prüfungen lag kein aktueller Anlaß zugrunde. Sie dienten vielmehr dazu, meiner Behörde einen ersten Überblick über bestimmte Bereiche der Informationsverarbeitung zu verschaffen. LKA und Polizeipräsidien zeigten sich sehr kooperativ und aufgeschlossen für datenschutzrechtliche Belange. Da die Kontrollbesuche ergaben, daß die festgestellten - teilweise gravierenden - Mängel, die meine Mitarbeiter vor Ort (mit Ausnahme des LKA) vorfanden, behoben werden und meine Vorschläge dazu aufgegriffen wurden, habe ich - soweit es die Polizeipräsidien betraf - gem. § 25 Abs. 2 Bbg DSG von Beanstandungen abgesehen.

Für das Ministerium des Innern trifft dies nicht zu. § 24 Abs. 1 Bbg DSG verpflichtet dazu, dem Datenschutzbeauftragten jede Datei bei Betriebsaufnahme anzuzeigen, so daß sie in das Dateienregister aufgenommen werden kann. Damit soll u.a. dem Bürger ermöglicht werden, sich einen ersten Überblick über die Datensammlungen zu verschaffen, in denen er registriert sein könnte. Darüber hinaus hat es eine wichtige Unterstützungsfunktion für meine Kontrolltätigkeit. Was die Datensammlungen der Polizeibehörde anbelangt, so ist das Ministerium des Innern für die Dateienregistermeldungen verantwortlich.

Bei den Kontrollbesuchen stellte sich heraus, daß LKA und Polizeipräsidien zahlreiche

---

54

55 vom 20. März 1991, GVBl., S. 82
vom 11. Oktober 1991, GVBl. 1991, S. 448

Dateien betrieben, für die mir zum Zeitpunkt der Prüfung noch keine Dateienregistermeldungen vom MdI zugegangen waren, obwohl die das Meldeverfahren regelnde Dateienregisterverordnung (DRegVOBbg)[56] bereits im November 1992 ergangen war.

§ 48 Gesetz über die Aufgaben und Befugnisse der Polizei i.V.m. § 1 Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg (VGPolG)[57] verpflichtet die Polizei, für jede automatisierte Datei eine Errichtungsanordnung zu erstellen. Gem. § 7 Abs. 2 Bbg DSG bin ich vor dem Erlaß von Verwaltungsvorschriften, die der Sicherstellung des Datenschutzes dienen, zu hören. Dies hatte das MdI bis dahin unterlassen. Darüber hinaus wurden zahlreiche Dateien ohne ausreichende Errichtungsanordnungen betrieben. In diesen drei Punkten habe ich das MdI gem. § 25 Abs. 1 Bbg DSG beanstandet.

Unterdessen hat sich die Zusammenarbeit mit dem MdI sehr verbessert. Soweit ich es überschauen kann, liegen für alle von der Polizei betriebenen Dateien Dateienregistermeldungen vor. Auch am Erlaß von Errichtungsanordnungen werde ich jetzt rechtzeitig beteiligt.

Bei allen Prüfungen war stets auch ein Vertreter des MdI zugegen. Dies wirkte sich insgesamt positiv für den Ablauf der Prüfungen und die Umsetzung der Ergebnisse aus. Schwerpunkte der Prüfungen waren:

- die Sammlung der Fingerabdruck-Blätter (Fa-Blätter) und das Verfahren zur rückwirkenden Erfassung von Fa-Blättern der ehemaligen DDR (im LKA),

- die Kriminalaktenführung (im LKA und den Polizeipräsidien) sowie

- die Errichtungsanordnungen gem. § 48 VGPolG Bbg sowie die Dateibeschreibungen gem. § 8 Bbg DSG bzw. die Dateienregistermeldungen gem. § 24 Bbg DSG der von den Abteilungen Einsatz/Ermittlung und Verwaltung sowie in den Kommissariaten geführten Dateien und

- die technische Ausstattung und Organisation der Datenverarbeitung (in den Polizeipräsidien).

3.6.2.1 Fingerabdruck-Blätter

Fingerabdruck-Blätter (Fa-Blätter) gehören zum Handwerkszeug jeder Polizei. Das GLKA hat insgesamt ca. 700.000 Fa-Blätter aus dem Bestand der Volkspolizei übernommen und bis zu seiner Auflösung in mehreren Schritten gesichtet. Etwa 160.000 Fa-Blätter waren in das EDV-gestützte Projekt "DRAT-SPUT" (daktyloskopische Registrierung aktiver Täter - Spuren unbekannter Täter) eingestellt. Diese Datei wurde zusammen mit den Fa-Blättern auf die fünf neuen Bundesländer und Berlin verteilt. Auf Brandenburg entfielen ca. 30.000 Datensätzen.

Im August 1993 habe ich von der Absicht erfahren, einen Teil der Fa-Blätter der ehemaligen DDR in das Automatisierte Fingerabdruck-Identifizierungssystem (AFIS) einzugeben. Dazu haben die Länder den ihnen vom GLKA überstellten Bestand an Fa-Blättern auf der Grundlage der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener

---

[56] vom 19. November 1992, GVBl. II, S. 726

[57] vom 11. Dezember 1991, GVBl. I, S. 636

Sammlungen (KpS-Richtlinien)[58] bereinigt. Ca. 55.000 Blätter sind als AFIS-relevant an das BKA überstellt worden, von denen etwa 25.000 in INPOL erfaßt wurden.

Bei den restlichen ca. 30.000 Fa-Blättern reichten aus Sicht des BKA die anlaßbezogenen Angaben nicht aus, um sie ohne Verstoß gegen datenschutzrechtliche Bestimmungen erfassen und nutzen zu können. Die Länder machten dagegen geltend, daß die von ihnen überstellten Fa-Blätter vorher einer datenschutzrechtlichen Überprüfung unterzogen worden seien und ihren Bestimmungen entsprächen. Für Brandenburg konnte dies nicht zutreffen, da ich an dem Vorgang nicht beteiligt worden war.

Auf meine Anfrage teilte das MdI im Oktober mit, daß noch keine Fa-Blätter aus dem Altbestand an das BKA übermittelt worden seien, da das LKA das Bereinigungsverfahren noch nicht abgeschlossen habe. Grundsätzlich würden nur Fa-Blätter zur AFIS-Erfassung vorgesehen, die vollständig ausgefüllt seien und den erforderlichen Aktenrückhalt hätten.

Die Prüfung im LKA ergab, daß

- verfahrensbedingte Mängel bei den in AFIS zu erfassenden Fa-Blättern nicht zu erwarten sind,

- bei Stichproben keine mangelhaften Fa-Blätter gezogen wurden.

Auf meine Anfrage zum Stand hat das LKA im Februar 1994 mitgeteilt, daß

- 5347 Fa-Blätter zur AFIS-Erfassung vorgesehen sind (von 14115 bis dahin überprüften Unterlagen)

- die Bereinigung im Mai 1994 abgeschlossen sein soll und

- ca. 10.000 Fa-Blätter an das BKA gehen werden.

Derzeit hat Brandenburg ca. 4.000 Datensätze in AFIS eingespeichert. Bei jeder erkennungsdienstlichen Behandlung wird ein Fa-Blatt angelegt. Neben den Fingerabdrücken enthält es die Identifizierungsdaten des Betroffenen sowie anlaßbezogene Angaben, wie z. B. den Tat-vorwurf. Die Fa-Blätter werden in den Polizeipräsidien angelegt, dem LKA zugestellt, dort abgelegt und mittels der seit Ende 1993 im LKA verfügbaren AFIS-Station an das BKA übermittelt. Das BKA stellt die Daten in das Informationssystem der Polizei (INPOL) ein. Sie stehen damit allen Polizeidienststellen des Bundes und der Länder zur Verfügung. Seit 1993 wird die Erkennungsdienstdatei mittels AFIS betrieben und auch so bezeichnet.

Zur landesweiten Speicherung und Recherche von Finger- und Handabdrücken (letzteres ist in AFIS noch nicht möglich) sowie zur Unterstützung des Bereinigungsverfahrens betreibt das LKA seit März d. J. die Datei "PC-DRAT". An dem Erlaß der Errichtungsanordnung bin ich beteiligt worden. Ein erster Entwurf ist mir im November 1993 zugegangen.

Bei der endgültigen Fassung der Errichtungsanordnung sind meine Vorschläge, wie

- den Kreis derjenigen Personen, die in die Datei eingestellt werden, zu verringern,

- eine Frist von einem Jahr festzulegen, nach deren Ablauf geprüft wird, ob die Voraussetzungen für eine weitere Speicherung noch vorliegen und

---

58 vom 1. April 1992, ABl. 1993, S. 1046

- Übermittlungen aus der Datei in der jeweiligen Kriminalakte zu dokumentieren,

aufgegriffen worden.

3.6.2.2 Prüfung der Kriminalakten im Landeskriminalamt und in den 5 Polizeipräsidien

Kriminalakten sind Teile der kriminalpolizeilichen Sammlungen. Sie dienen zur Abwehr von Gefahren, zur Verhütung und Aufklärung von Straftaten sowie zur Ermittlung von Straftätern. Kriminalakten werden angelegt, wenn ein Ermittlungsverfahren eingeleitet worden ist und wegen der Art, Ausführung und Schwere der Tat sowie der Persönlichkeit des Betroffenen die Gefahr der Begehung weiterer Straftaten besteht (Negativprognose). Laut Anweisung des MdI[59] soll die Kriminalakte einen Überblick über den kriminellen Lebenslauf des Betroffenen und sein Vorgehen bei der Vorbereitung und Ausführung von Straftaten vermitteln sowie Personen- und Sachzusammenhänge aufzeigen.

Bei der *Prüfung der Kriminalakten, die nach dem 03.10.1990 angelegt wurden*, ergaben sich folgende grundsätzliche Mängel:

- *Fehlende Negativprognose*

  Aus keiner der überprüften neu angelegten Kriminalakten ging hervor, ob und mit welchem Ergebnis eine Negativprognose (siehe oben) durchgeführt wurde. Dies ist jedoch eine der Voraussetzungen für die Abwägung, ob es zur polizeilichen Aufgabenerfüllung erforderlich ist, überhaupt eine Kriminalakte zu dem Betroffenen anzulegen bzw. ob es erforderlich ist, diese noch weiter aufzuheben.

- *Fehlende Rückmeldung der Staatsanwaltschaft (StA)*

  In einigen Kriminalakten war die Abgabe des Ermittlungsverfahrens an die StA dokumentiert, in der überwiegenden Mehrzahl fehlte sie jedoch. In keiner der überprüften Kriminalakten fand sich die Rückmeldung der StA mit Aktenzeichen. Damit läßt sich aus den Kriminalakten auch nicht ersehen, welchen Fortgang das Ermittlungsverfahren genommen hat bzw. ob StA oder Gericht den polizeilichen Verdacht bestätigt haben. Die zur Entscheidung, ob die weitere Aufbewahrung der Kriminalakte bzw. Speicherung der personenbezogenen Daten noch zulässig ist, unabdingsbaren Informationen (wie z. B. die Eröffnung des Hauptverfahrens, die Einstellung des Verfahrens nach § 170 Abs. 2 StPO oder der Ausgang der Hauptverhandlung) liegen nicht vor. Damit entfällt eine notwendige Voraussetzung effektiver polizeilicher Arbeit. Ein verläßlicher Informationsstand als Arbeitsgrundlage weiterer Ermittlungen kann nur durch regelmäßige Überprüfung - und Bewertung - des vorhandenen Bestandes erreicht werden. Darüber hinaus besteht die Gefahr, daß Kriminalakten weiter aufbewahrt werden, obwohl sie für die Aufgabenerfüllung nicht mehr erforderlich sind. Dies ist ein rechtswidriger Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen.

- *Vergabe von Aussonderungsprüffristen*

  Auf vielen, wenn auch längst nicht allen, Akten war zwar ein Aussonderungsdatum (in der Regel 5 oder 10 Jahre nach Anlage der Akte) vermerkt, Prüffristen waren jedoch nie vergeben. § 41 Abs. 4 VGPolG schreibt aber vor, daß nach einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, zu prüfen ist, ob die Voraussetzungen für eine weitere

---

59 Rundschreiben an alle Polizeibehörden zur Führung von Kriminalakten vom 22. Januar 1992

Aufbewahrung der Kriminalakte noch vorliegen. Dazu benötigt die Polizei u. a. die Information über den weiteren Fortgang des Ermittlungsverfahrens. Das Ergebnis der Prüfung ist in der Akte zu vermerken.

- *Beispielhafte Einzelfälle*

Bei mehreren überprüften Akten habe ich angeregt, die Aktenaufbewahrungsfrist zu verkürzen. So war im Fall eines Ladendiebstahls eine Aufbewahrungsfrist von fünf Jahren vergeben. Der Tatvorwurf "Gemeinschaftlich begangener Diebstahl" (§ 242 StGB) beruhte auf der Tatsache, daß sich die Beschuldigte - ein 14-jähriges Mädchen - in der Gesellschaft anderer Kinder befunden hatte. Aus der Akte war jedoch nicht ersichtlich, daß die anderen Jugendlichen an der Tat beteiligt waren. Ich habe vorgeschlagen, zu überprüfen, ob die weitere Aufbewahrung überhaupt noch erforderlich ist bzw. die Aufbewahrungsfrist auf zwei Jahre zu verkürzen.

Bei der Prüfung von Akten des 4. Kommissariats in einem Polizeipräsidium fand sich die höchste Aufbewahrungsdauer (10 Jahre) besonders häufig. Darüber hinaus waren viele Akten in dem beim BKA als INPOL-Bestandteil geführten Kriminalaktennachweis (KAN-Bund) eingestellt (s. unter 3.6.5.3).

Die Speicherung in einer Datei, auf die alle Polizeidienststellen des Bundes und der Länder Zugriff haben, stellt einen tiefen Eingriff in das Persönlichkeitsrecht der Betroffenen dar. Dabei ist auch zu berücksichtigen, daß durch den Nachweis, wo und zu welchen Tatvorwürfen eine Kriminalakte vorliegt, die weitergehenden Informationen dieser Akte auf Nachfrage zur Verfügung stehen. Die Speicherung im KAN-Bund ist daher an besondere Voraussetzungen geknüpft. Sie kommt nur in Fällen schwerer oder überregional bedeutsamer Straftaten in Betracht. Als schwere Straftaten definiert die Errichtungsanordnung Verbrechen und die in § 100a StPO aufgeführten Vergehen. Überregional bedeutsam sind Straftaten, wenn u. a. der Verdacht besteht, daß sie bandenmäßig begangen werden, zur Verfolgung extremistischer Ziele dienen bzw. wenn zu vermuten ist, daß der Betroffene erneut außerhalb seines Wohn- oder Aufenthaltsbereichs Straftaten begehen wird.

Bei den überprüften Akten, die eine KAN-Bund-Notierung aufwiesen, lagen diese Voraussetzungen nicht in vollem Umfang vor.

So war im Fall einer Sachbeschädigung (§ 303 StGB) die Einstellung im KAN-Bund vor dem Hintergrund erfolgt, daß die Sachbeschädigung bei einem "Kameradschaftsabend", der in einer Privatwohnung stattgefunden hatte, begangen worden war. § 303 StGB ist kein Verbrechen i.S.v. § 12 StGB. Der Tatbestand gehört auch nicht zu dem Straftatenkatalog des § 100a StPO. Aus der Kriminalakte ergibt sich darüber hinaus auch kein Hinweis oder Verdacht, daß die Straftat "überregional bedeutsam" im Sinne der Errichtungsanordnung KAN-Bund sein könnte. Da die Voraussetzungen der Errichtungsanordnung nicht erfüllt sind, ist die Speicherung im KAN-Bund zu löschen.

In mehreren Fällen war die Speicherung im KAN-Bund wegen des Tatvorwurfs nach § 86a StGB (Verwenden von Kennzeichen verfassungswidriger Organisationen) erfolgt. Dieser Tatbestand ist kein Verbrechen i.S.v. § 12 StGB. Vielmehr handelt es sich um ein Vergehen von vergleichsweise geringer Bedeutung aus dem Katalog des § 100a StPO. Auch wenn somit die Voraussetzungen für eine Speicherung im KAN-Bund dem Buchstaben nach gegeben sind, ist dennoch zu prüfen, ob sie dem Verfassungsgebot der Verhältnismäßigkeit genügt. Dies dürfte regelmäßig nicht der Fall sein, wenn der Betroffene mit dem Verstoß gegen § 86a StGB zum ersten Mal straffällig geworden ist und Hinweise auf überregionale Bedeutung sowie auf erneute Straffälligkeit nicht vorliegen. Angesichts dieser Sachlage scheint die Speicherung in einer Datei mit bundesweitem Zugriff unverhältnismäßig.

Die Stellungnahme des Innenministeriums zu den Mängeln sowie zu den oben aufgeführten Einzelpunkten lag zum Ende des Berichtzeitraumes noch nicht vor.

Die Prüfung von *Kriminalakten, die von der Volkspolizei der ehemaligen DDR angelegt* worden waren und nach Bereinigung in den Kriminalaktenbestand übernommen wurden, ergab zum Teil gravierende Mängel.

Aufgrund ihrer Personalsituation sehen die Polizeipräsidien sich nicht in der Lage, Polizeibedienstete ausschließlich zur Bereinigung der Altakten abzustellen, so daß dies im Zuge der täglichen Aufgabenerfüllung geschehen muß.

Trotz der damit verbundenen Schwierigkeiten sind die Mängel, die rechtswidrige Eingriffe in das Persönlichkeitsrecht der Betroffenen darstellen, nicht hinnehmbar. Das MdI teilt diese Auffassung und hat unterdessen einen Maßnahmenkatalog zur Behebung der Mängel (siehe unten) entworfen, der noch im Abstimmungsverfahren ist.

Trotz des Bereinigungsverfahrens enthalten viele Krimininalakten Aktenbestandteile, für die es entweder keine Rechtsgrundlage mehr gibt, oder deren Aufbewahrung nur noch mit Einschränkungen zulässig ist. Zu den vorgefundenen Akteninhalten, die wegen fehlender Rechtsgrundlagen entnommen werden müssen, zählen:

- Personenkennzahl (PKZ),

- Protokolle der Kollektivberatung, die nicht nur unzulässig tief in die Privatsphäre der Betroffenen eindringende Informationen enthalten, sondern auch Namen und Anschriften derjenigen Kollektivvertreter, die die Resozialisierung des Betroffenen unterstützen sollten,

- Angaben über Hobby's/Freizeitbeschäftigungen des Betroffenen, ohne daß ein Zusammenhang mit der Straftat erkennbar ist,

- Abschlußberichte der Strafvollzugsanstalt,

- gesellschaftliche Beurteilung des Betroffenen durch den Betrieb sowie die vollständige Anschrift des Betriebes, indem der Betroffene zum Zeitpunkt seiner Vernehmung gearbeitet hat bzw. der Betriebe, in denen sich der Betroffene nach der Haftverbüßung vorgestellt hat oder Arbeit gefunden hat, ohne daß ein Bezug zur Straftat hergestellt werden kann,

- Mitgliedschaft in einer gesellschaftlichen Organisation (wie z. B. FDGB oder einer Partei) bzw. Hinweise, daß der Betroffene nicht Mitglied ist.

Die meisten der o. a. unzulässigen Informationen finden sich in Vernehmungsprotokollen, die teilweise zur Aufgabenerfüllung der Polizei erforderlich und daher weiter aufzubewahren sind. Häufig fanden sich jedoch auch noch Vernehmungsprotokolle zu Straftaten, die nach dem StGB keine Delikte mehr sind.

Im folgenden wird ein besonders negatives Beispiel für die Gemengelage unzulässiger Informationen aufgrund der früheren und heutigen Gesetzeslage dargestellt. In der Akte fanden sich über Seiten hinweg Zeugenvernehmungen zu dem Tatvorwurf "Asozialität" (nach der Wende kein Straftatbestand gem. StGB mehr). Der Beschuldigten war nach ihrer Haftentlassung zur Auflage gemacht worden, nach 22.00 Uhr keine Besuche mehr in ihrer Wohnung zu empfangen. Nach einer Anzeige wurden alle bekanntgewordenen Besucher vorgeladen und vernommen. Diese Vernehmungsprotokolle strotzen geradezu von Vorhaltungen und Angaben, die unzulässig tief in die Privatsphäre der Vernommenen und der

Betroffenen eindringen. An anderer Stelle wird die Betroffene zum Tatvorwurf der Hehlerei (§ 259 StGB) befragt und äußert sich dabei auch zu Fragen und Vorhaltungen über ihre Sexualgewohnheiten. Desweiteren finden sich Angaben über Krankheiten, die in keinem Zusammenhang mit dem Tatvorwurf stehen.

Zur Behebung der Mängel habe ich vorgeschlagen:

- nur Einleitungsverfügung und Schlußbericht der Vernehmungsprotokolle zu denjenigen Straftaten, die Delikten nach dem StGB zuzuordnen sind, aufzubewahren und

- den Rest der Vernehmungsprotokolle sowie

- die übrigen unzulässigen Aktenbestandteile (s.o.)

aus der Akte zu entfernen. Auf diese Weise ließe sich das zeit- und personalaufwendige Schwärzen der unzulässigen Informationen in den Vernehmungsprotokollen, das bei weiterer Aufbewahrung und Nutzung erforderlich wäre, vermeiden. Gleichzeitig wäre aber auch sichergestellt, daß Informationen über Straftaten, die zur Aufgabenerfüllung noch erforderlich sind, weiterhin zur Verfügung stehen, weil Einleitungsverfügung bzw. Schlußbericht den Tatvorwurf vermerken.

In dem Entwurf eines Maßnahmeplans zur Bereinigung von Kriminalakten listet das MdI diejenigen Aktenbestandteile auf, die grundsätzlich zur Aufgabenerfüllung der Polizei nicht mehr erforderlich sind und legt darüber hinaus fest, daß Akten erst nach erfolgter Bereinigung auskunftsfähig sind.

Inwieweit mein Vorschlag (s.o.) aufgegriffen wird, ist noch unklar, da das MdI noch nicht Stellung genommen hat.

3.6.2.3 Prüfung der Errichtungsanordnungen gem. § 48 VGPolGBbg sowie der Dateibeschreibungen gem. § 8 Bbg DSG bzw. der Dateienregistermeldung gem. § 24 Bbg DSG

Ebenso wie die Kriminalakten wiesen auch die o. g. Unterlagen bei der Festsetzung von Fristen zur Speicherung/Löschung der Daten Mängel auf. Häufig fehlte sie ganz. Meist waren die Fristen schematisch auf 10 Jahre festgesetzt. Dies entspricht weder dem Polizeiaufgabengesetz (§ 41 VGPolGBbg) noch Ziff. 5 der KpS-Richtlinien, die eine Prüfung der Speicherungsdauer im Einzelfall vorschreiben und regeln, daß Speicherung und Prüftermine zusammen nicht länger als 10 Jahre bei Erwachsenen, 5 Jahre bei Jugendlichen und 2 Jahre bei Kindern sein dürfen.

Die o. g. Unterlagen, die die Dateiverarbeitungsabläufe der jeweiligen Datei darstellen und regeln sollen, müssen sowohl die erforderliche Einzelfallprüfung als auch die Fristen, nach deren Ablauf sie erfolgen soll, festlegen.

In vielen Unterlagen waren die Rechtsvorschriften nicht ausreichend bezeichnet. Aus den Rechtsgrundlagen muß hervorgehen, welche Straftatbestände zur Aufnahme von personenbezogenen Daten in eine Datei führen. Ohne diese Festlegung läßt sich der Kreis der Betroffenen, die zulässigerweise in einer bestimmten Datei gespeichert werden, nicht abgrenzen von denjenigen Personen, die in diese nicht aufgenommen werden dürfen. Ohne exakt festgelegte Rechtsgrundlagen können auch weder die zulässige Speicherungsdauer noch die Nutzung der Daten, z. B. die Übermittlung an andere Stellen, ausreichend bestimmt werden. Daher reicht es, wegen der gerade in den Spezialgesetzen zu findenden Differenzierung von Speicherungs-und/oder Nutzungsbefugnissen, auch nicht aus, die Rechtsvorschrift ohne Paragraphenzuordnung aufzuführen.

Diese Problematik wird besonders bei der automatisierten Vorgangsauswertung (AVA) deutlich. Dazu unterhalten alle Polizeipräsidien eine Datei. Die Vorgangsverwaltung ist eine Hilfsfunktion der Verwaltung, die der Registrierung von "Vorgängen" dient. Soweit es sich dabei um Vorgänge handelt, die im Rahmen der Gefahrenabwehr, der Strafverfolgung oder der vorbeugenden Straftatenbekämpfung entstanden sind, ist die Verarbeitung von Daten zu diesem Zweck in Spezialgesetzen geregelt. Vorgänge, die nicht oder nicht mehr zur Aufgabenerfüllung in den o. a. Bereichen aufbewahrt werden dürfen, können zum Zweck der Vorgangsverwaltung oder zur befristeten Dokumentation gem. § 42 VGPolGBbg gespeichert werden. Sie dürfen dann allerdings nicht bzw. nicht mehr zur allgemeinen polizeilichen Aufgabenerfüllung genutzt werden. Die Speicherung dient ausschließlich zum Zweck der Vorgangsverwaltung, also z. B. um bestimmte Akten zu finden oder um ihren Verbleib im Sinne der Aktenordnung zu registrieren. Um zu verhindern, daß durch eine extensive Auslegung und Anwendung des Begriffs "Vorgangsverwaltung" die Speicherungsbefugnis ausgehöhlt wird, legt § 42 VGPolGBbg ausdrücklich fest, daß sie nur zu diesem Zweck genutzt werden dürfen und § 41 VGPolGBbg, der die Durchbrechung des Zweckbindungsgrundsatzes regelt, keine Anwendung findet.

Als Konsequenz aus dem oben Gesagten ergibt sich für die Datei AVA, daß die aufgeführten Rechtsvorschriften § 163 StPO und § 42 VGPolG Bbg in sich widersprüchlich sind. In diesen - wie in weiteren Punkten - müssen die in Frage kommenden Unterlagen so korrigiert werden, daß der Zweck der Datei klar erkennbar wird.

Eine Stellungnahme des MdI dazu steht noch aus.

3.6.2.4. Prüfung der technischen Ausstattung und der Organisation der Datenverarbeitung in den Polizeipräsidien

In der technischen Ausstattung haben die Polizeipräsidien im allgemeinen einen Standard erreicht, der die Arbeitsfähigkeit der Datenverarbeitung gewährleistet. Daß es überall noch problematische Bereiche gibt, in denen eine unzulängliche technische Ausstattung und die dadurch bedingte Verfahrensorganisation der Datenverarbeitung zu unnötigen Eingriffen in das Persönlichkeitsrecht Betroffener führt, muß im Hinblick auf die erst vor zwei Jahren erfolgte Einrichtung der Polizeipräsidien hingenommen werden. So ist es z. B. aufgrund der verfahrensbedingten Organisation der Datenstation nicht zu vermeiden, daß alle Mitarbeiter, die sich dort aufhalten, ohne Erfordernis bei allen telefonischen Fahndungsabfragen tief in das Persönlichkeitsrecht eingreifende Informationen über die Betroffenen erfahren.

In allen Polizeipräsidien wird eine Datei betrieben, die aus den im Einzugsbereich des Präsidiums zur Fahndnung ausgeschriebenen Tatverdächtigen besteht. Sie ist damit ein Teilbestand der INPOL-Personenfahndung, auf die die Datenstationen der Polizeipräsidien uneingeschränkt Zugriff haben. Gem. § 2 Abs. 1 Ziff. 1 Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (BKAG)[60] wird die INPOL-Anwendung "Personenfahndung" in allen Bundesländer parallel geführt. Daraus läßt sich jedoch keine Befugnis für regionalisierte Teildatenbestände ableiten, so daß die Speicherung der Betroffenen in der INPOL-Personenfahndung und in den jeweiligen Dateien der Polizeipräsidien eine unzulässige Doppelspeicherung darstellt. Sie ist jedoch darauf zurückzuführen, daß zwischen der Ausschreibung und der Einstellung der Daten des Betroffenen in die INPOL-Personenfahndung ein Zeitraum bis zu sechs Wochen verstreichen kann. Wenn sichergestellt ist, daß die Betroffenen immer dann bei den Polizeipräsidien gelöscht werden, wenn die INPOL-Einspeicherung erfolgt ist, bestehen gegen diese Dateien datenschutzrechtlich keine Bedenken.

---

60 vom 29. Juni 1973, BGBl. I, S. 449, zuletzt geänd. am 9. Dezember , BGBl. I, S. 3393

Die Datenübermittlungen aus den Melderegistern an die Polizei gestaltet sich in allen Polizeipräsidien aufgrund der technischen Ausstattung und der Organisation als äußerst problematisch. Bei Personalienfeststellungen während der Bürostunden erfolgt die Überprüfung der Meldedaten durch telefonische Abfragen der Polizei in den Meldestellen. Dies ist datenschutzrechtlich hinnehmbar, wenn durch technische und organisatorische Maßnahmen sichergestellt ist, daß die Auskunft nur an dazu berechtigte Polizeibedienstete erteilt wird und im Einzelfall überprüfbar ist. Letzteres wird durch Protokollierung in den Akten erreicht.

Datenschutzrechtlich äußerst bedenklich ist allerdings die in einem Polizeipräsidium mit den meisten Meldestellen seines Einzugbereichs getroffene Regelung für Anfragen außerhalb der Bürostunden. Dazu hat das betreffende Polizeipräsidium die Schlüssel der Meldestellen erhalten. Bei diesem Verfahren ist nicht zu gewährleisten, daß nur die zulässigen Daten eingesehen werden. Zumal eine Protokollierung durch die einsichtnehmenden Polizeibediensteten nicht vorgesehen ist, so daß eine datenschutzrechtliche Kontrolle der Datenübermittlungen nicht vorgenommen werden kann.

Darüber hinaus widerspricht die "Schlüssellösung" auch der ersten Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (1. MeldDÜÄV)[61], die festlegt, daß die Meldebehörden den zuständigen Polizeipräsidien monatlich einmal die zulässigen Daten auf maschinell lesbaren Datenträgern oder Listen übermittelt. Unterdessen ist das erste Gesetz zur Änderung des Melderechtsrahmengesetzes (MRRG)[62] verabschiedet, das in § 24 die "Schlüssellösung" für die neuen Bundesländer ermöglicht (s. unter 3.4.3). Datenschutzrechtlich ist die Schlüssellösung allenfalls dann hinnehmbar, wenn die Pro-tokollierungspflicht vorgeschrieben wird.

Gravierende Mängel fanden sich bei der Prüfung mehrerer Dateien im 4. Kommissariat eines Polizeipräsidiums. Entgegen den Festlegungen der Errichtungsanordnungen sowie der Dateienregistermeldungen ergaben sich folgende Mängel:

- Fehlen des Speicherungsanlasses

  Aus welchem Grund (Straftat und/oder Anlaß) der Betroffene gespeichert wird, war nicht ersichtlich. Ein entsprechendes Datenfeld ist zwar vorgesehen, aber nicht belegt. Für Informationen über den Speicherungsgrund ist die Polizeidienststelle auf das Erinnerungsvermögen der Sachbearbeiterin angewiesen. Nur soweit gegen die Betroffenen Ermittlungsverfahren eingeleitet worden sind, gibt die Kriminalakte Auskunft über den Speicherungsgrund.

- Speicherungen ohne tatsächlichen Anlaß

  Mehrere Betroffene sind nur aufgrund von Fernschreiben anderer Polizeibehörden im Rahmen bestimmter Meldeverfahren (KPMD-S oder KTA) in die Dateien eingestellt worden. Dies erfolgte auch dann, wenn Betroffenen nicht im Einzugsbereich des betreffenden Polizieräsidiums wohnen und dort nicht in Erscheinung getreten sind. In diesen Fällen besteht ein Aktenrückhalt nur aus den Fernschreiben, die in der Polizeidienststelle gesammelt werden.

- Keine jährliche Überprüfung auf Erforderlichkeit

---

61 vom 8. Dezember 1993, GVBl. II, S. 776, vgl. hierzu auch unter 3.4.1

62 vom 11. März 1994, BGBl. I, S.569

Die jährlich vorzunehmende Überprüfung auf Erforderlichkeit, die neben dem VGPolG auch die Errichtungsanordnungen und die Dateienregistermeldungen der entsprechenden Dateien vorschreiben, war bis zum Zeitpunkt der Überprüfung noch nicht erfolgt.

- Vermeidbare Mehrfachspeicherungen

  Einzelne Betroffene sind in allen Dateien registriert, obwohl ein enger inhaltlicher Zusammenhang zwischen verschiedenen Dateien besteht. Diese Mehrfachspeicherungen sind nicht hinnehmbar, da sie vermeidbar das Recht auf informationelle Selbstbestimmung der Betroffenen verletzen.

Eine der Dateien ist nach der Prüfung aufgelöst worden. Bei einer weiteren sind die Errichtungsanordnung bzw. die Dateienregistermeldung korrigiert worden. Diese Korrekturen dürften nicht ohne Auswirkung auf die Datei vor Ort bleiben. Bei einer weiteren Datei steht die Stellungnahme des MdI noch aus.

3.6.3 Zu weitgehende Unterstützung eines Tankwarts

Ein Bürger wandte sich wegen der Überprüfung seiner Personalien durch Polizeiangehörige an mich und bat, diese Angelegenheit zu überprüfen. Die Personalienüberprüfung fand auf einer Tankstelle statt. Nachdem der Petent getankt hatte, gab es Probleme bei der Bezahlung mittels einer Kreditkarte. Der Tankstellenbesitzer lehnte die Rechnungsbegleichung durch Scheck ab, die ihm der Petent anstelle der Kreditkarte anbot. Als der Petent sich weigerte, seine Personalien anzugeben, rief der Tankstellenbesitzer die Polizei. Nachdem der Petent den Polizeibeamten seinen Personalausweis ausgehändigt hatte, gaben diese die Personalausweisdaten an den Tankstellenbesitzer weiter. Dagegen erhob der Petent zu Recht Beschwerde.

§ 33 a Abs. 1 Ziff. 2 des VGPolGBbg befugt die Polizei, personenbezogene Daten zu erheben, wenn sie zum Schutz privater Rechte nach § 1 Abs. 2 VGPolGBbg erforderlich sind. Diese Befugnis gilt jedoch nicht uneingeschränkt. Vielmehr darf die Polizei zum Schutz privater Rechte nur dann eingreifen, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert werden würde. Diese Voraussetzungen waren im vorliegenden Fall nicht erfüllt. Der Petent machte geltend, zahlungswillig und auch zahlungsfähig gewesen zu sein. Davon hätten sich die Polizeiangehörigen durch Befragung des Petenten und Inaugenscheinnahme von Scheck und Scheckkarte sowie Kreditkarte überzeugen können. Die Datenerhebung durch Überprüfung des Personalausweises war dazu nicht erforderlich.

Auch für die Weitergabe der Personalausweisdaten an den Tankstellenbesitzer gibt es keine gesetzliche Grundlage. Zwar regelt § 43 Abs. 3 VGPolGBbg, daß die Polizei zur Erfüllung polizeilicher Aufgaben oder zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder für die schutzwürdigen Belange einzelner personenbezogene Daten an andere Personen übermitteln kann. Dies gilt jedoch im vorliegenden Falle nicht, da es schon für die Erhebung der Daten - wie oben ausgeführt - keine Rechtsgrundlage gibt.

§ 16 Bbg DSG, der die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs regelt und in Absatz 1 an die Voraussetzung knüpft, daß diese Personen oder Stellen die Daten zur Verfolgung ihrer wirtschaftlichen Zwecke oder Ziele benötigen, kann als Rechtsgrundlage für die Datenübermittlung ebenfalls nicht in Frage kommen, weil der Petent - wie oben ausgeführt - die Rechnung mittels Scheck und Scheckkarte bezahlen wollte und konnte.

Das Polizeipräsidium teilt diese Auffassung. Es hat sich bei dem Petenten entschuldigt und weitere geeignete Schritte zur Vermeidung ähnlicher Vorfälle eingeleitet.

3.6.4 Foto- und Videoaufnahmen der Polizei und anderer Stellen bei Versammlungen

Durch Anfragen von Journalisten und Presseberichte bin ich im Berichtszeitraum zweimal mit Foto- bzw. Videoaufnahmen durch eine Stadtverwaltung bzw. durch die Polizei bei Versammlungen befaßt worden.

Der erste Fall hat sich anläßlich einer Demonstration vor einem Stadthaus ereignet. Es erwies sich als äußerst schwierig und zeitaufwendig, den tatsächlichen Sachverhalt - also wer wo aus welchem Anlaß Video- bzw. Fotoaufnahmen gefertigt hat - herauszufinden. Aufgrund der Anfrage eines Journalisten sowie diverser Presseberichte und der telefonischen Bestätigung durch Mitarbeiter der Stadtverwaltung bzw. des zuständigen Polizeipräsidiums ging ich davon aus, daß Mitarbeiter des Magistrats die Teilnehmer der Demonstration vor dem Stadthaus fotografiert hätten.

Bei der Demonstration handelte es sich um die Ausübung des Grundrechts auf Versammlungsfreiheit. Bei Versammlungen unter freiem Himmel - wie hier der Fall - darf in die sonst ungehinderte und freie Ausübung des Grundrechts (Art. 8 Abs. 2 Grundgesetz) durch staatliche Maßnahmen eingegriffen werden. Dazu bedarf es jedoch eines Gesetzes.

Nach allgemeiner Rechtsauffassung stellt die optische Dokumentation einer Demonstration durch Foto- oder Videoaufnahmen einen Eingriff in der Grundrecht der Versammlungsfreiheit dar, unabhängig davon, ob Übersichts- oder Einzelaufnahmen angefertigt werden. Der beabsichtigte Verwendungszweck der Aufnahmen spielt keine Rolle. Es bleibt auch dann ein Eingriff in das Grundrecht der Versammlungsfreiheit, wenn zum Zeitpunkt der Aufnahme noch nicht feststeht, ob diese entwickelt und ausgewertet werden sollen bzw. der Verwendungszweck noch nicht festgelegt worden ist.

Als spezialgesetzliche Regelung für Eingriffe in das Grundrecht auf Versammlungsfreiheit ist das Gesetz über Versammlungen und Aufzüge (VersammlungsG)[63] heranzuziehen. § 19 i. V. m. § 12a regelt, daß nur die Polizei zu Bild- und Tonaufnahmen bei Versammlungen unter freiem Himmel befugt ist. Voraussetzung ist, daß tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von der Versammlung eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung ausgeht. Im weiteren regelt § 12a VersammlungsG abschließend die Nutzung der Bild- und Tonaufnahmen. Sie sind zu vernichten, wenn

- sie nicht zur Verfolgung von Straftaten von Teilnehmern oder
- im Einzelfall auch zur Gefahrenabwehr genutzt werden.

Ausgehend vom oben geschilderten Sachverhalt habe ich die Stadtverwaltung aufgefordert, die fraglichen Fotoaufnahmen zu vernichten, da nur die Polizei zu solchen Aufnahmen befugt ist.

Im Verlaufe des längeren Schriftverkehrs stellte sich jedoch der Sachverhalt anders dar. Während das Polizeipräsidium zuerst zum Sachverhalt nur mitteilte, daß Polizeiangehörige vor Ort gewesen waren - und Videoaufnahmen gemacht hatten -, aber sonst nicht eingegriffen hätten, ergab sich schließlich, daß sich Demonstrationsteilnehmer im Eingangsbereich aufgehalten und den Zugang zum Stadthaus versperrt hatten. Diese Personen wurden vom

---

63 i. d. Fassung der Bekanntmachung vom 15. November 1978, zuletzt geänd. durch Art. 3 Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und des VersammlungsG und zur Einführung einer Kronzeugenregelung bei terroristischen Straftaten vom 09. Juni 1989, BGBl. I, S. 1059

Leiter des Ordnungsamtes - unterstützt von Polizisten - aus dem Gebäude herausgedrängt. Bei dieser Maßnahme haben Mitarbeiter des Magistrats fotografiert. Auch vor diesem Hintergrund ist die Anfertigung der Fotos äußerst fragwürdig. Es kann bezweifelt werden, ob die "Ausübung des Hausrechts" den Träger dieses Rechts befugt, Fotos ohne Einwilligung der Betroffenen anzufertigen. Soweit der Aufenthalt von Personen in einem Haus eine Straftat darstellt, ist die anwesende Polizei befugt und verpflichtet, im Rahmen der Verhältnismäßigkeit alles erforderliche zu tun, um die Straftat aufzuklären.

Polizeipräsidium und Stadtverwaltung haben unterdessen mitgeteilt, daß sowohl die Videoaufnahme als auch die Fotos vernichtet worden sind.

In einem weiteren Fall hat eine Polizeibedienstete in Zivil anläßlich einer *Pressekonferenz Videoaufnahmen von dem Veranstaltungsort* - einem besetzten Haus - und den Teilnehmern der Pressekonferenz gemacht. Dabei fiel sie jedoch auf. Da sie keinen Presseausweis vorzeigen konnte, gab sie eine Telefonnummer des zuständigen Polizeipräsidiums an und entfernte sich anschließend. Es wurde eine ca. einminütige Aufnahme gefertigt.

Zur Begründung dieses Einsatzes gibt das Polizeipräsidium an, daß die Hausbesetzung durch die Veranstalter der Pressekonferenz erfolgt sei. Insbesondere zur Verfolgung der bei der Besetzung verwirklichten Straftatbestände (wie z. B. Hausfriedensbruch und Sachbeschädigung) müsse die Polizei gem. § 163 StPO alle zur Beweissicherung erforderlichen Maßnahmen - wie in diesem Fall das Videographieren - ausschöpfen. Daneben habe die Maßnahme auch der Gefahrenabwehr gedient.

Als Rechtsgrundlage für die Anfertigung von Videoaufnahmen zur Gefahrenabwehr ist § 36 Abs. 1 Ziff. 2 VGPolGBbg heranzuziehen. Diese Rechtsvorschrift befugt die Polizei, Daten durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen über Personen zu erheben, soweit Tatsachen die Annahme rechtfertigen, daß von diesen Personen Straftaten von erheblicher Bedeutung begangen werden sollen, sowie über deren Kontakt- oder Begleitpersonen, wenn die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

Bei einer Datenerhebung durch den verdeckten Einsatz einer Videokamera anläßlich einer Pressekonferenz ist jedoch nicht nur das VGPolGBbg bzw. die StPO hinsichtlich der Eingriffsermächtigung zu prüfen, sondern auch ob und inwieweit die in Art. 5 Grundgesetz (GG) garantierte Pressefreiheit eingeschränkt wird. Ungeachtet dessen, daß gem. Art. 5 Abs. 2 GG die Pressefreiheit den Schranken der allgemeinen Gesetze unterliegt (zu denen unter bestimmten Voraussetzungen das StGB, die StPO und das VGPolGBbg zählen können) ist dennoch zu prüfen, ob bei dem Eingriff das Verhältnismäßigkeitsprinzip gewahrt bleibt. Insgesamt ist die Eingriffsschwelle in die Pressefreiheit hoch anzusetzen angesichts ihrer Bedeutung für eine demokratische Gesellschaft.

Im vorliegenden Fall dürfte bei der Abwägung des Interesses an der Strafverfolgung von Delikten im Zusammenhang mit der Hausbesetzung, der vorbeugenden Verbrechensbekämpfung sowie der Gefahrenabwehr einerseits und der Pressefreiheit andererseits letzterer das größere Gewicht einzuräumen sein:

- Da aus der Einladung zur Pressekonferenz hervorging, daß eine Gruppe über ein anderes Anliegen informieren wollte, konnte aus der Tatsache, daß einzelne Personen aus dieser Gruppe an der Besetzung des Hauses beteiligt waren, in dem die Pressekonferenz stattfand, nicht automatisch geschlossen werden, daß dort öffentliche Bekenntnisse über Straftaten abgelegt würden, die im Zusammenhang mit der Hausbesetzung verübt worden waren.

- Bei den an der Pressekonferenz teilnehmenden Pressevertretern konnte in ihrer überwiegenden Mehrheit nicht davon ausgegangen werden, daß sie Straftaten von erheblicher Bedeutung begehen werden bzw. daß sie Kontakt- oder Begleitpersonen von

Straftätern seien. Somit lag keine Eingriffsermächtigung nach § 36 Abs. 1 Ziff. 1 VGPolGBbg vor.

- Zur Rechtmäßigkeit der verdeckten Datenerhebung reicht die Erfahrung nicht aus, daß es in der Vergangenheit bei Häuserräumungen zu Ausschreitungen gekommen ist, in deren Verlauf Straftaten begangen wurden; vielmehr müssen Tatsachen vorliegen, die sich dem konkreten Anlaß - hier:der Pressekonferenz - zuordnen lassen.

Darüber hinaus wird die Vermutung, daß die verdeckte Datenerhebung mittels Videokamera bei der Pressekonferenz doch nicht das geeignete Mittel war, um die Straftaten aufzuklären, die bei der Besetzung des fraglichen Hauses begangen worden waren, gestärkt durch die Mitteilung der Polizei, daß sie zwischenzeitlich die Identität der Hausbesetzer anderweitig festgestellt habe und eine Löschung der Videoaufnahme beabsichtige.

Die Frage, inwieweit die verdeckte Datenerhebung mittels Videokamera bei der fraglichen Pressekonferenz rechtmäßig war, kann jedoch noch nicht abschließend beantwortet werden, da der Vorgang noch offen ist. Die Stellungnahme der Polizei steht noch aus. Sie hat lediglich unterdessen mitgeteilt, daß sie von ihrer Absicht, die Videoaufnahme zu vernichten, abgerückt ist und die Aufnahme bis zum Abschluß der Ermittlungen aufbewahren möchte.

3.6.5 Stellungnahme zu Verwaltungsvorschriften

3.6.5.1 Vorübergehend zu bestimmten Ermittlungsverfahren betriebene Dateien

Im Berichtszeitraum richteten einige Polizeipräsidien für bestimmte Ermittlungsverfahren Dateien ein. Um die Dateien möglichst ohne Zeitverlust für die Ermittlungen nutzen zu können, wird in solchen Fällen die Datei eingerichtet, ehe das Ministerium des Innern (MdI) die vom Polizeipräsidium erstellten Unterlagen, wie Errichtungsanordnung und Dateienregistermeldung, geprüft und freigegeben hat. Das MdI setzt mich von der Absicht des Polizeipräsidiums in Kenntnis und schickt die Errichtungsanordnung mit der Bitte um Stellungnahme, sobald diese vorliegt. Da es sich um laufende Ermittlungsverfahren handelt, die keinen Zeitaufschub dulden, habe ich gegen dieses Verfahren keine Einwände.

Die vorgelegten Errichtungsanordnungen entsprachen im allgemeinen den Anforderungen des § 48 VGPolGBbg.

In einer Errichtungsanordnung war allerdings mit § 43 VGPolGBbg nicht die richtige Rechtsgrundlage für die Übermittlungen der Daten an die Staatsanwaltschaft (StA) angegeben. Dieser Paragraph regelt die Datenübermittlung an andere Behörden oder öffentliche Stellen, die für die Gefahrenabwehr zuständig sind, soweit die Übermittlung zur Erfüllung polizeilicher Aufgaben erforderlich ist. § 1 VGPolG Bbg weist der Polizei u. a. die Aufgaben der Gefahrenabwehr sowie der vorbeugenden Bekämpfung von Straftaten zu.

Bei Ermittlungen zur Aufklärung einer Straftat handelt die Polizei jedoch nicht im Rahmen ihrer Aufgabenzuweisungen nach dem VGPolGBbg, sondern als "Hilfsbeamte der Staatsanwaltschaft" gem. § 152 Gerichtsverfassungsgesetz (GVG)[64]. Nach § 163 StPO übersendet sie der StA "ihre Verhandlungen", d. h. die Ermittlungsergebnisse ohne Verzug. Die StA ist, insoweit als die Daten für die Durchführung des Ermittlungsverfahrens erforderlich sind, die "Herrin der Daten".

Bei der fraglichen Datei, die ausschließlich im Rahmen eines konkreten

---

64 i. d. Fassung der Bekanntmachung vom 9. Mai 1975, BGBl. I, S. 1077, zuletzt geänd. am 11. Januar 1993, BGBl. I, S. 50

Ermittlungsverfahrens betrieben wird, verfügt die Polizei erst nach Abschluß des Ermittlungsverfahrens im Rahmen ihrer eigenständigen Aufgabenzuweisung nach dem VGPolGBbg über die Daten. Gem. § 41 VGPolG Bbg kann sie personenbezogene Daten von Tatverdächtigen, die sie im Rahmen von Ermittlungsverfahren gewonnen hat, in Dateien speichern und verändern sowie sonst nutzen.

3.6.5.2 Vorläufige Richtlinie "Informationsaustausch Schleuser"

Dazu hat das MdI mir den Entwurf eines gemeinsamen Runderlasses des MdI und des Ministeriums für Arbeit, Soziales, Gesundheit und Frauen des Landes Brandenburg zugeleitet und um Stellungnahme gebeten.

Ziel des Informationsaustausches ist es, Bundes- und Länderbehörden gemeinsame und aufeinander abgestimmte Maßnahmen zur Bekämpfung illegaler Schleusertätigkeiten und damit zusammenhängender Straftaten zu ermöglichen. Dazu erstellt die bei der Grenzschutzdirektion Koblenz eingerichtete "Zentralstelle zur Bekämpfung der illegalen Einreise von Ausländern" Lagebilder, in die auch die von den Ländern mittels des Informationsaustausches erstellten Lagebilder einfließen. Im Rahmen des Informationsaustausches melden die beteiligten Stellen der Zentralstelle Daten wie Nationalität, Alter und Geschlecht, jedoch nicht die Namen der einreisenden Personen. Die vorläufige Richtlinie "Informationsaustausch Schleuser" hat erhebliche datenschutzrechtliche Relevanz angesichts der Tatsache, daß bundesweit mit Ausländerfragen im weitesten Sinn befaßte Behörden an dem Informationsaustausch beteiligt sind. Ein Katalog der Straftatbestände, die bundes- bzw. landesweit ausgetauscht werden dürfen, fehlt. Dies ist nur hinzunehmen, wenn sichergestellt ist, daß in keinem Fall weitere Daten als die o. a. übermittelt werden.

Eine Stellungnahme des MdI liegt dazu noch nicht vor.

3.6.5.3 Bundesweites Meldesystem "Fremdenfeindliche Straftaten"

Die IMK hat auf ihrer Sitzung am 14. Mai 1993 in Potsdam der Einführung dieses Sondermeldedienstes zugestimmt. Dazu wird bei Meldung einer fremdenfeindlichen Straftat an das BKA in den Dateien "Personenfahndung", "Kriminalaktennachweis" (KAN) und "Erkennungsdienst" (AFIS) im Datensatz des Betroffenen der personenbezogene Hinweis (PHW) "Fremdenfeindlich" vergeben.

Obwohl Brandenburg der Einführung des Meldedienstes zugestimmt hatte, war ich an dem Verfahren nicht beteiligt, so daß ich erst nachträglich auf datenschutzrechtliche Kriterien, die bei der Vergabe des PHW zu berücksichtigen sind, hinweisen konnte. Ich habe ausgeführt, daß nicht jede gegen einen Ausländer gerichtete Straftat - auch wenn sie gelegentlich mit ausländerfeindlichen Äußerungen des Täters begleitet wird - mit dem PHW zu versehen ist. Der PHW kann nur dann vergeben werden, wenn der Täter mit der Zielrichtung im Kern zum Ausdruck bringen will, 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. Weder im Bereich Staatsschutz noch in INPOL kann eine Speicherung einer fremdenfeindlichen Straftat allein wegen dieser Qualität an sich vorgenommen werden. Vielmehr müssen die allgemeinen Voraussetzungen für die Speicherung einer Straftat in der Arbeitsdatei PIOS Innere Sicherheit (APIS) bzw. in INPOL vorliegen. Erst wenn die allgemeinen Voraussetzungen zur Speicherung einer Person in diesen bundesweiten polizeilichen Informationssystemen gegeben sind, kann die mit der Tat - ggf. auch die mit einer anderen Straftat - zum Ausdruck kommende Motivation des Straftäters zum Anlaß genommen werden, die Speicherung eines entsprechenden Merkmals zur Person vorzunehmen.

Bedauerlicherweise ist dies bisher bei der Einstellung von Daten im KAN-Bund nicht beachtet worden (s. unter 3.6.2.2). Eine Stellungnahme des MdI zu diesem Schreiben steht noch aus. Die geänderten Errichtungsanordnungen zu den Dateien "Personenfahndung", KAN und AFIS liegen mir noch nicht vor.

3.6.5.4 Datei "Gewalttäter Sport"

Auf der unter 3.6.5.3 angeführten IMK-Sitzung wurde die Errichtungsanordnung zur Datei "Gewalttäter Sport" verabschiedet. An dem Verfahren war ich beteiligt. Dabei habe ich im wesentlichen geltend gemacht, daß vor jedem Informationseingriff geprüft werden muß, ob die Maßnahme geeignet und/oder erforderlich ist, um dem Verfassungsprinzip der Verhältnismäßigkeit zu genügen. Weder das Ministerium des Innern noch die Polizei haben dargelegt, in welcher Weise der Meldedienst geeignete und erforderliche Informationen liefern kann, die der Polizei in konkreten Situationen die Abwehr von Gefahren und die Verfolgung von Straftaten ermöglichen. Zumal - wie das Ministerium des Innern selbst feststellte - gewaltgeneigte Fußballfans nicht mehr an ihrem äußeren Erscheinungsbild zu erkennen sind und sich die Störaktivitäten weg von den Stadien auf die Reisewege verlagert haben.

Unabhängig von einer eventuellen Speicherung in einer Datei muß die Polizei vor Ort anlaßbezogene Maßnahmen ergreifen, wenn es zu Störungen kommt. Auch für die Folgemaßnahmen kann nur die konkrete Situation ausschlaggebend sein. Dies gilt auch für Personen, die als Gewalttäter in der Datei registriert sind. Nimmt die Polizei aufgrund bestimmter Tatsachen an, daß eine konkrete Gefahr besteht, so muß sie Maßnahmen gegen die Störer ergreifen, unabhängig davon, ob sie in der Datei gespeichert sind oder nicht. Die Schwierigkeiten, die sich für die Polizei regelmäßig ergeben, wenn sie einzelne aus einer gewaltbereiten oder gewalttätigen Gruppe herauslösen muß, um deren Personalien festzustellen, werden durch den Meldedienst nicht aufgehoben oder vermindert. Die Datei ist auch ein ungeeignetes Instrument für die Beurteilung einer etwaigen Gefahrenlage. Dazu eignet sich die "Zentrale Informationsstelle Sporteinsätze" (ZIS), die bereits eingerichtet ist. Sie enthält in einem Vorausbericht, der an die zuständigen Polizeidienststellen geht, alle zur Beurteilung einer Gefahrenlage erforderlichen Informationen.

Trotz meiner Bedenken hat die Landesregierung der Errichtungsanordnung zugestimmt. Ende 1993 teilte das MdI mit, daß die als Ausgleichsmaßnahme bis zur endgültigen Realisierung der Datei vorgesehene Anlaß/Zweck-Kombination in der INPOL-"Personenfahndungsdatei" erfolgt ist. Mit dieser Kombination wird bei einer zur Fahndung ausgeschriebenen Person darauf hingewiesen, daß bei der ebenfalls aufgeführten Polizeidienststelle ein Vorgang zu dem Betroffenen existiert.

3.7 Bundeskriminalamtsgesetz

Das Volkszählungsurteil des Bundesverfassungsgerichts[65] macht auch eine Novellierung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtsgesetz - BKAG) erforderlich. Zu dem am 15.12.1993 vorgelegten Entwurf der Bundesregierung habe ich Stellung genommen.

Der Entwurf weist dem Bundeskriminalamt (BKA) nicht nur wie im Gesetz über die

---

65 BVerfGE 65, 1 ff.

Einrichtung eines Bundeskriminalpolizeiamtes (BKAG)[66] die Bekämpfung länderübergreifender und internationaler Kriminalität zu, sondern auch die Bekämpfung der Kriminalität von erheblicher Bedeutung. Ob damit eine Aufgabenerweiterung des BKA bezweckt wird, geht aus der Begründung nicht hervor. Der Begriff "Kriminalität/Straftat von erheblicher Bedeutung" erfüllt das Verfassungsgebot der Normenklarheit nicht, da eine Festlegung in einem Strafkatalog fehlt. Die Definition des Begriffs in der Begründung behebt diesen Mangel nicht. Im Interesse der Normenklarheit sollten die zu weit reichenden Zuständigkeiten und Eingriffsbefugnisse, die das BKA in dem Gesetzentwurf erhält, durch einen Straftatenkatalog, eingegrenzt werden, der definiert, welche Straftaten oder Kriminalitätsformen die Qualität "einer erheblichen Bedeutung" haben oder erreichen.

Nach § 5a des Entwurfs darf das BKA zur Feststellung des Anfangsverdachts Daten erheben. Die Feststellung des Anfangsverdachts sowie Ermittlungen im Vorfeld eines Anfangsverdachts, um festzustellen, ob dieser sich konkretisiert, ist Aufgabe der Strafverfolgungsbehörden der Länder. Der Generalbundesanwalt ist dafür nicht zuständig. Im Unterschied zu den Regelungen des Landespolizeirechts ist hier die Befugnis jedoch nicht von tatsächlichen Anhaltspunkten, die dafür sprechen, daß Straftaten begangen werden sollen, abhängig. Daraus ergeben sich erhebliche Eingriffe in Grundrechte der Betroffenen. Erst bei Feststellung eines Anfangsverdacht stehen dem Tatverdächtigen die Rechte der Strafprozeßordnung zur Verfügung, die er jedoch nicht hat, solange noch weit im Vorfeld eines konkreten Anfangsverdachtes ermittelt wird. Die Erforderlichkeit so tiefgreifender Eingriffe in die Grundrechte der Betroffenen ist im Entwurf nicht dargelegt.

Ein wesentlicher Ansatzpunkt meiner Kritik ist die in § 19 des Entwurfs geregelte datenschutzrechtliche Verantwortung im jeweiligen polizeilichen Informationssystem. In diesem Paragraphen ist die Kontrollzuständigkeit für das INPOL-System allein nach § 24 BDSG geregelt. Abweichend von der gegenwärtigen Praxis wäre es damit den Landesbeauftragten nicht möglich, Protokolle über das Abrufverhalten von Landesbehörden, die ihrer jeweiligen Kontrollzuständigkeit unterliegen, anzufordern. Der Bundesbeauftragte kann jedoch aufgrund eigener Zuständigkeit keine Feststellungen über die Hintergründe einzelner Abrufe treffen. Es wäre den Landesbeauftragten auch verwehrt, Datenbestände, die von der Polizei ihres Bundeslandes in INPOL eingegeben worden sind, selbständig zu prüfen. Damit wäre auch keine förmliche Beanstandung der Datenverarbeitung der Länder im INPOL-System möglich. Sie könnte nur vom BfD ausgesprochen werden, der jedoch keine Adressaten für seine Beanstandungen hätte. Bisher war unumstritten, daß sich die Kontrollzuständigkeit nach Landesdatenschutzgesetzen begründet, wenn eine Landesstelle aufgrund landesgesetzlicher Befugnisse Daten zur Gefahrenabwehr oder Strafverfolgung im INPOL-System speichert oder abruft. Die Kontrollzuständigkeit des BfD ist nach § 24 BDSG gegeben, wenn eine Stelle des Bundes Daten im INPOL-System verarbeitet. Diese bisherige Praxis sollte im Gesetz festgeschrieben werden. In seiner gegenwärtigen vorliegenden Fassung kann § 19 nicht hingenommen werden.

Nach meinem Kenntnisstand ist § 19 in dem unterdessen überarbeiteten Entwurf entsprechend den Einwänden der Datenschutzbeauftragten geändert worden.

3.8 Ausländerwesen

3.8.1 Ausländerzentralregistergesetz

Am 02. März 1994 hat das Bundeskabinett einen Entwurf für ein

---

66 vom 29. Juni 1973, BGBl. I, S. 449, zuletzt geänd. am 9. Dezember, BGBl. I, S. 3393

Ausländerzentralregistergesetz verabschiedet. Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 in Potsdam ausdrücklich begrüßt, daß nunmehr endlich eine gesetzliche Grundlage für das seit 1953 bestehende Ausländerzentralregister geschaffen werden soll. Sie haben sich jedoch insbesondere dagegen gewandt, daß das Ausländerzentralregister nach dem Entwurf nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern auch darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll (s. Anlage 18).

Der Landesregierung gegenüber habe ich mich noch einmal nachdrücklich dagegen gewandt, daß der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden soll und daß vorgesehen ist, in dem Register Angaben zu Personen zu speichern, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden jedoch eigene Informationssysteme zur Verfügung. Deshalb dürfen derartige Erkenntnisse nicht in das Ausländerzentralregister aufgenommen werden.

Ich habe die Landesregierung darum gebeten, durch ein entsprechendes Abstimmungsverhalten im Bundesrat darauf hinzuwirken, daß der von der Bundesregierung vorgelegte Gesetzentwurf in seiner gegenwärtigen Fassung vom Bundesrat nicht gebilligt wird.

3.9 Statistik

3.9.1 Mikrozensusgesetz

Die statistischen Erhebungen nach dem sog. Mikrozensusgesetz und seinen Verordnungen[67] waren Anlaß zu vielen Anfragen und Eingaben an mich. Auf der Grundlage des Bundesgesetzes werden seit 1985 in den alten Bundesländern und seit 1991 in Brandenburg Daten zu Personen, Haushalten und Wohnungen (Erhebungseinheiten) stichprobenartig erhoben. Die Auswahl der Erhebungseinheiten erfolgt aufgrund mathematischer Zufallsverfahren auf der Basis von Flächen oder vergleichbarer Bezugsgrößen (Auswahlbezirke). Die Erhebungen erfassen 1 % der Bevölkerung über 4 Jahre, wobei pro Jahr 0,25 % alte Auswahlbezirke durch neue ersetzt werden. Für die Erhebungsbögen 1 und 1 E besteht Auskunftspflicht, die Bögen 2 und 2 E beruhen auf Freiwilligkeit.

Meiner Behörde obliegt lediglich die datenschutzrechtliche Kontrolle der Umsetzung des Bundesgesetzes im Land Brandenburg. Insoweit habe ich die verwandten Erhebungsbögen geprüft. Sie entsprechen den gesetzlichen Grundlagen. Hinzuweisen ist darauf, daß jeder zur

---

67 Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt vom 10. Juni 1985, BGBl. I, S. 955, i.d.F.d. Änd. vom 17. Dezember 1990, BGBl. 1990 I, S. 2837; Mikrozensusverordnung vom 14. Juni 1985, BGBl. I, S. 967, i. d. Fassung d. Änd. vom 12. April 1991, BGBl. 1991 I, S. 902; Bundesstatistikgesetz vom 22. Januar 1987, BGBl. I, S. 462 und S. 565, i.D.F.d. Änd, vom 17. Dezember 1990, BGBl. 1990 I, S. 2837; Verordnung (EWG) Nr. 3711/91 des Rates vom 16. Dezember 1991.

Auskunft verpflichtete Bürger die Möglichkeit hat, die Erhebungsbögen selbst auszufüllen und an das Landesamt für Datenverarbeitung und Statistik zu verschicken, wenn ihm die übliche Art der Befragung durch einen Interviewer, der dazu speziell ausgebildet und zur Geheimhaltung verpflichtet wurde, nicht behagt.

3.9.2 Wohnungsstatistikgesetz

Ähnlich dem Mikrozensus wurde nach Maßgabe des Wohnungsstatistikgesetzes[68] zum 30. September 1993 in der Bundesrepublik eine einprozentige Gebäude- und Wohnungsstichprobe durchgeführt. Die dafür im Land Brandenburg verwendeten Erhebungsbögen (Wohnungsbogen mit Haushaltsangaben und Gebäudebogen mit Grundstücksangaben) waren aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Zum 30. September 1995 soll darüber hinaus in den neuen Bundesländern auf der Grundlage des Wohnungsstatistikgesetzes eine lückenlose Gebäude- und Wohnraumerfassung erfolgen, wie sie 1987 nach Maßgabe des Volkszählungsgesetzes[69] in ähnlicher Form in den alten Bundesländern durchgeführt wurde. Dabei wird es zu einer umfangreichen Erhebung von auf die Person des Gebäudeeigentümers beziehbaren Daten kommen.

3.9.3 Landesstatistikgesetz

Zu diesem Gesetz liegt bereits ein erster Entwurf vor. In meiner Stellungnahme dazu habe ich insbesondere empfohlen, die dort vorgesehene Regelung der Datenverarbeitung im Auftrag normenklar neu zu fassen sowie in das Gesetz Bestimmungen aufzunehmen, die bereichsspezifisch den Einsatz neuerer technischer Möglichkeiten (z. B. von Laptops) bei der Verar-beitung personenbezogener Daten zu statistischen Zwecken regeln (s. unter 3.9.4).

3.9.4 Einsatz neuer Technik bei statistischen Erhebungen

Um die Erfassung der Daten für den Mikrozensus durch den Interviewer zu erleichtern und auch die Datensicherheit zu erhöhen, plant das Landesamt für Datenverarbeitung und Statistik den zukünftigen Einsatz von Laptops (s. Anlage 1). Sehr sensible personenbezogene Daten, wie sie die Erhebungsdaten zum Mikrozensus darstellen, müssen auf der Festplatte des Laptops nach einem anspruchsvollen mathematischen Verfahren verschlüsselt sein, damit sie bei Diebstahl des Laptops nicht ausgelesen werden können. Die Besonderheit der Datenerfassung durch den Interviewer legt für den Datenversand zum Landesamt die Nutzung von Disketten nahe. Dadurch entstehen weitere Risiken. Diesen kann nur dadurch begegnet werden, daß auch die Disketten nach derselben Methode wie die Festplatte verschlüsselt werden. Ferner ist eine Sicherheitssoftware und -hardware zu bevorzugen, die nur die Nutzung des jeweiligen Statistik-/Erhebungsprogramms zuläßt und den Rechner an den jeweiligen Interviewer bindet.

3.10 Katastrophenschutzgesetz

An dem mir vorgelegten Gesetzentwurf war im wesentlichen zu beanstanden, daß die dort erfolgten Aufgabenbestimmungen zwar durchaus die Verarbeitung personenbezogener Daten zwingend voraussetzen, eine bereichsspezifische Regelung dieser Datenverarbeitung jedoch nicht erfolgt ist. Dies wird im weiteren Gesetzgebungsverfahren zu korrigieren sein.

68

69 vom 18. März 1993, BGBl. I, S. 337
vom 8. November 1985, BGBl. I, S. 2078

3.11 Kommunales

3.11.1 Unzulässige Veröffentlichung im Gemeindemitteilungsblatt

Die Interessenvertreter einer Erbengemeinschaft, die beim Amt für offene Vermögensfragen (AROV) Antrag auf Rückgabe von Grundstücken gestellt hatte, wandten sich im Berichtszeitraum an mich, weil sie sich durch die Veröffentlichung ihres Namens im Zusammenhang mit der Rückübertragung im Mitteilungsblatt der Gemeinde in ihren Persönlichkeitsrechten verletzt sahen. Zuvor hatte die Gemeindevertretung die Erbengemeinschaft um Stellungnahme zum Rückgabeverfahren gebeten und diesen Beschluß öffentlich ausgehängt. Die Erbengemeinschaft antwortete darauf mit einem Offenen Brief. Im letzten Absatz des Offenen Briefs erteilten die Interessenvertreter die Erlaubnis, ihren Brief einschließlich Unterschrift in einer Ausgabe des Mitteilungsblattes abzudrucken. Diese Zustimmung erstreckte sich jedoch nicht auf die Nennung ihrer Namen im redaktionellen Teil des Mitteilungsblattes. Die Interessenvertreter machten vielmehr im Nachsatz ihres Offenen Briefs deutlich, daß sie eine Veröffentlichung auch auszugsweise oder in geänderter Form von einer erneuten Zustimmung abhängig machten, die jedoch nicht erteilt wurde. Die Gemeinde konnte auch nicht davon ausgehen, daß die Zustimmung erteilt worden wäre. Die Namensnennung im redaktionellen Teil war mit der Information verknüpft, daß vermögensrechtliche Ansprüche erst Ende 1992 gegenüber dem AROV konkretisiert worden waren. Gerade diesem Sachverhalt widersprach der Offene Brief jedoch ausdrücklich.

Die Petenten machten zu Recht geltend, daß sie durch die Namensnennung im Zusammenhang mit der von ihnen bestrittene Konkretisierung ihres Antrags auf Rückübergabe von Grundstücken in ein negatives Licht gerückt werden. Da der Sinn des Satzes sich nicht verändern hätte, wenn die Namensnennung nicht erfolgt wäre, ist der Eindruck nicht von der Hand zu weisen, daß die Gemeindevertretung den Sachstand nicht mit der gebotenen Neutralität einer nicht direkt am Verfahren beteiligten öffentlichen Stelle darstellte.

Als Rechtsgrundlage für die Beanstandung der Namensnennung ist § 4 Abs. 1 Bbg DSG heranzuziehen, der festlegt, daß eine Datenverarbeitung - dazu zählt auch das Bekanntgeben von Daten - nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Da es keine einschlägige Rechtsgrundlage für die Namensnennung gibt, konnte sie nur mit Einwilligung der Betroffenen erfolgen. Die Einwilligung lag jedoch nur vor, soweit der Offene Brief einschließlich Unterschrift unverändert abgedruckt wurde.

Mit der Veröffentlichung in dem Mitteilungsblatt, daß der vermögensrechtliche Anspruch Ende 1992 gegenüber dem AROV konkretisiert wurde, teilte die Gemeinde darüber hinaus Einzelheiten aus einem schwebenden Verfahren mit. Dafür gibt es keine rechtliche Grundlage. Sie ist auch nicht durch die Aufgabenzuweisung des Gemeindeamts erforderlich, da die Klärung vermögensrechtlicher Ansprüche nicht durch das Gemeindeamt, sondern durch das ausschließlich zuständige AROV erfolgt.

Meine zu beiden Punkten ausgesprochenen Beanstandungen hat das Gemeindeamt im wesentlichen anerkannt.

3.11.2 Freiwillige Datenerhebung mittels Fragebögen

Mehrere Gemeinden starteten im Berichtszeitraum Datenerhebungsaktionen bei den Gewerbetreibenden, um so Ansatzpunkte für gezielte Wirtschaftsförderungsmaßnahmen zu finden. Darunter beispielsweise:

- die Überarbeitung des Flächennutzungsplans,
- Aufstellung aller Gewerbetreibenden einer Gemeinde,
- Unternehmensbefragung usw.

Die Teilnahme der Unternehmen an der Datenerhebung war freiwillig. Um sicherzustellen, daß die dazu verwendeten Fragebögen datenschutzrechtlichen Anforderungen genügten, baten die Gemeindeverwaltungen mich, die Formulare zu prüfen.

Gem. §§ 4 Abs. 1, 12 Abs. 3 Bbg DSG ist eine Verarbeitung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Die Einwilligung ist schriftlich zu erteilen. Diese schriftliche Einwilligung sahen die jeweiligen Fragebögen auch vor, allerdings erst auf der letzten Seite. Um zu vermeiden, daß Betroffene die Fragen beantworten, ehe sie die Freiwilligkeit zur Kenntnis nehmen, habe ich vorgeschlagen, die schriftliche Einwilligung den Fragen voranzustellen.

3.11.3 Keine Weitergabe der Ermächtigung zum Gebühreneinzug im Lastschriftverfahren bei Aufgabenübertragung

Zahlreiche Gemeinden haben die Abfallentsorgung den Landratsämter übertragen. In diesem Zusammenhang fragte eine Stadtverwaltung bei mir an, ob sie dem nunmehr für die Aufgabe zuständigen Landratsamt alle Daten - einschließlich der für das Lastschrifteinzugsverfahren erforderlichen - übermitteln muß. Sie machte geltend, daß die Bürger nur die Stadtverwaltung ermächtigt hatten, die Abfallentsorgungsgebühren mittels Lastschriftverfahren einzuziehen und nur ihr die dazu erforderlichen Daten zur Verfügung gestellt haben.

Auch ich bin der Auffassung, daß die Gemeinden die für das Lastschrifteinzugsverfahren erforderlichen Daten im Rahmen der Abfallentsorgung nicht an das nunmehr dafür zuständige Landratsamt übermitteln dürfen. Bei dem Lastschrifteinzugsverfahren handelt es sich um eine privatrechtliche Abmachung zwischen den Bankkunden und ihren Banken, durch die dem begünstigten Dritten Zugriff auf das Konto des Bankkunden eingeräumt wird. Diese vertragliche Regelung ist nicht auf andere übertragbar. Dazu bedarf es einer erneuten Abmachung zwischen den nunmehr Beteiligten, ohne die die Bank nicht befugt ist, das Lastschrifteinzugsverfahren durchzuführen. In dem vorliegenden Fall bedeutet dies, daß die Gemeinde zwar verpflichtet ist, alle für die ordnungsgemäße Abrechnung der Abfallentsorgung erforderlichen Daten an die nunmehr zuständige Behörde - das Landratsamt - zu übergeben, nicht aber die Daten des Lastschrifteinzugsverfahrens. Zur Abrechnung der Abfallentsorgung sind diese Daten nicht erforderlich, da es dem Bürger freigestellt ist, wie er die dabei anfallenden Gebühren begleicht. Das Landratsamt kann nicht unbedingt davon ausgehen, daß die Bürger mit ihm dieselbe Abmachung treffen wollen wie mit der Stadtverwaltung.

3.11.4 Akteneinsichtsrecht - ein schwer zu schluckender Brocken für die Verwaltung?

Die Besitzer eines 1988 in der ehemaligen DDR stillgelegten Betriebes haben sich an mich gewandt, weil eine Gemeindeverwaltung ihnen die Einsicht in die zu ihrem Betrieb beim Umweltamt vorhandenen Verwaltungsakten verwehrte. Der Eingabe war ein monatelanges Hinhalten der Verwaltung vorausgegangen, das die verwaltungsinternen Barrieren gut ausleuchtet, die der Umsetzung des in der Brandenburgischen Verfassung garantierten Anspruchs auf Einsicht in Verwaltungsakten entgegenstehen.

Nachdem die Gemeindeverwaltung zunächst mitgeteilt hatte, es gäbe keine Akten, suchte sie sodann Zuflucht in einer partiellen Amnesie und behauptete, sich weder an den Antrag noch an Gespräche dazu zu erinnern zu können, um schließlich in rigor mortis zu verfallen und gar nicht mehr zu reagieren.

Obwohl die Petenten ihren Antrag mit dem in Art. 11 der Brandenburgischen Verfassung garantierten Akteneinsichtsrecht begründet hatten, verweigerte die Verwaltung die Einsicht mit Verweis auf § 29 Verwaltungsverfahrensgesetz für das Land Brandenburg

(VwVfGbbg)[70], in dem ein Akteneinsichtsrecht nur vorgesehen ist, wenn ein Beteiligter am Verwaltungsverfahren die Akteneinsicht zur Verfolgung seiner Rechte benötigt. Da der Betrieb der Petenten nicht mehr existiere und ein Verwaltungsverfahren, an dem die Petenten beteiligt waren, zur Stillegung in der ehemaligen DDR nicht durchgeführt worden war, sah die Verwaltung für die Akeneinsicht keine Rechtsgrundlage, weil es "nicht wünschenswert" sei, "wenn Amtsinterna Gegenstand eines allgemeinen Besichtigungsrechts werden". Lapidar befand die Gemeinde, daß es ein "Akteneinsichtsrecht nach Maßgabe der Verfassung des Landes Brandenburg" nicht gebe.

Diese Rechtsauffassung widerspricht Art. 11 Verfassung des Landes Brandenburg sowie der "Richtlinie des Rates der Europäischen Gemeinschaften vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt" (s. unter 8.1). Letztere bestimmt, daß jede natürliche und juristische Person des Privatrechts Auskunft über die bei einer Behörde vorhandenen Umweltinformationen sowie Einsicht in Umweltakten und in die in sonstigen Informationsträgern enthaltenen Umweltinformationen verlangen kann.

Erst nachdem ich die Gemeindevertretung in der Angelegenheit angesprochen hatte, korrigierte die Verwaltung ihre Auffassung und gewährte den Petenten Akteneinsicht.

3.11.5 Knöllchen aus dem Wohnzimmer

Durch die Eingabe eines Bürgers wurde ich darauf hingewiesen, daß eine Mitarbeiterin des Rechts- und Ordnungsamtes einer Stadtverwaltung Verstöße gegen die Straßenverkehrsordnung zu Hause auf ihrem privaten PC arbeitete.

Ein Kontrollbesuch bestätigte, daß eine Mitarbeiterin des Verkehrsamtes mit Billigung des Amtsleiters ihren privaten Computer in ihrer Wohnung nicht nur zur Bearbeitung von Ordnungswidrigkeiten im ruhenden Straßenverkehr nutzte, sondern auch Programme erstellte, die eine umfassende Bearbeitung der Ordnungswidrigkeiten von der Erfassung der auf der Straße ermittelten Daten bis zur Erstellung der Bußgeldbescheide und der Zahlungseingangskontrolle ermöglichte.

Die Verarbeitung personenbezogener Daten auf privaten Computern ist grundsätzlich abzulehnen, weil davon auszugehen ist, daß die in § 10 Abs. 2 Bbg DSG geforderten Maßnahmen zur Sicherheit personenbezogener Daten unter diesen Bedingungen normalerweise nicht eingehalten werden können. Jede öffentliche Stelle ist nach § 7 und 10 Bbg DSG zur datenschutzrechtlichen Selbstkontrolle verpflichtet. Dazu gehört insbesondere auch, daß die innerbetriebliche Organisation der Arbeit so gestaltet wird, daß den Mitarbeitern entsprechende Räume und technische Hilfsmittel im Bereich der Verwaltung zur Verfügung gestellt werden.

Nach einer Darstellung der Mängel sicherte das Ordnungsamt zu, die Bearbeitung der Ordnungswidrigkeiten in die Dienststelle zu verlagern. Dort sollte sie allerdings solange auf dem privaten PC der Mitarbeiterin betrieben werden, bis das für die Bearbeitung von Ordnungswidrigkeiten vorgesehene Softwarepaket zur Verfügung stand.

4 Justiz

4.1 Strafverfahrensänderungsgesetz

Die Datenschutzbeauftragten des Bundes und der Länder haben seit Jahren eine gesetzliche

---

70 vom 26. Februar 1993, GVBl. I, S. 26

Regelung der Informationsverarbeitung im Strafverfahren gefordert. Nunmehr liegt ein Gesetzesantrag der Länder zum Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG 1994) vor, der Dateienregelungen im Strafverfahren enthält. Die im derzeitigen Entwurf enthaltenen Vorschriften über den Umgang mit personenbezogenen Daten genügen in wesentlichen Bereichen nicht den Anforderungen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung.

Die Datenschutzregelungen des StVÄG 1994 stellen gegenüber dem Regierungsentwurf aus dem Jahre 1989 bei datenschutzrechtlicher Betrachtung eine inhaltlich nachteilige Veränderung dar. So sind Regelungen zum Schutz des Rechts auf informationelle Selbstbestimmung zum Teil entfallen bzw. erheblich abgeschwächt worden.

Im Hinblick auf die Vielzahl höchst sensibler Daten, insbesondere auch über Opfer von Straftaten und Zeugen in den strafrechtlichen Ermittlungsakten, ist es nicht zu vereinbaren, wenn die Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienen. Vielmehr sind die einzelnen Zwecke und die zugriffsberechtigten Stellen abschließend und normenklar festzulegen.

Durch die Verwendung von generalklauselartigen Formulierungen im vorliegenden Entwurf eines StVÄG entsteht hingegen die Gefahr einer fehlenden Normenklarheit und einer entsprechenden Rechtsunsicherheit. Die Forderung des Bundesverfassungsgerichts, Datenübermittlungen nur in gesetzlich bestimmten Fällen zuzulassen, wird im Entwurf sogar dadurch umgekehrt, daß eine Vielzahl von Übermittlungen von Daten aus dem Strafverfahren an andere öffentliche Stellen zugelassen wird, soweit keine anderen gesetzlichen Bestimmungen einer solchen Übermittlung entgegenstehen. Im Hinblick auf die derzeit in vielen Bereichen noch fehlenden bereichsspezifischen Regelungen erscheint dies besonders bedenklich.

Darüber hinaus wird der besonderen Sensibilität des Inhalts von Strafakten durch die erweiterte Ermöglichung einer Übersendung der gesamten Akte anstelle einer bloßen Einsicht oder Auskunft aus der Strafakte nicht genügend Rechnung getragen. Desweiteren sieht der Entwurf die Möglichkeit einer Akteneinsicht schon für den Fall vor, wenn die Erteilung einer Auskunft mit einem unverhältnismäßigem Aufwand verbunden ist. Dadurch wird das Interesse der Verwaltung an eine Entlastung von "unverhältnismäßigem Aufwand" als ausreichend angesehen, das Recht auf informationelle Selbstbestimmung einzuschränken. Das Grundrecht des Bürgers wird dementsprechend nicht ausreichend gewichtet.

Ebenso wird dem Gebot der Zweckbindung dadurch widersprochen, daß der Entwurf für die verschiedenen Phasen der Informationsgewinnung und Verarbeitung durch die Staatsanwaltschaft und die Polizei in dem Strafverfahren bzw. der Strafrechtspflege keine differenzierten Regelungen enthält. So findet auch eine Unterscheidung nach dem Grad der Betroffenheit der am Verfahren beteiligten Personen nicht statt. Die Befugnis für Gerichte, Staatsanwaltschaften und andere Justizbehörden, personenbezogene Daten in gemeinsamen oder verbundenen Dateien zu speichern, führt zu einer nicht überschaubaren und damit auch nicht mehr nachvollziehbaren Verflechtung der verschiedensten Datensammlungen; insbesondere auch zwischen Strafverfolgung und Gefahrenabwehr.

Darüber hinaus ist durch den Entwurf nicht sichergestellt, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird. Vielmehr ist die Regelung im Entwurf über eine Verwendung personenbezogener Informationen zu Forschungszwecken im Hinblick auf entsprechende Regelungen des Brandenburgischen Datenschutzgesetzes als erheblicher datenschutzrechtlicher Rückschritt zu bewerten (s. Anlage 17).

Der Minister für Justiz wurde dementsprechend unter Hinweis auf den o. a. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gebeten, die gravierenden

datenschutzrechtlichen Bedenken gegen den vorliegenden Gesetzesvorwurf aufzugreifen und die diesbezüglichen Empfehlungen bei den Beratungen im Strafrechtsausschuß der Justizministerkonferenz einzubringen.

4.2 Verbrechensbekämpfungsgesetz

Mit dem vorliegenden Entwurf setzt sich die Tendenz fort, daß in immer neuen Gesetzen bzw. in Novellierungen gerade erst verabschiedeter gesetzlicher Regelungen die Eingriffsbefugnisse für die Sicherheits- und Strafverfolgungsbehörden stetig erweitert werden. Die mit dem Gesetz zur Bekämpfung der organisierten Kriminalität und der Rauschgiftkriminalität sowie dem Geldwäschegesetz geschaffenen zusätzlichen Ermittlungsbefugnisse für die Strafverfolgungsbehörden konnten in der Praxis noch gar nicht wirksam werden. Wie oft und mit welchem Ergebnis sie angewandt bzw. sie eingesetzt wurden, läßt sich daher auch noch nicht nachprüfen. Dennoch liegt mit dem o. g. Entwurf bereits wieder ein weiteres Gesetz mit zusätzlichen Eingriffsbefugnissen für die Strafverfolgungsbehörden vor. Ich habe daher in meiner Stellungnahme u. a. gefordert, daß zunächst das Ergebnis einer Erfolgskontrolle der bereits vorhandenen Eingriffsbefugnisse abgewartet wird, ehe sie mit dem vorliegenden Entwurf erweitert werden.

U. a. sieht der Entwurf in Art. 4 Nr. 2 vor, den Katalog der Straftaten, nach denen gem. § 100a StPO Telefonabhörmaßnahmen angeordnet werden können, zu erweitern. In diesem Zusammenhang ist der Entwurf der Fraktion der SPD eines zweiten Gesetzes zur Bekämpfung des illegalen Rauschgifthandelns und anderer Erscheinungsformen der organisierten Kriminalität (2. ORGKG mit Stand vom 27.01.1993) zu begrüßen. Hier wird nämlich vorgeschlagen, jährlich einen Bericht über Anlaß, Verlauf und Ergebnisse abgeschlossener Telefonabhörmaßnahmen nach § 100a StPO mit Nennung der antragstellenden Staatsanwaltschaft und des die Anordnung treffenden Gerichts zu veröffentlichen (Art. 12 Nr. 5 des o. g. Entwurfs). Der Bericht sollte jedoch nicht nur die Zahl der überwachten Anschlüsse, sondern auch die Zahl der erfaßten Telefongespräche und der durch diese Maßnahme betroffenen Bürger beinhalten.

Der Entwurf sieht mit Art. 4 Nr. 12 ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister vor. Die Einzelregelungen lassen allerdings eine Reihe von Fragen offen. Nicht zuletzt bleibt fraglich, ob es überhaupt erforderlich ist, solche Datenarten, wie Fahrlässigkeitstaten, Einstellungen, Freisprüche, anonyme Anzeigen usw., in einer Datei mit bundesweitem Zugriff zwei Jahre lang zu speichern mit der Möglichkeit, diese Frist noch zu verlängern.

Problematisch ist schließlich, daß das Register, in dem sämtliche Ermittlungsverfahren - auch im Bagatelldeliktbereich - gespeichert sind, nicht nur den Staatsanwaltschaften, sondern auch der Polizei bundesweit zur Verfügung steht. Im Informationssystem der Polizei (INPOL) ist eine Speicherung nur bei überregionaler Bedeutung der Straftat zulässig.

Dies gilt auch für den Zugriff der Verfassungsschutzbehörden, bei dem zu befürchten ist, daß so das Trennungsgebot zwischen Polizei und Nachrichtendiensten unterlaufen wird.

Abgelehnt habe ich die im Art. 12 durch Änderung des Gesetzes zu Art. 10 Grundgesetz (G 10)[71] vorgesehene Erweiterung der Befugnisse des Bundesnachrichtendienstes (BND),

---

71 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 Grundgesetz) vom 13. August 1968, BGBl. I, S. 949, zuletzt geändert am 27. Mai 1988, BGBl. I, S. 997

durch die dieser in die Bekämpfung der organisierten Kriminalität mit einbezogen werden soll.

Der BND hat die gesetzliche Aufgabe, Erkenntnisse über das Ausland zu sammeln, die von außen- und sicherheitspolitischer Bedeutung sind. Von sicherheitspolitischer Bedeutung sollen nun nicht nur die in § 3 G 10-Gesetz bislang ausdrücklich erwähnte militärische Bedrohung, sondern auch andere Aktivitäten sein, wenn sie für die Sicherheit und den Bestand der Bundesrepublik Deutschland als Ganzes eine ernste Gefahr darstellen können.

Bei der vom BND zur Abwehr der Gefahr eines bewaffneten Angriffs bisher praktizierten Fernmeldeaufklärung nach dem G 10-Gesetz ist aus datenschutzrechtlicher Sicht von zentraler Bedeutung, daß keine Begrenzung auf bestimmte Personengruppen erfolgt. Vielmehr werden - anders als bei zielgerichteten Maßnahmen der technischen Überwachung zur Strafverfolgung - in der Art einer Rasterfahndung ohne Vorliegen eines Anfangsverdachts unvermeidlich in großer Zahl Unbeteiligte flächendeckend in Abhörmaßnahmen mit einbezogen. Damit wird in großem Umfang in das Fernmeldegeheimnis eingegriffen, das nicht nur durch Art. 10 Grundgesetz sondern auch international durch Art. 8 der Europäischen Menschenrechtskonvention und Art. 17 des Internationalen Paktes über bürgerliche Rechte besonders geschützt ist.

Durch den Entwurf wirkt der BND - ohne ausdrückliche Änderung seiner Aufgaben - faktisch bei der Verbrechensbekämpfung mit, indem er die von ihm erhobenen personenbezogenen Daten an Strafverfolgungsbehörden übermitteln darf. Hier wären zumindest verstärkte datenschutzrechtliche Kontrollen im G 10-Bereich erforderlich. Die bisher bestehende Einschränkung der Kontrollkompetenz des Bundesbeauftragten für den Datenschutz muß entfallen.

Grundsätzlich erfüllt es mich mit Sorge, daß in der Gesetzgebungshektik im Bereich der Inneren Sicherheit der Schutz der Persönlichkeitsrechte der Bürger zu kurz kommt. Das Prinzip, daß der unbescholtene Bürger ein Recht hat, "vom Staat in Ruhe gelassen zu werden", findet hier keine Anwendung. Vielmehr wird er mit Verweis auf ein vermeintliches Grundrecht auf "Schutz vor Verbrechen" bei Strafverfolgungsmaßnahmen zunehmend in Anspruch genommen.

4.3 Erstes Gesetz zur Bereinigung von SED-Unrecht

Da nach dem Vertrag über die Herstellung der Einheit Deutschlands (Einigungsvertrag) Strafurteile der DDR-Justiz grundsätzlich wirksam blieben, war es notwendig, eine gesetzliche Grundlage dafür zu schaffen, daß alle Personen rehabilitiert werden können, die Opfer einer politisch-motivierten Strafverfolgungsmaßnahme geworden waren. Dies ist mit dem ersten Gesetz zur Bereinigung von SED-Unrecht (Erstes SED-Unrechtsbereinigungsgesetz)[72] geschehen. Soweit danach strafgerichtliche Entscheidungen auf Antrag für rechtsstaatswidrig erklärt und aufgehoben worden sind, können soziale Ausgleichsleistungen in Form von Kapitalentschädigungen, Unterstützungsleistungen und Versorgungsmaßnahmen gewährt werden[73].

Für die Beantragung solcher sozialer Ausgleichsleistungen wird in Brandenburg ein Fragebogen verwendet, in dem nicht - wie in anderen Bundesländern - direkt nach einer

---

[72]

[73] vom 29. Oktober 1992, BGBl. I S. 1814

vgl. Art. 1 des 1. SED-UnBerG §§ 16 ff. Strafrechtliches Rehabilitierungsgesetz - StrRehaG -

inoffiziellen oder offiziellen Mitarbeit beim MfS/AfNS gefragt wird. Es wird lediglich darauf hingewiesen, daß dies ein Ausschlußgrund für die beantragten Leistungen sein kann und die Abgabe einer Erklärung, daß Umstände, die einen Ausschluß der Leistungen gem. der vorgenannten Vorschrift[74] rechtfertigen, nicht bekannt sind, gefordert.

4.4 Einführung von Informationstechnik im Gerichtsvollzieherbüro

Gerichtsvollzieher verarbeiten bei der Erledigung der ihnen übertragenen Aufgaben in erheblichem Umfang personenbezogene Daten. Daher begrüße ich es ausdrücklich, daß das Ministerium der Justiz den Entwurf einer allgemeinen Verfügung vorgelegt hat, um diesen Bereich im Hinblick auf den Einsatz von Informationstechnik einer genaueren Regelung zu unterwerfen.

Es erscheint mir aber notwendig, an einzelnen Stellen der allgemeinen Verfügung den Datenschutzaspekt wegen der besonderen Sensibilität der im Gerichtsvollzieherbüro verwendeten Daten noch stärker Rechnung zu tragen und so das diesbezüglich in anderen Bundesländern erreichte Datenschutzniveau auch für Brandenburg sicherzustellen (s. unter 1.4 und Anlage 1).

Ich habe demzufolge gegenüber dem Ministerium der Justiz aus datenschutzrechtlicher Sicht einige Änderungen empfohlen. So sollte die vorgelegte allgemeine Verfügung dahingehend ergänzt werden:

- daß der Gerichtsvollzieher als speichernde Stelle im Sinne des Bbg DSG unmittelbar für die Beachtung und Einhaltung des Datenschutzes verantwortlich ist und so die Kontrollbefugnis des Landesbeauftragten für den Datenschutz in diesem Bereich hervorgehoben wird;

- daß das für den Bürobetrieb eingesetzte Informationssystem zur Ausstattung des Geschäftszimmers gehört und dadurch unter Hinweis auf das Brandenburgische Datenschutzgesetz eine ausreichende Kontrollmöglichkeit durch die Aufsichtsbehörden gewährleistet wird;

- daß für die Beantragung des Einsatzes der Informationstechnik auf die Regelung im Bbg DSG zur Sicherstellung des Datenschutzes und zur Dateibeschreibung[75] verwiesen und so die Wahrung des diesbezüglichen datenschutzrechtlichen Standards klargestellt wird;

- daß zur Präzisierung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz auf die entsprechende Vorschrift des Bbg DSG ausdrücklich hingewiesen wird;

- daß zur Wahrung des Datengeheimnisses der Gerichtsvollzieher vor Aufnahme einer automatischen Datenverarbeitung durch den Direktor des Amtsgericht auf die Pflicht zum Wahren des Datengeheimnisses hinzuweisen ist.

4.5 Anonymisierung von Prüfungsakten beim 2. juristischen Staatsexamen

---

74

75 § 16 Abs. 2 StrRehaG

§§ 7 und 8 Bbg DSG

Im Land Brandenburg sollen von den Rechtsreferendaren im Rahmen der zweiten juristischen Staatsprüfung ausschließlich Klausuren geschrieben werden. Diese werden auf Grundlage von Originalakten mit oft sehr sensiblen Daten hergestellt, z. B. Gerichtsakten.

Mit dem Ministerium der Justiz wurde sich auf folgendes verständigt: Zur Verhinderung der Beeinträchtigung der Persönlichkeitsrechte der Verfahrensbeteiligten sollen daher keine Originalakten an die Prüfungskandidaten ausgehändigt werden, sondern lediglich Aktenauszüge, in denen die Namen und die Anschriften der Parteien und ihrer Anwälte geändert werden. Ebenso soll in der mündlichen Prüfung hinsichtlich der Kurzvorträge, die als Examensaufgabe zu halten sind, verfahren werden. Auch hierbei sollen den Kandidaten lediglich Aktenauszüge erst eine Stunde vor Vortragsbeginn übergeben werden. Originalakten, aus denen sich die Namen und Anschriften der Parteien und ihrer Anwälte ergeben, sollen auch bei der mündlichen Prüfung keine Verwendung finden.

Festzuhalten bleibt, daß in allen Fällen eine Ausgabe der Akten ohne Einverständnis der Betroffenen oder ohne eine Anonymisierung, die keine Rückschlüsse auf die Beteiligten mehr zuläßt, datenschutzrechtlich unzulässig ist.

5 Bildung, Jugend und Sport

5.1 Verwaltungsvorschriften und Verordnungen im Schulbereich

Das Ministerium für Bildung, Jugend und Sport hat im Berichtszeitraum von seiner Ermächtigung gem. § 75 Erstes Schulreformgesetz[76] Gebrauch gemacht und verschiedene Verwaltungsvorschriften und Verordnungen im Schulbereich erlassen.

5.1.1 Verwaltungsvorschriften über die Aufnahme von Schülerinnen und Schüler in die Grundschule (VV-GSAufn)

Die Vorschrift regelt alle für die Einschulung erforderlichen Schritte und Maßnahmen. Dabei wird unter Nr. 1 Abs. 2 auf die Übermittlungsbefugnis von Listen personenbezogener Daten der Schulanfänger durch die zuständigen Meldebehörden gem. § 5 Abs. 2 Erste Verordnung zur Veränderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (1. MeldeDÜÄV)[77] an die Schulverwaltungsämter verwiesen; dagegen läßt sich im Entwurf der Verwaltungsvorschrift keine Löschungsregelung dieser Daten in Analogie zu § 19 Abs. 2 Buchst. b Bbg DG entnehmen. Falls dazu nicht eine Vorschrift an anderer Stelle vorgesehen ist, habe ich angeregt, die Verwaltungsvorschrift diesbezüglich zu ergänzen.

Für fremdsprachige schulpflichtige Kinder kann gem. § 8 Abs. 3 eine abweichende Regelung für die Einschulung getroffen werden. Soweit bei der in jeder Hinsicht viel zu unbestimmten Regelung auch offen bleibt, ob dadurch eine datenschutzrelevante Ungleichbehandlung möglich sein soll, ist zu fordern, daß dies ausdrücklich ausgeschlossen sein soll.

5.1.2 Verwaltungsvorschriften über die Bestellung und Tätigkeit von Beratungslehrerinnen und Beratungslehrern (VV-Beratungslehrer)

Nach dieser Vorschrift hat die Schule für bestimmte Problembereiche Lehrer zur Verfügung zu stellen, die die Schüler in verschiedenen Lebensbereichen (z. B. Drogenprobleme) beraten. Die unter Nr. 4 Abs. 3 aufgezählten Aufgaben und Aufgabenbereiche von Beratungslehrern

---

[76]

[77] vom 1. Juli 1992, GVBl. I, S. 258
vom 8. Dezember 1993, GVBl. II, S. 776

gehen meiner Ansicht nach weit über den Rahmen der Erfüllung des allgemeinen schulischen Bildungs- und Erziehungsrahmens hinaus. Im Hinblick auf einen ggf. erforderlichen Ausgleich divergierender Interessen der Eltern und ihrer Kinder ist gegen eine Beratung und Betreuung, die auf ausdrücklichen Wunsch der Schüler erfolgt, auch aus datenschutzrechtlicher Sicht nichts einzuwenden; allerdings wird in diesen Fällen zu prüfen sein, ob nicht die Eltern - zumindest im nachhinein - darüber zu informieren sind.

5.1.3 Verwaltungsvorschriften über die Schulpsychologische Beratung (VV-Schulpsychologische Beratung)

Bei dieser Verwaltungsvorschrift ist ebenfalls eine Beratung und Betreuung minderjähriger Schülerinnen und Schüler ohne Zustimmung der Erziehungsberechtigten zulässig. Gerade im Hinblick auf die tiefgreifenden Einwirkungsmöglichkeiten einer psychologischen Betreuung und Beratung halte ich eine nachträgliche Information der Eltern für unbedingt notwendig. Insbesondere auch, zumal mangels ausgebildeter Fachkräfte diese Aufgaben nach Nr. 9 auch Nichtpsychologen wahrnehmen dürfen.

5.1.4 Verwaltungsvorschrift über wissenschaftliche Untersuchungen in Schulen (VV-WissU)

Die Vorschrift gilt für wissenschaftliche Untersuchungen über Bildungs- und Erziehungsprozesse an Schulen, die durch öffentliche Stellen oder Körperschaften und Anstalten des öffentlichen bzw. privaten Rechts zu genehmigen sind. Ein mir Ende 1992 vorgelegter Entwurf wurde zwischenzeitlich völlig überarbeitet, ohne daß meine Empfehlung über die Verwendung alternativ formulierter Einwilligungserklärungen aufgenommen worden ist.

Weiterhin sollen den Anträgen gem. Nr. 3 Buchst. g alle Unterlagen beigefügt werden. Dazu zählt auch die Einwilligungserklärung des Betroffenen, wenn eine gesetzliche oder rechtliche Regelung die vorgesehene Erhebung nicht zuläßt. Insoweit wäre die von mir angeregte Präzisierung möglich gewesen.

Ich habe ausdrücklich alternativ formulierte Einwilligungserklärungen empfohlen, weil selbst renommierte Forschungsinstitute der alten Bundesrepublik für ihre Forschungsvorhaben Einwilligungserklärungen verwendet haben, worin es u. a. hieß: "Ich möchte nicht, daß mein Kind an wissenschaftlichen Untersuchungen teilnimmt." So formuliert stellt eine "Einwilligungserklärung" faktisch eine Verweigerungserklärung dar. Auf die Eltern wird indirekt Zwang ausgeübt, die Nichtteilnahme ihres Kindes an der Studie ausdrücklich zu offenbaren. Manche Eltern werden unter diesen Umständen davon abgehalten, die von ihnen nicht gewollte Teilnahme abzulehnen.

Nur eine "neutrale Formulierung" einer Einverständniserklärung löst das Problem befriedigend. Sie könnte lauten: "Ich bin mit der Verarbeitung (Erhebung und Übermittlung) der Daten meines Kindes im Rahmen der (speziellen) wissenschaftlichen Untersuchung nicht einverstanden/einverstanden."

5.1.5 Verwaltungsvorschrift über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen (VV-Datenschutz/Statistik)[78]

Im Entwurf dazu wurde unter Nr. 1 ("Grundsätze") bei der Erhebung von personenbezogenen Daten auf die Möglichkeit des Zurückgreifens auf bereits in der Schule vorliegende Daten

---

78 vom 26. November 1993, ABl., S. 1730

verwiesen. Hier besteht jedoch die Gefahr, daß aus Bequemlichkeit, Unkenntnis oder anderen Gründen gegen den datenschutzrechtlichen Grundsatz der Zweckbindung bereits erhobener Daten gem. § 13 Abs. 1 Bbg DSG verstoßen wird. Ich habe deshalb eine entsprechende Klarstellung in der Verwaltungsvorschrift gefordert. Eine Durchbrechung des Zweckbindungsgrundsatzes wäre nur durch eine materiell-rechtliche Regelung zulässig.

5.1.6 Sonstige Verwaltungsvorschriften und Verordnungen

Bei den folgenden Verwaltungsvorschriften

- Verwaltungsvorschriften über die Arbeit der Sonderpädagogischen Förder- und Beratungsstellen

- Prüfungsordnung für die Abiturprüfung in der gymnasialen Oberstufe (PO - GOST)[79]

- Verordnung über die Ausbildung und Prüfung in Einrichtungen des Zweiten Bildungsweges (Ausbildungs- und Prüfungsordnung Zweiter Bildungsweg - APO-ZBW -)[80]

- Verordnung über die Durchführung des Berufspraktikums im Erzieherberuf (ErzberPrak-VO)

- Vorläufige Ausbildungs- und Prüfungsordnung der Fachschulen im Land Brandenburg (VAPO-FS)[81]

hatte ich keine datenschutzrechtlichen Bedenken.

5.2 Eingaben/Anfragen aus dem Schulbereich

5.2.1 Inhalt von Hausaufgaben

Ein Bürger bat mich um datenschutzrechtliche Beurteilung folgenden Problems: Die Schule seines Kindes hatte als Hausaufgabe einen Aufsatz über die häuslichen Verhältnisse aufgegeben. Eine solche Aufgabe schien ihm "ein wenig zu sehr in die Privatsphäre zu reichen".

In einer solchen Situation sind Bürger möglichst an einem praktischen Lösungsvorschlag interessiert; deshalb habe ich ihm geraten, in einem vertraulichen Gespräch mit dem Lehrer zu versuchen, ein alternatives, weniger verfängliches Thema zu vereinbaren. Dieses Vorgehen war offensichtlich erfolgreich, denn ich erhielt daraufhin keine Rückfragen mehr.

Prinzipiell vertrete ich auch aus der Sicht des Datenschutzes keinesfalls die Ansicht, daß die Familie in der Schule ein Tabu-Thema sein soll; jedoch sehe ich in dessen Behandlung erst dann ein lohnenswertes pädagogisches Ziel, wenn dies im Zusammenhang mit einer beabsichtigten Diskussion von Persönlichkeitsrechten und ihrer Bedeutung geschieht. Diese Auffassung habe ich dem Ministerium für Jugend, Bildung und Sport im Zusammenhang mit der Eingabe vorgetragen; sie ist dort aufgeschlossen aufgenommen worden.

79

80 vom 27. Juli 1993, GVBl. II, S. 592

81 vom 1. November 1993, GVBl. II, S. 700

vom 1. November 1993, GVBl. II, S. 796 (VAPO-FS)

5.2.2 Schweigsame Elternversammlungen

Die Handhabung des Datenschutzes in der Schule bereitet derzeit offenbar noch große Unsicherheiten. Eine Petentin berichtete mir über eine für sie "unangenehm fremde Elternversammlung, bei der die Leistungskarten schweigend verteilt wurden" und "das Gefühl bestand, ja nicht zu genau zum Nachbarn zu gucken" sowie eine verunsicherte "Lehrerin, die auch das Offen-über-Leistungen-Reden besser fand, aber nun nicht (mehr) darf".

Die Verwaltungsvorschrift über Akten in Schulen in öffentlicher Trägerschaft (VV-Schulakten)[82] ist zwar restriktiv abgefaßt und sieht eine Offenbarung von Schülerdaten nur mit Einverständnis vor. Dies bedeutet nicht - wie viele Lehrer und Eltern meinen -, daß in der Praxis auf der Basis einer schriftlich festgehaltenen Einwilligungserklärung gem. § 4 Abs. 1 und 2 Bbg DSG eine Offenbarung erfolgen kann.

Die Eltern und Lehrer eröffnen sich damit Möglichkeiten, in einem selbst festgelegten Rahmen, z. B. bei Elternversammlungen, Meinungen über den Unterricht einschließlich Leistungsbeurteilung auszutauschen. Niemand ist damit ausgegrenzt, jeder kann sich in eine offene Diskussion einbringen und erfahrungsgemäß ergeben sich dadurch auch bessere Lösungswege für anstehende Probleme. Diese Entscheidung für eine weniger restriktive Handhabung des Datenschutzes in der Schule stellt damit ein schönes Beispiel dar, daß das Recht auf informationelle Selbstbestimmung aktiv zu gebrauchen ist. Keinesfalls kann jedoch durch Mehrheitsbeschluß gegen den Willen eines einzelnen eine Offenbarung durchgesetzt werden.

5.2.3 Erhebungsbögen des Landesamtes für Soziales und Versorgung bzgl. Eingliederungshilfe für Sprach- und Hörgeschädigte

Aufgrund einer Eingabe waren Erhebungsbögen des Landesamtes für Soziales und Versorgung, die als Anträge auf Gewährung von Leistungen der Eingliederungshilfe für die Förderung von Sprach- und Hörgeschädigten genutzt werden, in bezug auf die Zulässigkeit der Abfragen zu überprüfen. Dazu gehörten auch die Erklärungsbögen zu Einkommen und Einkünften.

Die Prüfung ergab, daß weitere im Haushalt des Unterhaltspflichtigen oder außerhalb dieses lebende Personen (Kinder, Familienangehörige, sonstige Angehörige oder unterstützte Personen) nur dann Angaben liefern müssen, wenn sie unterhalts- oder kostenersatzpflichtig sind. Trifft dies nicht zu, sind über diese Personen keine Angaben zu machen. Eine Abforderung dieser Daten ist unzulässig, denn es gelten hier nicht nur §§ 60 - 65 SGB I[83], sondern auch §§ 116 (Pflicht zur Auskunft) i.V.m. 28 (Personenkreis) Bundessozialhilfegesetz (BSHG)[84]. Im allgemeinen sind nach § 28 BSHG nur die Eltern unterhaltspflichtig. Deshalb sind beispielsweise Geschwister nicht zur Auskunft verpflichtet, da sie nur moralisch, jedoch nicht rechtlich verpflichtet sind, Unterhalt zu gewähren.

Dies habe ich dem Landesamt für Soziales und Versorgung mitgeteilt und eine Änderung der

---

82

83 ABl. MBJS 1992, S. 10

Sozialgesetzbuch (SGB), 1. Buch (I), vom 11. Dezember 1975, BGBl. I, S. 3015, zuletzt geänd. 24. Juni 1993, BGBl. I, S.
84 1038

i. d. Fassung der Bekanntmachung vom 10. Januar 1991, BGBl. I, S. 94, ber. S. 808

Erhebungsbögen in diesem Sinne angemahnt. Zusätzlich habe ich auf die fehlenden Angaben bezüglich der Rechtsgrundlagen hingewiesen und eine Ergänzung gefordert.

5.2.4 Adreßlisten von Referendaren

Im Rahmen ihrer Dissertation wollte eine Doktorandin von einer ca. 25 Referendare umfassenden Versuchsgruppe Videoaufnahmen machen bzw. mittels Fragebögen Daten erfassen. Sie bat mich um "Genehmigung", damit ihr vom Ministerium für Bildung, Jugend und Sport (MBJS) die Liste der zur Zeit verfügbaren Referendare im Bereich der Ausbildung zu Sportlehrern ausgehändigt werden könne. Ziel der Dissertation sollte die Erforschung neuer Technologien in der Lehrerausbildung zum Thema, inwieweit sich das Training von Sportlehrern in der Handhabung eines Computerprogramms zur Analyse von eigenen, auf Video aufgezeichneten Lehrstunden auf die Veränderung und Verbesserung bestimmter Lehrerverhaltensweisen auswirkt, sein.

In einem Begleitschreiben der Universität wurde bestätigt, daß die geplanten Untersuchungen der Doktorandin im Arbeitsbereich Sportpädagogik/Sportdidaktik wissenschaftlich eingebunden sind und der mittelfristigen qualitativen Verbesserung der Referendarausbildung dienen sollen.

In meiner datenschutzrechtlichen Bewertung mußte ich darauf hinweisen, daß eine Übermittlung der benötigten Daten durch das MBJS nicht so ohne weiteres möglich sei. Nach § 28 Abs. 1 Bbg DSG darf eine Übermittlung personenbezogener Daten - auch zur Verarbeitung für wissenschaftliche Zwecke - nur nach Einwilligung der Betroffenen erfolgen. Ein Verzicht auf die Einwilligung wird nur zugelassen, wenn schutzwürdige Belange der Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden, oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Da die erste Alternative nur durch Einzelfeststellung bei den Betroffenen bestätigt werden könnte, die zweite Alternative zumindest in Frage stand und in einem gesonderten Verfahren hätte beurteilt werden müssen, mußte ich die Zulässigkeit einer direkten Übermittlung der gewünschten Daten durch das MBJS verneinen; dabei dürfe die Einholung der Einwilligung auch nicht deshalb unterbleiben, weil sie mit einem nicht unerheblichen Arbeits- oder Kostenaufwand verbunden wäre. Das MBJS wäre in jedem Fall gehalten, vor einer Übermittlung alle Betroffenen zuvor schriftlich um deren Einverständnis zu bitten.

Allerdings befand ich die für die Übermittlung der erbetenen Daten notwendige Erforderlichkeit schon deshalb als nicht gegeben, weil das Forschungsprojekt auch im Wege der "Adreßmittlung" hätte durchgeführt werden können. Bei der "Adreßmittlung" würde sich die Doktorandin der Adreßdaten zwar nur mittelbar, aber in datenschutzrechtlich zulässiger Weise, bedienen können. Ich habe dieses Verfahren empfohlen, bei dem das Ministerium ein Schreiben der Doktorandin, in dem diese ihre Bitte um Mitarbeit an ihrem Forschungsprojekt vortragen könnte, mit einem Erläuterungsschreiben direkt an den in Frage kommenden Personenkreis versendet. Mit der zustimmenden Beantwortung dieses Schreibens würden die Referendare ihre freiwillige Einwilligung im Sinne des Bbg DSG bekunden. Ich hoffe, daß dieses - datenschutzrechtlich einwandfreie und in den meisten Fällen zum gewünschten Ergebnis führende - Verfahren auch in anderen Bereichen häufiger erkannt und genutzt wird. Die Einholung der Einwilligung dürfte deshalb auch nicht unterbleiben.

6 Wissenschaft, Forschung und Kultur

6.1 Ungenügende Berücksichtigung von Schutzfristen für Sozialdaten

im Brandenburgischen Archivgesetz

Vor dem Hintergrund der anstehenden Behandlung des Brandenburgischen Archivgesetzes (BbgArchivG)[85] ist die AOK an mich herangetreten, um vorsorglich klarzustellen, daß nach Inkrafttreten des Gesetzes für Sozialdaten nicht die Schutzfristen gem. § 10 Abs. 3 BbgArchG, sondern die gem. § 5 Abs. 3 BArchG (20 Jahre länger) maßgeblich sind. Ohne eine Angleichung der Schutzfristen für Sozialdaten im BbgArchivG an § 304 SGB V[86] i.V.m. § 84 SGB X[87] würde für diese die Anbietungs- und Übergabepflicht nach diesem Gesetz entfallen.

Damit wurde zu Recht auf die konkurrierende Situation von Bundes- und Landesgesetzen bezüglich der Archivierung von Sozialdaten aufmerksam gemacht. Um eine wissenschaftliche Auswertung zu ermöglichen, wurde 1988 vom Bundesgesetzgeber § 10 Nr. 1 Buchst. b in das BArchG 1988[88] aufgenommen. Da der überwiegende Teil der Unterlagen mit Sozialdaten aber im Bereich der Länder anfällt, wurde gleichzeitig § 71 Abs. 1 SGB X durch Satz 2 ergänzt, der klarstellt, daß die Abgabe von Sozialdaten an Staatsarchive zwar keine gesetzliche Aufgabe gem. § 69 Abs. 1 Nr. 1 SGB X darstellt, aber ihre Offenbarung insoweit erlaubt ist, als Landesarchivgesetze landesunmittelbare oder kommunale Stellen - wie in § 4 Abs. 1 BbgArchiVG geschehen - zur Vorlage bzw. Abgabe auch von derartigen Unterlagen verpflichten. Diese Offenbarungsbefugnis ist allerdings an die Bedingung geknüpft, daß wegen der hohen Sensibilität von Sozialdaten die in § 5 BArchG aufgestellten Schutzfristen nicht unterschritten werden.

Obwohl § 12 Abs. 2 BbgArchiVG sicherlich auch für Sozialdaten in Anwendung zu bringen wäre, habe ich dennoch in einem Schreiben an den Ausschuß für Wissenschaft, Forschung und Kultur des Landtages Brandenburg angeregt, eine diesbezügliche ergänzende Klarstellung im Gesetzestext, beispielsweise in § 10 BbgArchiVG, vorzunehmen. Die dargelegte Problematik trifft im übrigen nicht nur für die AOK, sondern auch für andere landesunmittelbare Sozialversicherungsträger - z. B. die Landesversicherungsanstalt - zu. Zum BbgArchiVG wurde ansonsten bereits im ersten Tätigkeitsbericht unter Pkt. 9.3 Stellung genommen.

---

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

86 Sozialgesetzbuch (SGB), 1. Buch, vom 20. Dezember 1988, BGBl. I, S. 2477, zuletzt geänd. am 26. Februar 1993, BGBl. I, S. 278

87 Sozialgesetzbuch (SGB), 10. Buch (X), vom 18. August 1980, zuletzt geänd. am 24. Juni 1993, BGBl. I, S. 1038

88 vom 6. Januar 1988, BGBl. I, S. 62, zuletzt geänd. am 13. März 1992, BGBl. I, S. 506

6.2 Eingaben zu archivrechtlichen Fragen

6.2.1 Eigentumsgeschichte in der sowjetisch-besetzten Zone und DDR

Im Rahmen einer Studie über die Umsetzung von Rechtsvorschriften in der ehemaligen DDR (z. B. Aufbaugesetz und deren Umsetzung durch Rahmenrichtlinien, Richtlinie über staatlich verwaltete Grundstücke) hatte eine auf offene Vermögensfragen spezialisierte private Dokumentationsstelle bei einem Kreisarchiv um Einsicht in Akten der ehemaligen Fachabteilungen für Finanzen/Staatliches Eigentum bzw. Inneres (Wohnungswirtschaft) gebeten. Das angefragte Archiv hatte Bedenken gegen dieses Anliegen und bat mich um Stellungnahme dazu.

Bei den in Rede stehenden Unterlagen handelte es sich um Altdaten i.S.v. §§ 34 ff. Bbg DSG (s. unter 3.1). Dementsprechend wurden sie nicht in den Verwaltungsvollzug übernommen, galten aber gem. § 37 Abs. 1 Bbg DSG für die Verwaltung bis zur Verabschiedung eines Archivgesetzes als gesperrt. Ihre Weiterverarbeitung zu wissenschaftlichen Zwecken war zwar gem. § 37 Abs. 2 Bbg DSG grundsätzlich gestattet. Da aber die zur Einsicht gewünschten Unterlagen auch für gewerbliche/berufliche Zwecke genutzt werden sollten, lagen die Voraussetzungen dieser Regelung nicht vor. Die der Sache nach begehrte Weiterverarbeitung von Altdaten war deshalb als unzulässig zu beurteilen.

6.2.2 Adlige Familienarchive - Aktenbestände des Brandenburgischen Landeshauptarchivs?

Ein Vertreter einer bis 1945 in Brandenburg ansässigen adligen Familie war an mich mit der Bitte herangetreten, sicherzustellen, daß das Archiv seiner Familie bis zur Zurückführung in den Besitz der Familie einer datenschutzgerechten Aufsicht unterstellt wird. Nach seiner Auffassung war es lediglich gem. einer Verfügung der Provinzialverwaltung der Mark Brandenburg vom 27.10.1945 "zum Schutz vor Vandalisierung" der Obhut der Provinzialverwaltung unterstellt worden. Es würde jedoch seitdem ständig unbefugt genutzt. Für wissenschaftliche Arbeiten sei er bereit, Einsichtsgenehmigungen zu erteilen.

Die Besitzungen der Familie fallen unter die Bestimmungen der Bodenreform. Da dabei grundsätzlich kein Unterschied zwischen beweglichen und unbeweglichen Gütern gemacht wurde, war deshalb auch das Familienarchiv in staatliches Eigentum übergegangen, so daß die Verfügungsbefugnisse nunmehr beim Land Brandenburg liegen. Dem Petenten habe ich deshalb mitgeteilt, daß somit die Nutzung der von ihm beanspruchten Archivbestände auf der Grundlage der für die öffentlichen Archive in Brandenburg geltenden Regelungen erfolgt.

6.2.3 Nachweise für Fremdarbeiter vor 1945

Aufgrund einer Umfrage unter den Landesbeauftragten für den Datenschutz bin ich darauf gestoßen, daß an das Brandenburgische Landeshauptarchiv (BLHA) seit 1990/1991 ca. 4.000 Auskunftsersuchen über Nachweise von Versicherungs- und Beschäftigungszeiten vor 1945 entweder durch den Internationalen Suchdienst (ISD) von Arolsen oder durch die ehemaligen Zivil- und Zwangsarbeiter selbst bzw. deren Angehörige gestellt worden sind. Trotz der hohen sozialen Verantwortung, zu der sich das BLHA gegenüber dieser Personengruppe verpflichtet fühlt, konnten bisher von diesen Anfragen nur ca. 1 % beantwortet werden.

Der Eilbedürftigkeit der Angelegenheit steht hemmend die Aktenlage gegenüber. Da über den Personenkreis Meldekarteien - soweit sie überhaupt geführt wurden - nur noch in einzelnen Fällen vorhanden sind, stehen zur Beantwortung der Auskunftsersuchen im wesentlichen lediglich zufällig erhalten gebliebene "Ersatzüberlieferungen" (Transportausweise und -listen, Arbeitskarten, Belegschaftslisten früherer Industriebetriebe, Krankenscheine, Strafverfahren) zur Verfügung, die jedoch nur den Aufenthalt zu einem bestimmten Zeitpunkt belegen und außerdem in bisher überwiegend unerschlossenen Beständen vorliegen.

Aufgrund des SMAD-Befehls Nr. 163 vom 07.12.1945 wurden Anfang 1946 kreisweise (vermutlich in der gesamten sowjetisch-besetzten Zone) alle Zivil- und Zwangsarbeiter registriert und - soweit möglich - mit Name, Vorname, Geburtsdatum, Heimatadresse, Nationalität sowie Einsatzort und -zeit erfaßt. Diese Dokumentationen sind kurz nach ihrer Erstellung außer Landes gegangen und stehen deshalb im Land Brandenburg bis auf eine Ausnahme nicht mehr zur Verfügung. Ich habe den ISD auf die Existenz solcher Unterlagen aufmerksam gemacht und Nachforschungen über ihren jetzigen Verbleib angeregt.

6.3 Hochschulen

6.3.1 Auch Datenschutz will finanziert sein

Bereits im 1. Tätigkeitsbericht unter 5.5 war über erhebliche sicherheitstechnische Mängel in den Archiven der Universität Potsdam zu berichten, die ich 1992 bei Kontrollen festgestellt hatte. Durch Bemühungen der Universitätsleitung konnten bei der Behebung der bestehenden Mängel im Jahre 1993 wesentliche Fortschritte erzielt werden. Einige der gerade besonders gravierenden Mängel sind jedoch wegen fehlender finanzieller Mittel erst im Laufe des Jahres beseitigt worden. Ich habe Zweifel, ob es sich bei dieser Entscheidung der Universität im Hinblick auf den verfassungsrechtlichen Rang des Grundrechts auf informationelle Selbstbestimmung um einen sachgerechten Ausgleich der um die finanziellen Mittel konkurrierenden Interessen handelt. Aus datenschutzrechtlicher Sicht ist es jedenfalls grundsätzlich nicht hinnehmbar, daß die Beseitigung schwerwiegender Mängel der Datensicherheit über einen Zeitraum von mehr als zwei Jahren zurückgestellt und eine erhebliche Gefährdung des Grundrechts auf informationelle Selbstbestimmung so bewußt längerfristig in Kauf genommen wird. Eine (bloße) Planung von Bauvorhaben, mit denen auch datenschutzrelevante Sicherheitsmängel beseitigt werden sollen, macht zumindest erste Sofortmaßnahmen zur Gewährleistung der erforderlichen Datensicherheit nicht entbehrlich. Selbstverständlich müssen die Belange des Datenschutzes künftig auch bei der Erstellung der Haushaltspläne angemessener berücksichtigt werden, als dies bislang geschehen ist.

6.3.2 Übermittlung von Immatrikulationsbescheinigungen an die Kindergeldstellen der Arbeitsämter

Beim Studentensekretariat der Universität Potsdam häuften sich Anfragen von Kindergeldstellen, die zur Überprüfung des Kindergeldanspruchs der Eltern Angaben über immatrikulierte Studenten erbaten. Die Universität hielt die unmittelbare Übermittlung von Immatrikulationsbescheinigungen an die Kindergeldstellen für unzulässig und bat mich um eine datenschutzrechtliche Beurteilung des Übermittlungsbegehrens.

In meiner Stellungnahme habe ich die Rechtsauffassung der Universität bestätigt. Gem. § 21 Abs. 1 Satz 1 SGB X können sich die Kindergeldstellen zur Überprüfung des Kindergeldanspruchs derjenigen Beweismittel bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich halten. Dabei ist der Zusammenhang dieser Bestimmung mit § 21 Abs. 2 Satz 1 SGB X zu sehen. Nach dieser Vorschrift sollen die Beteiligten bei der Ermittlung des Sachverhalts mitwirken. Ferner haben die Kindergeldstellen der Ausübung ihres Ermessens den Grundsatz der unmittelbaren Datenerhebung beim Betroffenen mit seiner Kenntnis zugrunde zu legen (§ 12 Abs. 2 Satz 1 Bbg DSG). Daraus folgt, daß das unmittelbar an die Universität gerichtete Auskunftsverlangen der Kindergeldstellen ermessensfehlerhaft und insoweit rechtswidrig war. Zur sachgerechten Erfüllung der Aufgaben der Kindergeldstellen hätte es völlig genügt, die Anspruchsteller aufzufordern, die den Studenten zu diesem Zweck von der Universität ausgestellten Immatrikulationsbescheinigungen zum Nachweis ihrer Anspruchsberechtigung vorzulegen.

Da die Voraussetzungen einer Übermittlung gem. § 14 Abs. 1 Satz 1 Bbg DSG nicht gegeben

waren, habe ich der Universität empfohlen, eine Übermittlung von Immatrikulationsangaben ihrer Studenten an die Kindergeldstellen auch weiterhin mit Hinweis auf die dargelegte Rechtslage abzulehnen.

6.3.3 Diplomarbeiten-Datenbank

Die Fachhochschule Worms hat zum bundesweiten Nachweis von geplanten und tatsächlich gefertigten Diplomarbeiten eine Datenbank entwickelt, die über Bildschirmtext abrufbar ist und Suchmöglichkeiten nach Verfassern, betreuenden Professoren sowie Schlagwörtern zuläßt.

Für den Fall, daß sich die Hoch- und Fachhochschulen im Land Brandenburg daran beteiligen wollen, habe ich das Ministerium für Wissenschaft, Forschung und Kultur angeschrieben und darauf aufmerksam gemacht, daß in Ermangelung einer bereichsspezifischen Regelung eine Speicherung zum Zweck der Übermittlung im automatisierten Abrufverfahren gem. § 9 Abs. 7 Bbg DSG nur mit schriftlicher Einwilligung des Betroffenen zulässig ist. Dabei ist es zur Wirksamkeit der Einwilligung gem. § 4 Abs. 2 Satz 2 und 3 Bbg DSG erforderlich, den Betroffenen in geeigneter Form über ihre Bedeutung, insbesondere über den Verwendungszweck und die Empfänger der Daten sowie über den Zweck der Übermittlung und unter Darlegung etwaiger Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann. Für den Fall, daß bereits Diplomarbeiten ohne Einwilligung des Verfassers in die Datenbank eingegeben worden sein sollten, gebietet die Rechtslage, daß - soweit die Einwilligung nicht nachträglich eingeholt wird - die Namen der Diplomanden gelöscht werden und nur die Themen sowie die Angaben über die Betreuer gespeichert bleiben. Ich habe darauf hingewiesen, daß auch urheberrechtliche Bestimmungen die Einwilligung der Diplomanden unverzichtbar machen dürften.

Betreffs der Angaben über die betreuenden Hochschullehrer ist dagegen keine förmliche schriftliche Einwilligung erforderlich, wenn und soweit die Führung der Diplomarbeiten-Datenbank als Aufgabe der Hochschulen angesehen werden kann. In diesem Fall ist die Angabe der Betreuernamen in der Datenbank zur Erfüllung dieser Aufgabe erforderlich. Das Recht auf informationelle Selbstbestimmung der Bediensteten, die hier als Amtsträger mit Außenwirkung tätig werden, wäre insoweit zulässig eingeschränkt.

6.4 Datenschutz bei Forschungsvorhaben

Die sprichwörtliche wissenschaftliche Akribie bringt - je nach Gegenstand der Forschung - in vielen Bereichen eine besondere datenschutzrechtliche Relevanz des jeweiligen Forschungsvorhabens mit sich, da sie zu sensibelsten Datenverarbeitungen bis in die Intimsphäre des Bürgers hineinführen kann. Deshalb kann die für das Forschungsvorhaben erforderliche Verarbeitung personenbezogener Daten grundsätzlich nur mit Einwilligung des Betroffenen erfolgen (§ 28 Abs. 1 Bbg DSG).

§ 28 Abs. 2 Bbg DSG bemüht sich dagegen im Sinne einer praktischen Konkordanz widerstreitender Interessenlagen um einen Ausgleich des datenschutzrechtlichen Integritätsinteresses einerseits und des wissenschaftlichen Forschungsinteresses andererseits. Der Gesetzgeber hat sich nach Maßgabe dieser Bestimmung dafür ausgesprochen, in den Fällen, in denen entweder schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden (§ 28 Abs. 2 Satz 1 Buchst. a Bbg DSG) oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann (§ 28 Abs. 2 Satz 1 Buchst. b Bbg DSG), die für das Forschungsvorhaben erforderlichen Datenverarbeitungen durch öffentliche Stellen auch ohne Einwilligung der Betroffenen zuzulassen. Dies ist auch aus datenschutzrechtlicher Sicht grundsätzlich nicht zu beanstanden.

Obwohl diese sog. "Wissenschaftsklausel" des § 28 Abs. 2 Bbg DSG scheinbar eine Erleichterung des Forschungsvorhabens darstellt, birgt sie zugleich besondere datenschutzrechtliche Gefahren, denn sie macht die Zulässigkeit der Datenverarbeitung im Ergebnis davon abhängig, daß jeweils besonders sorgfältig die Verhältnismäßigkeit des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung "am Betroffenen vorbei" geprüft und begründet wird.

Insoweit wirkt es sich sehr nachteilig für den Datenschutz aus, daß die Datenverarbeitung insbesondere in den Fällen des § 28 Abs. 2 Satz 1 Buchst. b Bbg DSG nicht - wie dies in anderen Datenschutzgesetzen vorgesehen ist - der vorherigen Zustimmung der zuständigen obersten Landesbehörde bedarf, sondern die Prüfung des überwiegenden öffentlichen Interesses allein der das Forschungsvorhaben durchführenden Stelle überlassen bleibt. Eine objektive Betrachtungsweise kann dabei schwerlich erwartet werden. Die Regelung in § 28 Abs. 2 Bbg DSG enthält deshalb keine den verfassungsrechtlichen Anforderungen[89] genügende verfahrensrechtliche Vorkehrung zum Schutz des Rechts der Betroffenen auf informationelle Selbstbestimmung. Ich habe daher gegenüber dem Innenausschuß bereits eine Neufassung des § 28 Bbg DSG in Anlehnung an die entsprechende Regelung im Schleswig-Holsteinischen Datenschutzgesetz empfohlen.

Die Anwendbarkeit der "Wissenschaftsklausel" (§ 28 Abs. 2 Bbg DSG) unterliegt insbesondere den folgenden Grundvoraussetzungen:

- Unterrichtung des Landesbeauftragten für den Datenschutz gem. § 28 Abs. 2 Satz 4 Bbg DSG,

- Erläuterungen zu den Auswertungsmodalitäten, der Form der Datenspeicherung (Beschreibung der Datenträger), Hinweise auf die teilweise oder gänzliche Vernichtung der Primärdaten mit verbindlichen Löschungszusagen,

- Bestätigung des Verbots, Angaben mit Personenbezug ohne Zustimmung der Betroffenen an Dritte zu übermitteln,

- Bestätigung, daß für die Phase des Personenbezugs am Ort der Speicherung eine Dateienregistermeldung nach dem jeweils geltenden Datenschutzgesetz an den zuständigen Landesbeauftragten für den Datenschutz erfolgt,

- Frühzeitige Anonymisierung, möglichst schon bei der Erfassung der Primärdaten,

- Aufklärende Darstellung des Untersuchungsgegenstands und des Auswertungsverfahrens sowie eindeutige Festlegung des Forschungszwecks,

- Hinweis auf die einschlägigen Datenschutzbestimmungen des § 28 Bbg DSG,

- ggf. besonderer Hinweis auf die Freiwilligkeit bestimmter Angaben,

- als vertrauensbildende Maßnahme: Hinweis auf die Kontrollbefugnis des Landesbeauftragten für den Datenschutz zumindest hinsichtlich des Erhebungsverfahrens,

- bei Auswertung an anderem Ort (z. B. Befragung der Humboldt-Universität zu Berlin in Schulen des Landes Brandenburg): auch Hinweis auf zusätzliche Kontrollbefugnis des dortigen Datenschutzbeauftragten.

---

89 BVerfGE 65, 1 (46)

Diese Voraussetzungen gelten - bis auf die zuerst genannte - grundsätzlich auch bei Datenverarbeitungen nach § 28 Abs. 1 Bbg DSG. Dabei ist jedoch zusätzlich insbesondere zu beachten, daß die Einwilligung den Anforderungen der §§ 4 Abs. 2, 12 Abs. 3 Bbg DSG entsprechen muß.

Ich gehe davon aus, daß regelmäßig ein angemessener Interessenausgleich zwischen den Persönlichkeitsrechten zu Befragender einerseits und dem öffentlichen Forschungsinteresse andererseits gefunden werden kann, wenn die Betroffenen jeweils detailliert über die vorgenannten Bearbeitungsschritte und Sachzusammenhänge aufgeklärt werden.

7 Arbeit, Soziales, Gesundheit und Frauen

7.1 Landesgleichstellungsgesetz

Stellung zu nehmen hatte ich auch zu dem Entwurf eines Gesetzes zur Gleichstellung von Frauen und Männern im öffentlichen Dienst im Land Brandenburg (Landesgleichstellungsgesetz - LGG -). Seiner Zielsetzung nach soll das LGG dazu dienen, dem Grundrecht des Art. 3 Abs. 2 Grundgesetz auf Gleichberechtigung von Männern und Frauen in der Verfassungswirklichkeit verstärkt Geltung zu verschaffen. Die Institutionalisierung einer Gleichstellungsbeauftragten ist als Mittel zu diesem Zweck zu begreifen, dessen Wirksamkeit nicht zuletzt von den Kompetenzen abhängen wird, die der Gesetzgeber der Gleichstellungsbeauftragten zugesteht.

Die vorgesehene Beteiligung der Gleichstellungsbeauftragten an Personalentscheidungen macht deutlich, daß die Einrichtung einer Gleichstellungsbeauftragten grundsätzlich in einem gewissen Spannungsverhältnis zum Datenschutz steht. Dessen besonderes und ganz elementares Anliegen ist es, den Kreis der Personen, die Personaldaten verarbeiten dürfen, möglichst begrenzt zu halten. Mit der Beteiligung der Gleichstellungsbeauftragten an Personalentscheidungen (z. B. bei Stellenbesetzungen) wird dieser Personenkreis jedoch gerade erweitert werden. Die Verarbeitung personenbezogener Daten durch die Gleichstellungsbeauftragte wird dabei um so umfangreicher sein, je weitgehender die Kompetenzen sind, die ihr vom Gesetzgeber zugestanden werden.

Wird der Zusammenhang anerkannt, der zwischen dem Umfang der Kompetenzen und der Wirksamkeit der Gleichstellungsbeauftragten zum Schutz des Grundrechts auf Gleichberechtigung von Männern und Frauen besteht, so ergibt sich, daß der Schutz dieses Grundrechts zwangsläufig mit Beschränkungen des Grundrechts auf informationelle Selbstbestimmung verbunden sein wird. Das Grundrecht auf informationelle Selbstbestimmung wird jedoch nicht schrankenlos gewährleistet und muß insbesondere mit anderen Grundrechtspositionen verfassungskonform in Ausgleich gebracht werden. Eine solche ist gem. Art. 3 Abs. 2 Grundgesetz auch die Gleichberechtigung von Männern und Frauen.

Hält der Gesetzgeber es für erforderlich, diesem Grundrecht durch entsprechende Regelungen im LGG in der Verfassungswirklichkeit verstärkt Geltung zu schaffen, so ist er dabei in der Wahl seiner Mittel grundsätzlich frei, soweit er mit seinen Regelungen die gebotene praktische Konkordanz des Grundrechts der Gleichberechtigung mit dem Grundrecht auf informationelle Selbstbestimmung wahrt. Aus datenschutzrechtlicher Sicht würde ich diese praktische Konkordanz auch bei umfassenden Rechten einer Gleichstellungsbeauftragten zur Mitwirkung an Personalentscheidungen grundsätzlich nicht beeinträchtigt sehen. Davon ausgehend habe ich in meiner Stellungnahme gegenüber dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen betont, daß jedoch jede gesetzliche Regelung dem Gebot der Normenklarheit entsprechen und die Rechtsstellung, Aufgaben und Befugnisse der Gleichstellungsbeauftragten klar und eindeutig bestimmen muß. Diesen

verfassungsrechtlichen Anforderungen entspricht der mir vorgelegte Gesetzentwurf nicht.

Zu beanstanden ist zunächst, daß wichtige Kompetenzen der Gleichstellungsbeauftragten bereits aus ihrer rechtlichen Stellung als Teil der Dienststelle hergeleitet werden sollen. Dies kommt schon deshalb nicht in Betracht, weil die Gleichstellungsbeauftragte lediglich eine sektorale Aufgabe wahrzunehmen hätte und den Dienstherrn bzw. Arbeitgeber keinesfalls in der Gesamtheit seiner Befugnisse repräsentieren würde. Sie kann daher mit diesem auch nicht im Sinne einer Teilidentität gleichgesetzt werden. Dies macht es erforderlich, daß die Kompetenzen der Gleichstellungsbeauftragten als eigene im Gesetz klar und eindeutig bestimmt werden. Dazu wird auch klarzustellen sein, daß die Gleichstellungsbeauftragte unabhängig von ihrer rechtlichen Stellung im übrigen eine eigene datenverarbeitende Stelle ist und als solche der uneingeschränkten datenschutzrechtlichen Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegt. Dabei sollte vorgesehen werden, daß sie, sofern Kontroll- und Weisungsbefugnisse der Dienststellenleitung nicht bestehen, selbst Adressatin etwaiger Beanstandungen ist. Ferner muß eine Bestimmung in das Gesetz aufgenommen werden, die, entsprechend der gesetzlichen Vorgabe in den §§ 23 Abs. 2 Satz 3, 41 Abs. 2 Bbg DSG, bereichsspezifisch die Datenverarbeitung regelt, die durch Gleichstellungsbeauftragte in Ausübung ihrer Befugnisse erfolgen soll.

Zur Regelung der Befugnisse der Gleichstellungsbeauftragten habe ich unter Berücksichtigung der Erfahrungen aus anderen Bundesländern nachdrücklich empfohlen, normenklar zu bestimmen, ob

- sich das Einsichtsrecht der Gleichstellungsbeauftragten nur auf Akten im engeren Sinne bezieht oder auch bezüglich anderer Unterlagen bestehen soll,

- es auch die Einsicht in Bewerbungsunterlagen, insbesondere die oft einzig interessante Einsicht in beigezogene Personalakten, umfaßt,

- die Beteiligung am gesamten Auswahlverfahren bei Lehrern auch die Teilnahme an den meist entscheidenden Lehrproben umfaßt,

- der vorgesehenen Informationspflicht der Dienststellenleitung auch ein entsprechendes Auskunftsrecht der Gleichstellungsbeauftragten korrespondiert,

- ein solches Auskunftsrecht inhaltlich qualifiziert oder nur formal besteht,

- die der Gleichstellungsbeauftragten zugestandenen Rechte jeweils von einem Einverständnis der Betroffenen abhängig sind oder insoweit ein Widerspruchsvorbehalt besteht sowie

- die Rechte der Gleichstellungsbeauftragten, insbesondere im Bewerbungsverfahren, nur bestehen sollen, wenn sich zugleich Männer und Frauen bewerben, d. h. nur bei einer konkreten Konkurrenzsituation, oder auch dann, wenn nur männliche oder nur weibliche Bewerber(-innen) zur Auswahl stehen.

Ich habe darauf hingewiesen, daß ein Einsichtsrecht der Gleichstellungsbeauftragten in Personalakten zwar insgesamt ausgeschlossen werden kann, nicht jedoch von der Zustimmung der Betroffenen abhängig gemacht werden darf. Bei einer Beteiligung der Gleichstellungsbeauftragten, beispielsweise bei der Personalauswahl, wäre die umfangreiche Verarbeitung personenbezogener Daten nur derjenigen Bewerber(-innen), die einer Einsichtnahme in ihre Personalakte zugestimmt haben, zur Erfüllung der Aufgaben der Gleichstellungsbeauftragten bereits nicht geeignet, da sie nur Auskunft über die Qualifikation dieser Bewerber(-innen) geben würde, nicht jedoch über die ihrer Konkurrenten und Konkurrentinnen. Auf die Qualität der Mitwirkung einer Gleichstellungsbeauftragten an Personalauswahlentscheidungen würde sich deshalb ihre Kenntnis der maßgebenden

Personalaktendaten nur eines Teils der Bewerber(-innen) nicht auswirken können. Die Ungleichbehandlung der Bewerber(-innen) wäre somit auch unter datenschutzrechtlichen Gesichtspunkten nicht gerechtfertigt. Bei einer Überarbeitung des Gesetzentwurfs ist aufgrund dieses Einwands zwischenzeitlich klargestellt worden, daß das vorgesehene Einsichtsrecht der Gleichstellungsbeauftragten in die entscheidungsrelevanten Personalaktendaten unabhängig von einer Zustimmung der Betroffenen bestehen soll.

In den übrigen Punkten hat meine Stellungnahme bislang keine Berücksichtigung gefunden. Eine von mir mehrfach erbetene Stellungnahme des federführenden Ministeriums ist bisher nicht erfolgt.

7.2 Gesundheit

7.2.1 Patientenunterlagen aus ehemaligen Einrichtungen - letzte Hindernisse genommen

Über einen Entwurf für einen gemeinsamen Runderlaß des Ministeriums für Arbeit, Gesundheit, Soziales und Frauen, des Ministeriums für Wissenschaft, Forschung und Kultur und des Ministeriums des Innern zu "Hinweisen zur Meldung, Aufbewahrung und Nutzung von Patientenunterlagen, Zentralkarteien, Zentralregistern und Zentraldateien mit patientenbezogenem (medizinischem) Inhalt aus ehemaligen Gesundheitseinrichtungen der DDR" wurde bereits im 1. Tätigkeitsbericht unter 5.4 berichtet. Die Mitzeichnung wurde jedoch ca. ein Jahr lang durch das Ministerium des Innern wegen der angespannten Finanzlage der Kommunen verweigert. Das Ministerium war dazu erst nach Streichung einer Passage bereit, die die Kreise und kreisfreien Städte verpflichtete, die erforderliche personelle, infrastrukturelle und materielle Ausstattung zur Verfügung zu stellen. Inzwischen ist der Runderlaß im wesentlichen unverändert Ende 1993 in Kraft getreten.

Das herauszögernde Verhalten hatte ich bedauert und dem Ministerium des Innern gegenüber zur Eile gemahnt, weil es sich bei der Sicherstellung und weiteren Nutzung von Patientendaten eindeutig um eine Pflichtaufgabe nach Art. 21 Abs. 2 Einigungsvertrag handelte, der sich die Kommunen mehrheitlich mit großem Engagement als einer Aufgabe der Selbstverwaltung seit 1990/1991 angenommen hatten. Jedoch bestand große Unsicherheit darüber, wie die weitere Nutzung zu handhaben war, zumal auch das Schreiben des Ministeriums für Wissenschaft, Forschung und Kultur vom 29. Juli 1992 an alle Landräte bzw. Oberbürgermeister über "Regelungen einzelner archivrechtlicher und archivfachlicher Fragen" den damit beauftragten Personenkreis nicht bekannt war.

Aufgrund mehrerer Eingaben bzw. Hinweise auch aus der Presse bin ich mehrmals dem Verbleib von Patientenakten nachgegangen. Dabei habe ich zugleich die Gelegenheit genutzt, die Lagerung und Nutzung dieser Akten vor Ort zu kontrollieren. Hierbei waren Mängel unterschiedlicher Art und Schwere festzustellen. Sie betrafen zum einen sicherheitstechnische Aspekte der Aufbewahrung der Patientenakten und zum anderen die Dokumentation der weiteren Nutzung.

Nach wie vor greifen behandelnde Ärzte, aber auch die Berufsgenossenschaften für Versicherungsangelegenheiten gem. § 1543d Abs. 1 Reichsversicherungsordnung (RVO)[90] im großen Umfang auf diese Akten zurück. Die Dokumentation darüber geschieht nicht immer sorgfältig. Ich habe feststellen müssen, daß auch die für die Abforderung der Patientenakte

---

90 vom 19. Juli 1911, RGBl., S. 509, in der Neubekanntmachung vom 15. Dezember 1924, RGBl. I, S. 779, zuletzt geänd. am 21. Dezember 1992, BGBl. I, S. 2266

durch den Arzt erforderliche schriftliche Einwilligungserklärung des Patienten nicht in jedem Fall vorlag. Für die Einwilligungserklärungen verwenden die Ärzte alle möglichen für andere Zwecke gedachten Formulare. Insoweit wurde die von mir geforderte Beseitigung der Mängel zugesagt.

In einem Extremfall diente eine für jedermann zugängliche Bodenkammer zur Unterbringung der Suchkartei der ehemaligen poliklinischen Abteilung für Lungenkrankheiten und TBC, deren Einzelkarten zum Teil letzte Befunde aus dem Jahre 1991 beigefügt waren. Ein Teil dieser Unterlagen war auf dem Boden verstreut und durch Tierkot beschmutzt. Diesen unhaltbaren Zustand habe ich gem. § 26 Abs. 1 Nr. 1 Bbg DSG förmlich beanstandet.

7.2.2 Datenschutz im öffentlichen Gesundheitswesen

7.2.2.1 Gesundheitsdienstgesetz

Mit diesem Gesetz soll die durch die letzte Volkskammer verabschiedete und noch gültige Verordnung über den öffentlichen Gesundheitsdienst und die Aufgaben der Gesundheitsämter in den Landkreisen und kreisfreien Städten[91] abgelöst werden. Der mir zunächst vorgelegte Entwurf einer Kabinettsvorlage vom 26.03.1992 enthielt als bereichsspezifische Regelung der Datenverarbeitung lediglich die Bestimmung, daß bei krankenpflegerischen Tätigkeiten im privat-wirtschaftlichen Bereich personenbezogene Daten nur mit Einwilligung der Betroffenen und hier in dem Umfang erhoben und sonst verarbeitet werden dürfen, als dies zur Aufgabenerfüllung erforderlich ist. Für den primären Bereich des öffentlichen Gesundheitsdienstes, der ständig im Rahmen der Gesundheitsvorsorge und Gesundheitsförderung mit äußerst sensiblen personenbezogenen Daten arbeitet, war dagegen keine bereichsspezifische Datenschutzregelung aufgenommen worden. Das Ministerium für Arbeit, Gesundheit, Soziales und Frauen (MAGSF) vertrat vielmehr die Meinung, daß das Brandenburgische Datenschutzgesetz selbst eine ausreichende Grundlage für die Datenverarbeitung im öffentlichen Gesundheitsdienst darstelle.

Daher forderte ich das MAGSF auf, gemäß den Bestimmungen des Brandenburgischen Datenschutzgesetzes eine bereichsspezifische Regelung der Datenverarbeitung in den Entwurf aufzunehmen und habe dazu Vorschläge zur Zweckbindung, Geheimhaltungspflicht, zu Aufbewahrungsfristen bei Aufzeichnungen über amts-, gerichts- und vertrauensärztlichen Tätigkeiten sowie zur Zusammenarbeit mit anderen Behörden unterbreitet. Meine Anregungen sind in den Gesetzentwurf zum Brandenburgischen Gesundheitsdienstgesetz (BbgGDG) weitestgehend übernommen worden.

Er enthält nunmehr einen eigenen aus zwei Paragraphen bestehenden Abschnitt mit der Überschrift "Datenschutz". U. a. findet sich dort die Regelung, daß das Erheben, Speichern oder Übermitteln personenbezogener Daten durch die Einrichtungen des öffentlichen Gesundheitsdienstes nur erlaubt ist, soweit ihre Kenntnis zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. Für das "Nutzen personenbezogener Daten" wird auf die Bestimmungen des Brandenburgischen Datenschutzgesetzes verwiesen. Ferner ist bestimmt, daß die Gesundheitsämter im Rahmen der Gesundheitsberichterstattung berechtigt sind, von anderen im Gesundheitsbereich tätigen Behörden sowie u. a. auch niedergelassenen Ärzten anonymisierte Daten zu erhalten. Desweiteren ist das Verbot der unbefugten Offenbarung personenbezogener Daten durch im öffentlichen Gesundheitsdienst tätige Personen - zu denen auch Unternehmen zählen, die krankenpflegerische Tätigkeiten anbieten - ausdrücklich normiert worden. Danach ist eine Verwertung oder sonstige Offenbarung der Gesundheitsdaten nur zulässig, soweit die betroffene Person eingewilligt hat. Die

---

91 vom 8. August 1990, GBl. der DDR I, S. 1068

Aufbewahrungsfrist bei Aufzeichnungen des öffentlichen Gesundheitsdienstes über amts-, gerichts- und vertrauensärztliche Tätigkeiten beträgt in der Regel 10 Jahre. Zugelassen wurde auch eine Übermittlung personenbezogener Daten durch Dienststellen des öffentlichen Gesundheitsdienstes an andere "Verwaltungsbehörden" in Fällen von Verstößen "gegen gesetzliche Vorschriften".

In einigen Punkten wird der Entwurf jedoch nicht meinen Forderungen gerecht. Im einzelnen betrifft dies

- die Aufnahme der unbefugten Offenbarung personenbezogener Daten in den Ordnungswidrigkeitskatalog in Anlehnung an die Regeln zu § 39 Abs. 1 Bbg DSG,

- die Aufnahme einer Verpflichtung, den Posteingang bei unteren Gesundheitsbehörden durch besondere Ausführungsvorschriften zu regeln. Dadurch soll dem Verwaltungspersonal in der Praxis eine verbindliche Anweisung an die Hand gegeben werden, wie mit Post, die das Vertrauensverhältnis von Arzt und Patient betrifft, zu verfahren ist. So sollten z.B. an den Landkreis adressierte Briefe für das Gesundheitsamt letzterem ohne Öffnung weitergeleitet werden.

- eine Präzisierung der Herkunft der Daten, die zur Erfüllung der Aufgaben zum Schutz vor Umwelteinflüssen nach § 5 Abs. 2 des Entwurfs, erforderlich sind. Es sollte zumindestens in der Einzelbegründung zum Bbg GDG darauf hingewiesen werden, daß der Datenaustausch nur innerhalb des jeweiligen Landkreises stattfinden darf.

- die Übermittlung in Fällen von Verstößen gegen gesetzliche Vorschriften. Sie sollte folgende Präzisierung erfahren: ..."in Fällen von Verstößen gegen gesetzliche Vorschriften, die durch die Wahrnehmung der Aufgaben im Rahmen des öffentlichen Gesundheitsdienstes festgestellt werden".

- die Verweisungstechnik auf das Brandenburgische Datenschutzgesetz. Damit ist eine unnötige Erschwerung der Lesbarkeit verbunden, wodurch das Gesetz die verfassungsrechtliche gebotene Normenklarheit verliert.

- die Einzelbegründung. Sie beschränkt sich - völlig unzureichend - jeweils für jeden Paragraphen auf lediglich einen Satz.

7.2.2.2 Totenscheine - nur gut zwischengelagert

Die Totenscheine aus der ehemaligen DDR waren bis 1990 im Archiv der staatlichen Zentralverwaltung für Statistik aufbewahrt und danach vom Bundesamt für Statistik übernommen worden, dessen Außenstelle am Alexanderplatz in Berlin gegen Ende des Jahres 1993 aufgelöst wurde. Die erhaltengebliebenen Bestände umfassen alle in der ehemaligen DDR Verstorbenen einschließlich der Totenscheine unbekannter Toter sowie Toter ausländischer Herkunft für den Zeitraum vom 01.01.1969 bis zum 31.08.1990. Sie sind zwar bereits für die Todesursachenstatistik ausgewertet worden; nach wie vor werden jedoch Anfragen durch die rentenberechtigten Erben über Versorgungsämter, Berufsgenossenschaften, Staatsanwaltschaften oder Notare und Rechtsanwälten vorrangig wegen

- Impfschäden mit tödlichen Ausgang,
- Arbeitsunfällen mit tödlichem Ausgang,
- Kriegsschäden und
- Rehabilitationsansprüchen von Häftlingen

gestellt.

Für die zur Beantwortung dieser Anfragen erforderliche Übernahme der Archivbestände durch das Land Brandenburg mußte eine Lösung gefunden werden, die diesen "Anfragen" Rechnung trägt. Nachdem zunächst eine kreisweise, dezentrale Unterbringung in den Gesundheitsämtern im Gespräch war, wurden die Totenscheine Ende 1993 vom Brandenburgischen Landeshauptarchiv lediglich zur Aufbewahrung übernommen. Ich habe dieser Vorgehensweise - vorbehaltlich einer Klärung der noch ungelösten Fragen der Auskunftserteilung und der weiteren Nutzung - zugestimmt. Dazu liegen mir noch keine abschließenden Vorstellungen des MAGSF vor. Bezüglich einer Aufbewahrungsfrist teilt das Ministerium meine Auffassung, daß diese maximal 10 Jahre betragen sollte.

Ich habe das Ministerium darauf aufmerksam gemacht, daß die übernommenen Bestände spezielle Lücken aufweisen, da zu DDR-Zeiten Totenscheine von Häftlingen und "Grenzverletzern" gesondert im Standesamt 2 von Berlin abgewickelt und im ehemaligen NVA-Lazarett aufbewahrt wurden. Die unverzügliche Sicherstellung dieses Datenmaterials durch Landesbehörden halte ich für unbedingt geboten. Meine entsprechende Empfehlung wird zur Zeit vom Ministerium geprüft.

7.2.2.3 Übermittlung von Geburtsfällen an die Gesundheitsämter durch die Standesämter

Anläßlich der Absicht des Ministeriums des Innern, die §§ 99 und 278 der Dienstanweisung für Standesbeamte und ihre Aufsichtsbehörden[92] über die Mitteilungspflicht des Standesamtes über Geburtsfälle an die Gesundheitsämter aufzuheben, bat mich das Ministerium für Arbeit, Soziales, Gesundheit und Frauen um eine Prüfung, "ob die bislang von den Standesämtern gegebene Information weiterhin für notwendig bzw. erforderlich gehalten werde".

Im Hinblick darauf, daß insbesondere durch ein Gefühl der Überforderung bei den Eltern infolge der durch die Geburt veränderten Umstände das Wohl der Neugeborenen schwer beeinträchtigt werden kann, halte ich das Angebot einer fachkundigen Beratung der Eltern zwar für durchaus sinnvoll. Um solche Besuche überhaupt ermöglichen zu können, müßten die Gesundheitsämter in der Tat rechtzeitig über die Geburtsfälle in Kenntnis gesetzt werden. Es war allerdings festzustellen, daß eine Übermittlung gemäß § 4 Abs. 1 Bbg DSG nur mit Einwilligung der Eltern zulässig ist, da es an einer bereichsspezifischen Übermittlungsbefugnis fehlt und die Voraussetzungen von § 14 Abs. 1 i.V.m. § 13 Abs. 1 und 2 Bbg DSG nicht vorliegen. Insbesondere setzt die Wahrnehmung der den Gesundheitsämtern zugewiesenen Aufgaben die in Rede stehende Datenverarbeitung nicht zwingend voraus.

Gem. § 70 Nr. 11 Personenstandsgesetz[93] sind Mitteilungspflichten der Standesbeamten entweder in Rechtsverordnungen oder in Verwaltungsvorschriften zu regeln. Bisher ist hierzu lediglich die Dienstanweisung für Standesbeamte und ihrer Aufsichtsbehörden vom 23.11.1987 in den §§ 98, 99, 277 und 278 erlassen worden. Danach haben Standesbeamte Meldungen über beurkundete Geburten einzeln oder in Form von Listen an die Meldestellen bzw. Gesundheitsämter vorzunehmen. Die Dienstanweisung entspricht jedoch mangels Rechtsnormqualität nicht den Anforderungen des § 4 Abs. 1 Buchst. a Bbg DSG.

Es besteht lediglich für die Gesundheitsämter nach § 28 Abs. 1 und Abs. 2

---

92 vom 23. November 1987 (Beilage zum BAnz. Nr. 227a), i.d.F.

93 vom 12. Juli 1993 (BAnz. Nr. 129, S. 6381)

vom 8. August 1957, BGBl. I, S. 1125, i.d.F. vom 31. August 1990 II, S. 889, 914

Brandenburgisches Meldegesetz[94] die Möglichkeit, die Geburtsdaten von den örtlichen Meldebehörden zu erhalten. Ein großer Nachteil dieser Übermittlung ist, daß damit für eine möglichst frühzeitige Betreuung eine Zeitverzögerung verbunden ist. Zur Lösung des Problems rege ich deshalb eine Ergänzung des Personenstandsgesetzes oder die Schaffung einer Übermittlungsbefugnis durch den Landesgesetzgeber an. Die Übermittlungsbefugnis sollte jedoch die Löschung der Daten ca. 6 - 10 Wochen nach der Geburt vorsehen, da davon auszugehen ist, daß nur sehr wenige Familien von dem Leistungsangebot der Gesundheitsämter Gebrauch machen werden.

7.2.2.4 Einschulungsuntersuchungen

Zur Einschulungsuntersuchung 1994 hatte das Ministerium für Arbeit, Soziales, Gesundheit und Frauen in Zusammenarbeit mit dem Landesgesundheitsamt einen umfangreichen Fragebogen an die Eltern versandt, der sich in zwei Teile untergliederte. Der erste Teil enthielt die unmittelbar auf die gesundheitliche Situation des Kindes bezogenen Fragen. Bereits hier wiesen einige dieser insgesamt sehr eingehenden und speziellen Fragen einen deutlichen Bezug zu Allergien auf. Im zweiten Fragenteil wurde mit nunmehr ganz überwiegendem, wenn nicht ausschließlichem Allergiebezug das soziale Umfeld des Kindes erfragt. Gefragt wurde nach der Lage der Wohnung, Schimmelbildung an den Zimmerdecken, nach den Heizquellen, nach Haustieren, nach dem Zigarettenkonsum, nach Familienstand, Berufstätigkeit, Schul- und Fachausbildung, Berufstätigkeit und Alter der Eltern. In einem Anschreiben wurde den Eltern unter Hinweis auf die gesetzlichen Grundlagen[95] erläutert, die entsprechenden Angaben seien für eine eingehende ärztliche Untersuchung zur Feststellung der Schulreife der Kinder erforderlich. Die Eltern wurden gebeten, den Erhebungsbogen ausgefüllt zur Untersuchung mitzubringen. Der Bogen sollte mit Orts- und Datumsangabe von den Eltern unterschrieben werden.

Demgegenüber war aus datenschutzrechtlicher Sicht deutlich zu machen, daß es sich bei der Einschulungsuntersuchung nicht um eine umfassende, dem Wohl des Kindes verpflichtete Untersuchung handelt, aus der letztlich das Recht, wenn nicht gar die Pflicht zu einer total erfassenden Datenerhebung abgeleitet werden könnte, die nicht mehr verbindlich zu begrenzen wäre, da kaum ein personenbezogenes Datum denkbar ist, von dem sich nicht behaupten ließe, daß es für das Wohl des Kindes relevante Aussagen über seinen gesundheitlichen Zustand ermöglichen könnte. Vielmehr ist die Einschulungsuntersuchung eine staatliche Pflichtuntersuchung, mit der ausschließlich die Schulreife des Kindes festgestellt werden soll, an die der Gesetzgeber rechtlich das Entstehen der dem Bürger auferlegten Schulpflicht geknüpft hat.

Die Schuluntersuchung ist damit nicht mehr und nicht weniger als eine von Amts wegen durchzuführende Prüfung von Anspruchs- und Verpflichtungsvorausetzungen. Die Verfolgung weiterer Zwecke wird von den schulgesetzlichen Grundlagen grundsätzlich nicht gedeckt. Solche anderen (z. B. gesundheitspolitischen Zwecke) können nur im Rahmen des gesetzlichen Angebots des öffentlichen Gesundheitsdienstes an den Bürger verfolgt werden. Das setzt jedoch voraus, daß das Leistungsangebot des öffentlichen Gesundheitsdienstes von dem Bürger freiwillig nachgefragt wird. Bei den Schulpflichtuntersuchungen ist dies gerade nicht der Fall.

Einem Teil der Eltern sollte "ergänzend zur Einschulungsuntersuchung" ein weiterer Elternfragebogen "Gesundheit und Lebensbedingungen" ausgehändigt werden, in dem insgesamt 59 Fragen zum Gesundheitszustand und den sozialen Lebensbedingungen des

---

94

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

Erstes Schulreformgesetz für das Land Brandenburg vom 1. Juli 1992, GVBl. S. 258

Kindes gestellt wurden. Obwohl das Anschreiben den Eltern eine anonymisierte Auswertung des Fragebogens zusicherte, war vorgesehen, daß der Fragebogen von ihnen unterschrieben wurde. Ferner wurde den Eltern mitgeteilt, daß die sogenannten Identifikationsdaten des Kindes (Name, Anschrift usw.) nicht erfaßt würden, obwohl der Erhebungsbogen vor der (anonymisierten) Übermittlung an das Landesgesundheitsamt von den Schulärzten mit dem Fragebogen der Einschulungsuntersuchung zusammengeführt werden sollte, beim Schularzt die Datenerhebung also sehr wohl personenbezogen erfolgte. Auch einen ausdrücklichen Hinweis auf die Freiwilligkeit der Teilnahme an der Studie, wie er gem. §§ 4 Abs.2, 12 Abs. 3 Bbg DSG vorgeschrieben ist, enthielt der Fragebogen nicht. Als Zweck der Studie wurde angegeben, sie sei Teil der Landesgesundheitsberichterstattung und diene dazu, Planungen im gesundheitlichen Bereich eine bessere Grundlage zu verschaffen.

Datenschutzrechtlich war dieser Sachverhalt in mehrfacher Hinsicht zu beanstanden: Zunächst war es irreführend, eine eindeutig der Allergieforschung dienende und in ihrer Konzeption so begründete Studie als allgemeine Erhebung zu Gesundheits- und Lebensbedingungen der schulpflichtigen Kinder und Ergänzung der Einschulungsuntersuchung zu bezeichnen. Richtigerweise hätte deutlich gemacht werden müssen, daß ein inhaltlicher oder gar rechtlicher Zusammenhang zwischen Einschulungsuntersuchung und Allergievorsorgeprojekt nicht bestand und daß vielmehr nur der Anlaß der Einschulungsuntersuchung dazu genutzt werden sollte, die Eltern der Kinder zu erreichen. Dabei hätte die Freiwilligkeit der Teilnahme an der Studie in besonderer Weise herausgestellt und die Maßnahmen zur Wahrung der Anonymität der Teilnehmer sehr viel sorgfältiger ausgearbeitet werden müssen.

Ferner war die personenbezogene Datenerhebung zum Zweck eines Allergievorsorgeprojektes nicht von den bestehenden Rechtsgrundlagen gedeckt und wird es nach Maßgabe des Entwurfs für ein brandenburgisches Gesundheitsdienstgesetz auch in Zukunft nicht sein. So legitimiert insbesondere die Pflichtaufgabe der Gesundheitsberichterstattung und Gesundheitsplanung den öffentlichen Gesundheitsdienst nicht zur ausschließlich dazu erfolgenden Erhebung personenbezogener Daten. Vielmehr werden die Gesundheitsämter dazu in § 28 Abs. 3 des Entwurfs zu Recht grundsätzlich auf bereits vorhandene Datenbestände verwiesen, die des weiteren nur anonymisiert genutzt werden dürfen. Außerdem begründeten die im Erhebungsbogen gestellten Fragen erhebliche Zweifel an der Geeignetheit der entsprechenden Datenverarbeitung zu dem vom Landesgesundheitsamt selbst definierten Zweck. Da jedoch öffentliche Stellen auch mit Einwilligung der Betroffenen personenbezogene Daten nur verarbeiten dürfen, soweit dies zur rechtmäßigen Erfüllung ihrer gesetzmäßigen Aufgaben geeignet und erforderlich ist, war die mit der Durchführung des Allergievorsorgeprojekts verbundene Datenverarbeitung als nicht rechtmäßig zu beurteilen.

Da die in der Herstellung zudem teuren Erhebungsbögen bereits versandt waren und die Durchführung der Untersuchungen schon begonnen hatte, konnte es für die Einschulungsuntersuchung 1994 zunächst nur noch darum gehen, kurzfristig die noch möglichen datenschutzrechtlichen Korrekturen nachzuholen. Dabei konnte - als Kompromißlösung - u. a. erreicht werden, daß in den Unterlagen des Schularztes nur Angaben zum ersten Teil des Erhebungsbogens aufgenommen wurden. Ferner wurden das erforderliche Einverständnis der Eltern nachgeholt und, wo dies nicht mehr möglich war oder verweigert wurde, die bereits ausgefüllten Erhebungsbögen mit Ausnahme der Angaben zum ersten Teil der Fragen vernichtet.

Ich gehe davon aus, daß die zuständigen Ministerien die aufgezeigten rechtlichen Grenzen der Datenverarbeitung bei der Feststellung der Schulreife künftig beachten werden, und werde selbstverständlich die kommenden Einschulungsuntersuchungen mit besonderer Aufmerksamkeit begleiten.

7.2.3 Datenschutz im Krankenhausbereich

7.2.3.1 Entwurf eines Landeskrankenhausgesetzes

Im Krankenhaus werden wie in kaum einer anderen Institution sensible Daten erhoben, gespeichert und übermittelt, deren Schutzwürdigkeit heute von niemanden bestritten wird. Besonders gravierend ist die Gefahr einer Stigmatisierung der Betroffenen bei einer unbefugten Offenbarung der Patientendaten gegenüber dem Arbeitgeber.

Dennoch enthielt der Entwurf eines Landeskrankenhausgesetzes (LKHG) keine bereichsspezifischen Regelungen für die Verarbeitung und den Umgang mit Patientendaten. Diesen Mißstand habe ich frühzeitig beanstandet.

Bei der Beratung des Gesetzentwurfs bat mich der Ausschuß für Arbeit, Gesundheit, Soziales und Frauen, ihm ausformulierte Vorschläge datenschutzrechtlicher Regelungen für das Landeskrankenhausgesetz zu unterbreiten. Dies ist daraufhin nach Abstimmung mit dem MAGSF und dessen vollinhaltlicher Billigung geschehen. Danach sollte der Patientendatenschutz in einem eigenständigen Abschnitt im Landeskrankenhausgesetz geregelt werden. Dazu gehörten im wesentlichen folgende Regelungsgegenstände:

- Patientendatenschutz

  Nach einer Definition des Begriffs "Patientendaten" wurden zunächst die Voraussetzungen für die Zulässigkeit der Datenverarbeitung hinsichtlich Form und Inhalt normiert. Hierbei kommt im Krankenhausbereich der Datenverarbeitung mit Einwilligung des Betroffenen ein besonderer Stellenwert Rolle, da die Einwilligung bzw. deren Verweigerung für den Patienten mit schwerwiegenden und nicht überschaubaren Folgen verbunden sein kann. Deshalb ist der Patient vorab umfassend aufzuklären und darf ihm keine pauschal abgefaßte Einwilligungserklärung abverlangt werden.

  Ferner sollte die absehbare technische Entwicklung in der Medizin, beispielsweise bei Datenfernübertragungen über öffentliche oder interne Netze, in Einklang mit dem Patientendatenschutz gebracht werden.

- Übermittlung von Patientendaten

  Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ohne Einwilligung des Betroffenen ist nur unter den engen Voraussetzungen des Grundsatzes der Erforderlichkeit zulässig, die in einem abschließenden Katalog festgelegt sind.

- Auskunft und Akteneinsicht

  Dem Patienten ist auf Antrag kostenfrei Auskunft und Einsicht in seine Krankenunterlagen einschließlich der ärztlichen und pflegerischen Dokumentation zu gewähren. Die Auskunft über medizinische Daten ist durch einen Arzt zu vermitteln und umfaßt auch Angaben über die Personen und Stellen, denen die Patientendaten übermittelt werden.

- Löschung und Sperrung von Patientendaten

  Patientenakten sind nach Abschluß der Behandlung zunächst zu sperren, spätestens aber nach Ablauf von 30 Jahren zu löschen oder gegebenenfalls zu anonymisieren.

- Datenverarbeitung im Auftrag

  Patientendaten dürfen grundsätzlich nur durch eigenes Personal und im Krankenhaus selbst

verarbeiten werden. Eine Datenverarbeitung im Auftrag kann nur unter engsten Voraussetzungen und besonders gelagerten Fällen in Betracht kommen.

- Wartung und Fernwartung

  Da bei der Wartung und Fernwartung von ADV-Systemen im Krankenhaus, auch Patientendaten unbefugt offenbart werden können (s. unter 1.2.1.2), bedarf es einer besonderen bereichsspezifischen Regelung, unter welchen Voraussetzungen dies zugelassen wird.

  Grundsätzlich darf inbesondere die Fernwartung nur als letzten Mittel zur Fehlerbehebung eingesetzt werden. Sie darf nur mit Willen des Krankenhauses und im Einzelfall, d.h. nicht für routinemäßige Wartungsarbeiten, erfolgen. Der Wartungsvertrag muß zu besonderen technischen und organisatorischen Vorkehrungen (wie z. B. die Protokollierung aller Aktivitäten innerhalb eines Wartungsvorganges) verpflichten.

- Datenschutz bei Forschungsvorhaben

  Die Verarbeitung von Patientendaten für Forschungszwecke ist grundsätzlich nur mit Einwilligung des Betroffenen zulässig. Wenn der behandelnde Arzt die Daten seiner eigenen Patienten zu Forschungszwecken verwenden möchte, sollte er der Einwilligungsvorbehalt nicht gelten.

- Klinisches Krankheitsregister

  Die im Krankenhaus geführten (klinischen) Krankheitsregister dienen einerseits Behandlungszwecken und werden andererseits über diesen Rahmen hinaus zur Erforschung von bestimmten Krankheiten genutzt. Insofern können die auch im Land Brandenburg bereits existierenden klinischen Krankheitsregister nicht unbegrenzt ohne eine gesetzliche Grundlage geführt werden. Insbesondere muß der Betroffene der Speicherung und ggf. Übermittlung seiner Daten zustimmen.

Der Ausschuß hat keine meiner Vorschläge inhaltlich in Abrede gestellt, schreckte jedoch zurück, diese detaillierte Regeldichte in das Gesetz aufzunehmen. Stattdessen sollte die Landesregierung ermächtigt werden, nach Inkrafttreten des Landeskrankenhausgesetzes unverzüglich eine Rechtsverordnung zu erlassen, in der meine Empfehlungen umgesetzt werden sollten. Ich bedaure diese Entscheidung aus zweierlei Gründen. Zum einen erfährt damit die im Krankenhausbereich inzwischen vielfach beklagte Rechtsunsicherheit beim Umgang mit Patientendaten eine weitere unnötige Verlängerung. Zum anderen hat sich damit das Parlament seiner Aufgabe entzogen, selbst durch ein öffentliches Gesetzgebungsverfahren materielle datenschutzrechtliche Regelungen zu schaffen, und hat stattdessen diese Aufgabe der Verwaltung überlassen.

7.2.3.2 Brandenburgisches Psychisch-Kranken-Gesetz

Dieselbe Problematik - wie beim Landeskrankenhausgesetz - zeigt sich beim Psychisch-Kranken-Gesetz. Auch hier wurde unterlassen, in den Gesetzentwurf bereichsspezifische Regelungen gem. § 41 Abs. 2 Bbg DSG aufzunehmen.

7.2.3.3 Kontrollbesuche in Krankenhäusern

Mehrere Krankenhäuser wurden im Berichtszeitraum aufgesucht, um die praktischen Probleme kennen zu lernen. Dabei wurde insbesondere

- der Stand und die Organisation der dv-mäßigen Verarbeitung von Patientendaten,
- die Überprüfung der verwendeten Formulare einschließlich der Einwilligungserklärung

sowie
- die Archivierung und Vernichtung von Patientenakten

geprüft. Die derzeitige datenschutzrechtliche Situation soll nachfolgend an zwei typischen Beispielen dargestellt werden:

- Das *1. Kreiskrankenhaus* verfügt gegenwärtig über insgesamt 130 Betten und unterhält drei Stationen (Chirurgie, Innere und Kinderabteilung).

  Die Angaben zu den Patienten werden bei der Anmeldung über einen PC, der durch ein lokales Netz mit dem Server-Rechner verbunden ist, in einer Datei gespeichert. Die Benutzerkontrolle am PC wird über Paßwortabfrage realisiert. Der Arbeitsplatz, an dem nachts die Datensicherung über einen Streamer (Magnetbandlaufwerk) erfolgt, ist nicht ausreichend gegen Zugriff Unbefugter abgesichert.

  Das Aufnahmeformular setzt den Patienten in Kenntnis, daß die im Rahmen des abgeschlossenen Behandlungsvertrages erhobenen personenbezogenen sozialen und medizinischen Daten "gespeichert, geändert bzw. gelöscht und erforderlichenfalls, soweit dadurch nicht offenkundig seine Interessen verletzt werden, an Dritte (z. B. Kostenträger) übermittelt werden". Unter dieser Maßgabe werden im Aufnahmeschein auch nach Konfession und Staatsangehörigkeit des Betroffenen gefragt, obwohl beide Daten mit dem eigentlichen Behandlungsvertrag nichts zu tun haben und insoweit nur auf freiwilliger Basis gem. § 4 Abs. 1 Buchst. b Bbg DSG erhoben werden dürften. Ein entsprechender Hinweis fehlt jedoch. Ähnlich verhält es sich mit der Notwendigkeit der Angabe zum Arbeitgeber, die nur im Falle eines Arbeitsunfalls als erforderlich anzusehen ist.

  Die Archivierung der Patientenakten des Krankenhauses wird in zwei getrennten Räumen vorgenommen. Ein gegenüber der Patientenaufnahme gelegener Teil des Archivs bot vorbildliche und gut gesicherte Lagerbedingungen. Der zweite Raum im Keller des Gebäudes war jedoch dagegen ungeeignet und gewährleistet wegen der allgemein zugänglichen, mit einem einfachen Sicherheitsschloß versehenen Tür keine Sicherheit gegen einen unbefugten Zugriff.

  Die neu installierte Telefonanlage ist mit einer zentralen Gebührenerfassung ausgestattet. Diese weist alle Einzelgespräche aus. Während bei den Privatgesprächen der Patienten eine Verkürzung der Zielrufnummern um die letzten drei Ziffern erfolgt, werden die Verbindungsdaten aller Dienstgespräche komplett aufgelistet.

  Die Aufbewahrung der Patientenakten mußte beanstandet werden. Darüber hinaus habe ich empfohlen, den Raum, wo die Datensicherung vorgenommen wird, in das im Haus bereits vorhandene Kontrollsystem über Bewegungsmelder einzubeziehen. Bezüglich der Aufnahmeformulare verweise ich auf 7.2.3.6.

- Das *2. Kreiskrankenhaus* besteht gegenwärtig noch aus zwei weit auseinander liegenden Standorten am Ort und wird demnächst schrittweise mit einem anderen Kreiskrankenhaus vereint

  Es verfügt derzeit über einen zentralen Server-Rechner vom Typ GPX 440, mit dem beide Häuser vernetzt sind. Mit dem vorhandenen Softwaresystem "Krankenhausverwaltung" werden die Bereiche Telefonie (Telefonverzeichnis), Patientendaten- und Diagnoseverwaltung und Statistik dv-mäßig abgedeckt. Neben dem Systembetreuer haben sonstige Mitarbeiter nur mittels Paßwort Zugriff auf spezielle Menüs. Die vorhandene Rechnertechnik soll im Zuge des geplanten Krankenhauszusammenschlusses ersetzt und die Vernetzung auf die hinzukommenden Standorte erweitert werden.

  Der Server-Rechner ist derzeitig räumlich in einer DDR-typischen Baracke, mit

ungeschützter Fensterfront direkt an der Straße gelegen, untergebracht. Ihre Außen-und Trennwände bestehen aus Preßplatten. Sicherheitsschlösser existieren nicht. Darüber hinaus ist nachts keine Bewachung vorgesehen. Diese Situation ist aus einer traditionellen Gebäudenutzung hervorgegangen, aber gemessen an Anforderungen, die heute an eine Sicherheitskonzeption zu stellen sind, völlig unakzeptabel. Zusätzlich geht das Krankenhaus ein weiteres Sicherheitsrisiko ein, indem es die Datensicherung über Nacht auf einem Streamer-Laufwerk vornimmt und dabei die Sicherungskopie praktisch bis zum nächsten Tag im Laufwerk verbleibt. Somit erfüllt die EDV-Zentrale des Krankenhaus nicht die gem. § 10 Bbg. DSG notwendigen technischen und organisatorischen Maßnahmen, was ich beanstandet habe.

Zur Abstellung dieser unhaltbaren Mängel habe ich empfohlen, als Übergangslösung bis zur anstehenden Zusammenlegung der beiden Krankenhäuser Bewegungsmelder in der EDV-Zentrale zu installieren, den Server-Rechner in einem einbruchsicheren Data-Safe aufzubewahren und die Anfertigung von Sicherheitskopien lediglich in Anwesenheit des EDV-Verantwortlichen vorzunehmen. Langfristig sind aber unabdingbar andere geeignete Räumlichkeiten als EDV-Zentrale vorzusehen.

Das Krankenhaus verwendet im wesentlichen Vordrucke, die auf das vorhandene Softwaresystem "Krankenhaus" abgestimmt sind. Dabei werden mit dem Antrag auf Krankenhausaufnahme in unzulässigem Umfang Daten (Beruf, Arbeitgeber, Konfession und Hausarzt) erhoben. Bei der auf dem Antrag rückseitig befindlichen Einverständniserklärung wird auf Vorschriften der alten Fassung des Bundesdatenschutzgesetz (BDSG) verwiesen, die insofern durch die entsprechenden Paragraphen des BDSG neuer Fassung im Text zu ersetzen wären. Der Text der Einwilligungserklärung hat folgenden Wortlaut:

> "Ich habe Kenntnis genommen, daß Daten zu meiner Person EDV-mäßig verarbeitet werden. Diese Datenverarbeitung erfolgt im Rahmen der gesetzlichen Zulässigkeit gem. § 22 Abs. 2 und 3 sowie §§ 23 - 30 BDSG. Eine Übermittlung der Daten findet statt, soweit dies erforderlich ist und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Eine Berichtigung, Sperrung und Löschung der Daten kann beim Dezernat Finanzwesen beantragt werden."

Für den Betroffenen ist weder ersichtlich noch nachvollziehbar, auf welche Tatbestände sich seine Einwilligung bezieht. Der Hinweis auf die Regelungen des BDSG ist unzutreffend; hierfür ist das Bbg DSG grundsätzlich maßgebend, soweit sich das Krankenhaus in öffentlich-rechtlicher Trägerschaft befindet. Mit Dezernat Finanzwesen war eine Stelle im Krankenhaus selbst gemeint. Trotzdem ist diese vorgesehene Verfahrensweise sehr zweifelhaft; ich habe darauf hingewiesen, daß es dabei in keinem Fall zu einer Beeinträchtigung des Vertrauensverhälnis zwischen Arzt und Patient kommen darf.

Die Archivierung der Patientenakten erfolgt in drei verschiedenen Räumen im Haupthaus. Gegenüber der Patientenaufnahme werden die neueren Krankenakten und eine Suchkartei für alte Akten relativ sicher und geordnet gelagert. Ältere Krankenakten werden sowohl in einem ungeeigneten Kellerraum (Sicherheitsstufe der Fenster) als auch in einem abgelegenen Raum des bewohnten Dachgeschosses gelagert. Im letzteren war keine systematische Aufbewahrung zu erkennen. Die Zugangssicherung über eine einfach verschlossene Tür ist ferner als nicht zufriedenstellend zu beurteilen. Dies habe ich beanstandet.

Die Aktenvernichtung erfolgt turnusmäßig nach 30 Jahren; dafür existiert eine vertragliche Vereinbarung, in der in § 3 lediglich von einer ordnungsgemäß durchgeführten Vernichtung die Rede ist. Der Vertrag enthält z.B. keine Angabe über die Art der Vernichtung (u.a. Streifenbreite, Zwischenlagerung) sowie innerhalb welcher Frist die

Vernichtung durch den Vertragspartner nach Abholung der Akten erfolgen muß. Darüber hinaus wird auch auf das Erfordernis eines Vernichtungsprotokolls verzichtet. Das habe ich beanstandet und gefordert, den Vertrag bezüglich der angesprochenen Punkte zu konkretisieren.

7.2.3.4 Warnmeldungen über Krankenhauswanderer

In Rundschreiben von Landeskrankenhausgesellschaften und Leistungsträgern sind verschiedentlich Krankenhäuser vor sog. "Krankenhauswanderern" mit dem Hinweis gewarnt worden, daß dieser so bezeichnete Personenkreis diverse Krankenhäuser aufsuchen würde und sich stationär wegen vorgeschobener Krankheiten behandeln ließe. Ich bin dieser Frage bei den im Berichtszeitraum kontrollierten Krankenhäusern nachgegangen. Dort war diese Problematik mit je einer Einzelmeldung aus dem Jahre 1992 bekannt.

Aus datenschutzrechtlicher Sicht ist die Erforderlichkeit und damit die Befugnis zur Offenbarung der Daten dieser Personen mit Namen, Geburtsdatum, Adresse und der Hinweis auf "Krankenhausvagabundismus" abzulehnen. Da die aufgenommenen Patienten ohnehin untersucht und je nach Untersuchungsergebnis behandelt werden müssen, kann eine solche Warnmeldung allenfalls Anlaß zu einer besonders kritischen Untersuchung geben. Es besteht weder eine Rechtsgrundlage für diese Warnschreiben noch für eine Speicherung oder Nutzung der übermittelten Daten durch das angeschriebene Krankenhaus. Letzteres ist schon deshalb grundsätzlich unzulässig, weil es sich dabei um eine grundrechtswidrige Datenverarbeitung auf Vorrat handeln würde. Deshalb dürfen die Krankenhäuser selbst

- keine Warnschreiben übermitteln, speichern oder nutzen und
- müssen etwa vorhandene Warnschreiben anderer Stellen unverzüglich vernichten.

7.2.3.5 Zentrale Rechnungserfassung in Kliniken

Durch Kollegen aus anderen Bundesländern erhielt ich den Hinweis, daß dort z. T. an Krankenhäusern eine sog. "zentrale Rechnungserfassung" eingeführt werden. Jede Postsendung, die nicht mit dem Vermerk "persönlich" versehen ist, wird in diesen Krankenhäusern, weil sie eine Rechnung enthalten könnte, durch die Poststelle von dem für den inneren Postablauf zuständigen Mitarbeitern des Klinikums geöffnet. Durch eine solche Vorgehensweise würden sich die Beanstandungen hinsichtlich der Ordnungsmäßigkeit des Postablaufs auf ein Minimum verringern.

Bei meinen Kontrollbesuchen in den relativ kleinen Krankenhäusern habe ich festgestellt, daß dort diese Frage überhaupt keine Rolle spielt, da die Postöffnung und -verteilung von den Sekretariaten der ärztlichen Direktoren vorgenommen wird.

Da aber auch der das Vertrauensverhältnis Arzt/Patient betreffende Postinhalt im Krankenhaus den Grundsätzen der ärztlichen Schweigepflicht unterliegt, ist klarzustellen, daß das Verwaltungspersonal die Post nur zu Abrechnungszwecken öffnen darf. Im übrigen muß der Zugang zu der zwischen Patient und Arzt vertraulichen Korrespondenz durch die Krankenhausverwaltung ausgeschlossen werden. Dazu soll wie folgt verfahren werden:

Alle Brief und Postsendungen,

- die in der Anschrift den Namen des Arztes an erster Stelle enthalten, sind nur von diesem bzw. seinen engsten Mitarbeitern zu öffnen : z. B. Herrn/Frau Dr. ... Persönlich" (mit Anschrift des Krankenhauses); Herrn/Frau Dr. ... (im Krankenhaus...),

- die den Zusatz "zu Händen von" enthalten, sind an die namentlich genannte Person weiterzuleiten. Dieser Zusatz dient dem Adressaten sowohl als Verteilungsmerkmal als auch zur Klarstellung, daß es sich nicht um private Post handelt und

- die an das Krankenhaus ohne namentliche Benennung einer Person in der Anschrift adressiert sind, können von der Krankenhausverwaltung geöffnet werden.

7.2.3.6 Einwilligungserklärung der Patienten

Gem. § 12 Bbg DSG dürfen Daten nur erhoben werden, wenn ihre Kenntnis zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Insofern sind zur Durchführung des Behandlungsvertrages bei der Aufnahme des Betroffenen ein Stammdatensatz sowie weitere Daten zu erfassen. Dazu gehören:

- Name, Geburtsdatum und Adresse des Patienten,
- Daten zur Abrechnung mit dem Kostenträger,
- Anamnesedaten im medizinischen Bereich und
- im Falle eines Betriebsunfalles die Angabe des Arbeitgebers.

Auch weitere Daten dürfen nur erhoben werden, soweit dies zur Durchführung des Behandlungsvertrages erforderlich ist; das ist auch der Fall, wenn der Patient dies ausdrücklich wünscht (beispielsweise im Hinblick auf eine seelsorgerische Betreuung).

Bei der gesamten Datenerhebung sind die Bestimmungen der §§ 4 Abs. 2, 12 Abs. 3 Bbg DSG zu beachten. Dies bedeutet: Der Patient ist präzise über den Verwendungszweck aufzuklären sowie - im Fall etwa beabsichtigter Übermittlungen - über die weiteren Datenempfänger. Er muß darauf hingewiesen werden, daß seine Angaben die Voraussetzung für die Durchführung des Behandlungsvertrages sind sowie darauf, daß dies bei bestimmten Angaben nicht der Fall und ihm eine Beantwortung der Fragen insoweit völlig freigestellt ist. Die Erklärung muß unter drucktechnischer Hervorhebung oder auf einem gesonderten Formular erfolgen.

Ich habe bei allen Krankenhäusern, die in öffentlicher Trägerschaft stehen, angefragt, ob sie im Zusammenhang mit der Aufnahme von Patienten eine Einwilligungserklärung verwenden und darüber hinaus mir diese zur Verfügung zu stellen. Es ergab sich, daß - nach eigenen Angaben - nur drei Krankenhäuser ohne jegliche Einwilligungserklärung arbeiten; überwiegend wird in den Allgemeinen Vertragsbedingungen (AVB) lediglich ein Hinweis auf Datenschutz gegeben, der als Einwilligungserklärung verstanden wird.

Bei der Durchsicht der zugesandten Einwilligungserklärungen fielen mir eine Reihe von Mängeln auf:

- Überwiegend wird mit zu pauschal gefaßten Einwilligungserklärungen gearbeitet, d.h. die Patienten werden nicht ausreichend über die Verarbeitung ihrer Daten im Krankenhaus informiert. Dazu nachfolgend zwei Beispiele:

  "Ich versichere... und bin mit der Verarbeitung der erfaßten Daten zwecks Abrechnung und Versorgung einverstanden."
  "Ich nehme zur Kenntnis, daß meine personenbezogenen Daten vom Krankenhaus unter Beachtung des Datenschutzgesetzes gespeichert werden und die für die Rechnungslegung erforderlichen Daten an ein Rechenzentrum weitergeleitet werden."

- Mehrheitlich wird auf Bestimmungen des Bundesdatenschutzgesetzes verwiesen statt auf die des Brandenburgischen Datenschutzgesetzes.

- Zum Teil wird auf Bestimmungen der Allgemeinen Vertragsbedingungen (§ 14 Abs. 4 AVB) Bezug genommen, die einen für den Patienten viel zu schwammigen und nicht nachvollziehbaren Inhalt hinsichtlich der Datenverarbeitung im Krankenhaus aufweisen. § 14 Abs. 4 AVB lautet folgendermaßen: "Die Verarbeitung der Daten einschließlich ihrer Weitergabe erfolgt unter Beachtung der gesetzlichen Regelungen, insbesondere der

Bestimmungen über den Datenschutz, der ärztlichen Schweigepflicht und des Sozialgeheimnisses".

- Häufig wird im Aufnahmeantrag nach der Konfession, Pfarrgemeinden und Hausarzt gefragt, ohne daß dem Patienten erläutert wird, wem und unter welchen Umständen - evtl. nur der zugehörigen Religionsgemeinschaft - seine Daten weitergegeben werden, und ohne daß auf die Freiwilligkeit dieser Angaben hingewiesen wird.

- In zwei Fällen sollte sogar nach den Aufnahmeanträgen die Personenkennzahl (PKZ) angegeben werden, obgleich nach dem Einigungsvertrag[96] die PKZ bis zum 31.12.1992 in allen Dateien und Akten zu löschen waren. Eine Erhebung der PKZ bei der Aufnahme in ein öffentlich-rechtliches Krankenhaus wäre ein schwerer Verstoß gegen die datenschutzrechtlichen Bestimmungen.

Erfreulicherweise gab es auch eine Ausnahme. In einem Krankenhaus hat der Patient bereits die Möglichkeit anzukreuzen, ob seine Daten den Gesundheitsfürsorgestellen sowie dem Besucherdienst der Kirchen übermittelt, ein Namensschild an der Tür angebracht und Auskünfte über ihn durch den Pförtner erteilt werden dürfen.

Eine Behebung der genannten Mängel ist unerläßlich. Deshalb werde ich auf die einzelnen Krankenhäuser zugehen und entsprechende Maßnahmen anregen (s. Anlage 22). Zunächst wird jedoch in Abstimmung mit dem MAGSF zu prüfen sein, ob nicht eine Mustererklärung entwickelt und empfohlen werden kann, die sich zugleich den jeweiligen Besonderheiten des abzuschließenden Krankenhausvertrags anpassen läßt.

7.2.3.7 Blutuntersuchung im Auftrag

Ein Krankenhaus wandte sich mit der Bitte an mich, zu prüfen, ob eine patientenbezogene Rechnungslegung für Blutuntersuchungen im Auftrag zu den Bestimmungen des Datenschutzes in Widerspruch steht. Es kaufe z. B. vom DRK-Blutspendedienst Blutkonserven und Blutkonservenderivate. Diese Blutkonserven würden z. T. für einen bestimmten Patienten zubereitet, in Rechnung gestellt und gegenüber dem Leistungsträger patientenbezogen abgerechnet. Der Auftragnehmer sei aber der Auffassung, daß das Verwaltungspersonal nicht der ärztlichen Schweigepflicht unterliege. Demgemäß sei er lediglich bereit, der Krankenhausverwaltung Sammelrechnungen über einen bestimmten Zeitraum ohne einen Patientenbezug zukommen zu lassen. Die Patientennamen mit den Laboruntersuchungen würden dagegen dem Leiter des blutgruppenserologischen Labors des Krankenhauses separat zugeschickt. Verwaltung und Labor des Blutspendedienstes müßten insofern parallel arbeiten, so daß Überschneidungen in den angegebenen Abrechnungszeiträumen entstünden. Eine anonymisierte Rechnungslegung und -kontrolle sei praktisch unmöglich.

Nach datenschutzrechtlicher Prüfung war festzustellen, daß gemäß § 301 Abs. 1 SGB V die Krankenhäuser bereichsspezifisch zur personenbezogenen Abrechnung gegenüber den Leistungsträgern verpflichtet und berechtigt. Die durch das Gesundheitsstrukturgesetz eingeführte Praxis soll dem Patienten die Nachvollziehbarkeit der Abrechnung des Leistungserbringers ermöglichen. Dafür ist jeweils die Krankenhausverwaltung zuständig. Ihrem Zugriff auf die zur entsprechenden Rechnungslegung erforderlichen personenbezogenen Daten stehen daher die datenschutzrechtlichen Bestimmungen nicht entgegen.

---

96 vom 31. August 1990, BGBl. II, S. 889, Art. 14 i.V.m. Anl. I, Kap. II, Sachgeb. C, Abschn. III, Ziff. 4, Buchst. b und c

7.2.3.8 Qualitätssicherung in der Krankenhaushygiene

Eine vom Bundesministerium für Gesundheit geförderte, bundesweite Studie über "Nosokomiale Infektionen in Deutschland

- Erfassung und Prävention (NIDEP)" soll klären,
- wie häufig derartige Krankenhausinfektionen auftreten,
- ob es hierbei Abhängigkeiten bezüglich Größe eines Krankenhauses, der Art der Stationen und des Alters der Patienten gibt und
- welche Hygienestandards eingehalten werden müssen, um sie zu unterbinden.

Insoweit befaßt sich die Studie mit Fragen, zu deren Einhaltung die betreffenden Krankenhäuser als stationäre Leistungserbringer bereits im Rahmen ihrer internen Qualitätssicherung gem. § 113 SGB V verpflichtet sind.

Nach der Projektbeschreibung ist beabsichtigt, daß auf diesem Gebiet besonders geschulte Ärzte 53 repräsentativ ausgewählte Krankenhäuser im Verlaufe von 4 Jahren für jeweils einige Tage aufsuchen und in dieser Zeit sämtliche in Behandlung befindliche Patienten auf Vorhandensein von nosokomialen Infektionen beurteilen. Dazu sollen sie an Visiten teilnehmen, ggf. Einzelfälle inspizieren sowie durch Einsicht in die Krankenakten und Befragung der behandelnden Ärzte fallweise anonymisierte Daten erfassen und dem Institut für Umweltmedizin und Krankenhaushygiene der Universität Freiburg zur Auswertung übermitteln.

Eine derartige Verfahrensweise würde eine Offenbarung bzw. Übermittlung von Patientendaten an Dritte (hier Studienärzte) bedeuten. Da es eine zur Offenbarung der Patientendaten legitimierte, bereichsspezifische Befugnisnorm gem. § 4 Abs. 1 Buchst. b Bbg DSG bisher in Brandenburg nicht gibt, wäre dafür vorher die Einwilligung des Betroffenen einzuholen. Auf die bestimmte Forschungsvorhaben privilegierte Bestimmung des § 28 Abs. 2 Bbg DSG kann nicht zurückgegriffen werden, da dessen Voraussetzungen nicht vorliegen. Die Patienten sollten deshalb in geeigneter Weise über Sinn und Zweck der Studie rechtzeitig während ihres Krankenhausaufenthaltes aufgeklärt werden und um ihre Einwilligung gebeten werden.

Dem hat das MAGSF vehement widersprochen; es will bislang nicht einmal anerkennen, daß bei diesem Forschungsvorhaben personenbezogene Daten übermittelt werden. Dabei ist z. B. das "Bereithalten von Akten zur Einsichtnahme" in § 3 Abs. 2 Nr. 4 Bbg DSG ausdrücklich als Datenverarbeitung in Form als Übermíttlung definiert.

7.2.4 Berufsordnung der Landesärztekammer Brandenburg

Bereits 1991 hatte die Ärztekammer Land Brandenburg aufgrund des § 6 Abs. 3 Nr. 3 Kammergesetz[97] eine Berufsordnung beschlossen. Sie orientierte sich weitgehend an bereits vorhandene Vorlagen der Altbundesländer; ihre Überarbeitung war jedoch aufgrund einer Anpassung an § 21 Abs. 1 Nr. 4 Heilberufsgesetz (HeilBerG)[98] erforderlich.

Bei dieser Gelegenheit wurden zwei bereichsspezifische Datenschutzvorschriften in die Berufsordnung der Landesärztekammer Brandenburg[99] aufgenommen. Geregelt wurde zum

---

97

98 GBl. der DDR 1990 I, S. 711

vom 28. Januar 1992, GVBl. I, S. 30, i.d.F. vom 14. Juni
99 1993, GVBl. I, S. 198

ABl. 1993, S. 263

einen die weiteren Nutzung ärztlicher Aufzeichnungen nach Aufgabe bzw. Verkauf von Arztpraxen. Ich habe sehr begrüßt, daß dabei die höchstrichterliche Rechtssprechung der letzten Jahre zugrundegelegt wurde[100]. In der alten Fassung der Berufsordnung hatte der Arzt seine Aufzeichnungen und Untersuchungen lediglich, "in gehörige Obhut" zu geben. Nun ist zusätzlich in § 15 Abs. 4 der Berufsordnung geregelt, daß die Weitergabe der Unterlagen grundsätzlich nur noch nach vorher eingeholter schriftlicher oder mündlicher Einverständniserklärung des Patienten zulässig ist. Ferner wird dem Arzt, der bei Praxisübernahme Untersuchungsbefunde in Obhut nimmt, auferlegt, diese unter Verschluß zu halten. Er darf sie nur mit Einverständnis des Patienten einsehen oder weitergeben.

Zum anderen wurde eine entsprechende Anregung von mir aufgegriffen und für klinische Versuche eine bereichsspezifische Datenschutzvorschrift in die Berufsordnung aufgenommen. Gem. § 1 Abs. 4 der Berufsordnung ist der Arzt nunmehr ausdrücklich verpflichtet, bei Verwendung personenbezogener Daten für klinische Versuche die Zustimmung seines Patienten einzuholen oder aber eine hinreichende Anonymisierung der Daten vorzunehmen.

7.2.5 Gesetz über die Ausübung des Berufes der Hebammen und des Entbindungspflegers

Das Bundeshebammengesetz[101] regelt lediglich die Berufszulassung der Hebammen. Im Rahmen der Kompetenzverteilung von Bund und Länder sind daher die Länder gehalten, Voraussetzungen für die Berufsausübung zu schaffen. Zusätzlich bestand für das Land Brandenburg bei der Verabschiedung eines Landeshebammengesetzes (HebGBbg) dringender Handlungsbedarf, weil bereits 1992 durch das Bundesgesundheitsministerium angemahnt worden war, die EG-Richtlinie 80/155/EWG vom 21.01.1980[102] in entsprechende landesrechtliche Regelungen umzusetzen.

Das inzwischen verabschiedete Gesetz[103] stellt im wesentlichen eine Ermächtigungsgrundlage für das zuständige Ministerium dar, durch Rechtsverordnung (Berufsordnung) die Pflichten und Befugnisse der Hebammen und Entbindungspfleger zu regeln. Die dabei insbesondere zu regelnden Sachverhalte betreffen die Pflicht zur Dokumentation, Melde- und Auskunftspflichten gegenüber den Gesundheitsbehörden u.a. Damit hat sich der Gesetzgeber in einem weiteren Fall seiner Verantwortung für die Schaffung von bereichsspezifischen Regelungen entzogen[104].

Bei den Beratungen im Ausschuß für Arbeit, Soziales, Gesundheit und Frauen hatte ich mich dafür ausgesprochen, das Brandenburgische Hebammengesetz und die Berufsordnung einschließlich sog. Hebammentagebuch zusammen zu behandeln und zeitgleich in Kraft treten zu lassen. In Bezug auf den Gesetzentwurf konnte nur noch erreicht werden, daß die Pflichten zur Dokumentation gem. § 1 Abs. 2 Nr. 3 HebGBbg durch Streichung des Wortes "insbesondere" enumerativ geregelt sind und das Gesetz diesbezüglich eine normenklare und abschließende Regelung trifft.

100

101 BGH Urteil vom 11.12.1991 - in: NJW 1992, S. 737

vom 4. Juni 1985, BGBl. I, S. 902, i.d.F. vom 23. März 1992

102 I, S. 719

Amtsblatt der Europäischen Gemeinschaft Nr. L 33-8 vom 11.

103 Februar 1980

104 vom 19. Oktober 1993, GVBl. I, S. 460

BVerfGE 65, 1, 1983

7.2.6 Berufsordnung für Hebammen und Entbindungspfleger

In Ausübung ihres Berufs erhalten vor allem freiberufliche Hebammen und Entbindungspfleger einerseits einen tiefen Einblick in die familiäre Situation der von ihnen betreuten Frauen und sind anderseits verpflichtet, ihre Tätigkeit in vorgegebener Weise zu dokumentieren. Hierzu enthält die Berufsordnung für Hebammen und Entbindungspfleger des Landes Brandenburg (HebBOBbg) bereichsspezifische Regelungen zur Datenverarbeitung.

Ich habe es begrüßt, daß in § 5 HebBOBbg auf die durch § 203 StGB geschützte berufliche Schweigepflicht ausdrücklich hingewiesen wird. Sie gilt hier auch für erhaltene schriftliche Mitteilungen und gegenüber Ärzten, die nicht zur Behandlung bzw. Betreuung herangezogen wurden.

Die Dokumentationspflichten der Hebammen und Entbindungspfleger beziehen sich gemäß § 4 Abs. 1 HebBOBbg auf die in Ausübung ihres Berufes getroffenen Feststellungen und Maßnahmen sowie - wenn die berufstätigkeit außerhalb von Krankenhäusern ausgeübt wird - auf die Führung eines Tagebuches. Alle diese Unterlagen sind gem. § 4 Abs. 2 HebBOBbg mindestens zehn Jahre aufzubewahren. Diese Regelungen sind vornehmlich unter auschließlich fachlichen Gesichtspunkten abgefaßt und bedürfen einer datenschutzrechtlichen Ergänzung. So fehlen vor allem normenklare Regelungen

- über die weitere Aufbewahrung bzw. Vernichtung dieser Unterlagen nach den vorgeschriebenen Aufbewahrungszeiten und

- über die Abgabe der Unterlagen im Falle im Falle des Todes bzw. eines endgültigen oder vorübergehenden Ausscheidens aus dem Berufslebens.

Ich hatte dem MAGSF vorgeschlagen, daß zuständige Gesundheitsamt in den genannten Fällen zu beauflagen, die Unterlagen in Verwahrung zu nehmen und diese für die restliche, vorgeschriebene Aufbewahrungszeit zu sperren. Das MAGSF hat dazu bisher nicht Stellung genommen.

Die Berufsordnung sollte gem. § 4 Abs. 1 HebBOBbg ein Muster für ein Hebammentagebuch enthalten. Über den Inhalt und die Gestaltung dieses vielfach als überflüssig angesehenen Tagebuchs sind mir bisher trotz mehrfacher Nachfragen und auch trotz der Erörterung im Ausschuß für Arbeit, Soziales, Gesundheit und Frauen keine Vorstellungen seitens des zuständigen Ministeriums mitgeteilt worden. Ich habe vorsorglich darauf hingewiesen, daß Eintragungen von verschiedener Personalien, insbesondere von Name, Anschrift und Beruf der Eltern und Geschwister - wie es in manchen alten Bundesländern noch praktiziert wird - nicht zulässig wäre.

§ 4 Abs. 3 HebBOBbg enthält die Pflicht zur Übermittlung anonymisierter Auskünfte für statistische Zwecke auf Anforderung des Gesundheitsamtes. Dazu bedarf es nach § 3 Abs. 2 und § 7 Abs. 1 des Entwurfs eines Landesstatistikgesetzes, weil die Angaben nicht ausschließlich aus allgemein zugänglichen Quellen oder öffentlichen Registern resultieren und es sich um eine Landesstatistik für die Dauer von mehr als 3 Jahren handelt.

7.2.7 AOK

7.2.7.1 Offenbarungsersuchen bei Unterhaltspflichtverletzungen

Unterhaltspflichtige haben gem. § 1605 Bürgerliches Gesetzbuch (BGB) Auskunft über ihre Einkünfte und ihr Vermögen zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltsverpflichtung erforderlich ist. Die Jugendämter sind ständig damit befaßt, Unterhaltverpflichtungen geltend zu machen und wenden sich deshalb gem. §§ 69, 74 Nr. 2 SGB X mit einem Offenbarungsersuchen an Krankenkassen. Dies

betrifft Auskünfte zu Anschrift, Arbeits- und Versicherungsverhältnis sowie ggf. zum Arbeitgeber des Unterhaltspflichtigen.

Die AOK hat mir vor diesem Hintergrund mitgeteilt, daß viele Jugendämter im Land Brandenburg für ihr Ersuchen ein Formularblatt verwenden, die keine amtliche Versicherung enthält, daß der Unterhaltspflichtige gemahnt wurde. Andere legen darüber lediglich eine formlose Bescheinigung bei. Diese Offenbarungsersuchen sind deshalb von der AOK bisher urschriftlich zurückgesandt worden mit der Bitte, die gem. § 74 SGB X erforderliche Erklärung nachzureichen. Insofern entstand für die Bearbeitung des jeweiligen Sachverhalts bei den Jugendämtern ein nicht notwendiger Zeitverlust und ein vermeidbarer Verwaltungsaufwand. Da die eigenen Bemühungen zu keinem Erfolg geführt hatten, bat mich die AOK darum, mich landesweit für "ein datenschutzrechtlich abgesichertes Verfahren bei Offenbarungsersuchen in Fällen der Unterhaltspflichtverletzung einzusetzen".

Die von der AOK praktizierte Verfahrensweise habe ich begrüßt. Für das Offenbarungsersuchen ist in der Tat eine amtliche Versicherung, daß gem. § 74 SGB X gemahnt wurde, erforderlich, aber auch ausreichend. Ich habe dem Ministerium für Bildung, Jugend und Sport die Angelegenheit vorgetragen und angeregt, daß, obwohl die Jugendämter gem. § 69 Abs. 1 Kinder- und Jugendhilfegesetz (KJHG)[105] i.V.m. § 1 AGKJHG-Org.[106] ihre Aufgaben im wesentlichen eigenständig wahrnehmen, ein Formblatt mit von Amts wegen bestätigter Mahnung ausgearbeitet und den Jugendämtern durch das Landesjugendamt dringend zur Nutzung für derartige Offenbarungsersuchen empfohlen wird. Das Ministerium hat zu diesem Vorschlag bislang nicht Stellung genommen.

Festzuhalten bleibt, daß die Jugendämter bei Unterhaltspflichtverletzungen nicht berechtigt sind, auf anderen Wegen als bei der Krankenversicherung Auskünfte über den Unterhaltspflichtigen einzuholen. In den alten Bundesländern ist dies gelegentlich u. a. über den Arbeitgeber oder über das Suchblatt des Deutschen Instituts für Vormundschaftswesen geschehen.

7.2.7.2 AOK Hilfsmittelberatung für das Land Brandenburg GmbH

Im August 1993 informierte mich das Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MAGSF) darüber, daß Anfang des Jahres die AOK Hilfsmittelberatung für das Land Brandenburg GmbH (HBB) gegründet worden war, deren Aufgabe es sein soll, bei der AOK für das Land Brandenburg zur verbesserten Beratung und Betreuung Versicherter eine Hilfsmittelberatung durchzuführen. Das Ministerium bat mich um eine datenschutzrechtliche Prüfung des Vertrages zwischen der AOK und der HBB, der im November 1993 noch durch einen "Datenschutzvertrag" ergänzt wurde, durch den ausdrücklich eine Datenverarbeitung durch die HBB im Auftrag der AOK geregelt werden soll, obgleich die AOK an anderer Stelle betont hat, daß es sich gerade nicht um eine Datenverarbeitung im Auftrag handle.

Letzteres ist auch zutreffend. Der Sache nach handelt es sich bei der Tätigkeit der AOK Hilfsmittelberatung GmbH nicht um eine Datenverarbeitung im Auftrag der AOK, sondern um die Wahrnehmung von Aufgaben der öffentlichen Verwaltung, die der HBB auf der Grundlage eines Geschäftsbesorgungsvertrages zur selbständigen Erledigung übertragen werden. Im Vordergrund steht nicht die Verarbeitung personenbezogener Daten, sondern die eigenständige, nach außen gerichtete Tätigkeit der GmbH.

105

106 vom 26. Juni 1990, BGBl. I, S. 1163
vom 19. Dezember 1991, GVBL. S. 676

Die Hilfsmittelberatung nach §§ 275 Abs. 3 Nr. 2, 127 Abs. 3 SGB V[107] ist eine den Krankenkassen zugewiesene Aufgabe, deren Wahrnehmung in das Ermessen der Krankenkassen gestellt ist. Dabei ist das Ermessen bezüglich der Art und Weise der Aufgabenwahrnehmung eingeschränkt. Nach der Regelung im § 275 Abs. 3 Nr. 2 i.V.m. Abs. 5 SGB V kann die AOK die Hilfsmittelberatung entweder nur selbst durchführen oder mit der Durchführung dieser Aufgabe den medizinischen Dienst beauftragen, der dazu vom Gesetzgeber ausdrücklich weisungsfrei gestellt worden ist. Ich bin in meiner Stellungnahme zu dem Ergebnis gekommen, daß die Beauftragung anderer Stellen nach Maßgabe dieser Regelung ausgeschlossen ist.

Gegenüber der AOK und dem Ministerium habe ich im einzelnen ausführlich begründet, warum deshalb die nach dem Vertrag vorausgesetzte Übermittlung personenbezogener Daten der bei der AOK Versicherten an die HBB nach Maßgabe der darauf anzuwendenden Bestimmungen der Sozialgesetzbücher I, V und X sowie des Bundesdatenschutzgesetzes und des Brandenburgischen Datenschutzgesetzes unzulässig ist. Eine Stellungnahme in der Sache ist bislang jedoch weder seitens der AOK noch seitens des Ministeriums erfolgt. In einer ersten Reaktion hat die AOK meine Stellungnahme Anfang des Jahres als "datenschutzrechtliche Anwürfe" zurückgewiesen und meine Ausführungen zur Rechtslage für entbehrlich gehalten, da die Prüfung, ob und gegebenenfalls inwieweit die Hilfsmittelberatung an Dritte übertragen werden könne, ausschließlich dem Ministerium obliege.

Ich hatte deshalb nachdrücklich auf eine Beachtung meiner Kompetenzen nach Art. 74 Abs. 1 Satz 3 der Landesverfassung sowie den Bestimmungen des Brandenburgischen Datenschutzgesetz zu bestehen. Gleichwohl ist eine Stellungnahme der AOK in der Sache nicht erfolgt, so daß nur von einer bislang einzigartigen Mißachtung meines Amtes als vom Parlament zur Erfüllung des verfassungsrechtlichen Auftrages gem. Art 11 und 74 der Landesverfassung gewählter Landesbeauftragter für den Datenschutz gesprochen werden kann.

Eine gemeinsame sachliche Suche nach datenschutzgerechten Lösungsmöglichkeiten konnte daher bislang nicht erfolgen. Vielmehr bleibt lediglich die unbefriedigende Tatsache zu berichten, daß wieder einmal auf rechtlich völlig ungesicherter Basis Maßnahmen von erkennbarer und sogar besonders ausgeprägter datenschutzrechtlicher Relevanz ergriffen wurden, ohne es auch nur im entferntesten für nötig zu halten, mich vorab darüber zu informieren, geschweige denn um die Meinung meiner Behörde zu fragen.

7.2.8 Bundeseinheitliche Rettungsdienst- und Notarzteinsatzprotokolle

Die Sektion Rettungswesen der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin (DIVI) hat ein Notarzteinsatzprotokoll erarbeitet und den Bund-Länder-Ausschuß "Rettungswesen" gebeten, sich für seine bundesweite Einführung zu verwenden. Das MAGSF trat deshalb an mich heran und bat um Prüfung, ob der Verwendung der Protokolle in Brandenburg zugestimmt werden kann. Dies betraf sowohl ein Protokoll für den Notarzt- (sog. Notarzteinsatzprotokoll), als auch für den Rettungsdiensteinsatz ohne Notarzt (sog. Rettungsdienstprotokoll). Beide Protokolle enthalten an personenbezogenen Daten Angaben zu Name, Geburtsdatum, Arbeitgeber, Versicherungsstatus und Wohnung des Patienten. Das Original verbleibt beim aufnehmenden Krankenhaus bzw. dem Rettungsdienst; die zwei bzw. eine im Durchschriftverfahren erstellte(n) Kopie(n) sind für spätere wissenschaftliche Auswertungen und Qualitätskontrollen des Rettungsdienstes vorgesehen.

---

107 vom 20. Dezember 1988, BGBl. I, S. 2477

Eine Umfrage bei den Datenschutzbeauftragten der Länder hat nicht bestätigt, daß diese Rettungs- und Notarzteinsatzprotokolle bundesweit eingesetzt werden. Dies ist bisher lediglich in Bayern und im Saarland der Fall. Meine Zustimmung zum Einsatz dieser Protokolle habe ich von der Bedingung abhängig gemacht, daß durch Schwärzung oder Nichtaufbringung in den für wissenschaftliche und statistische Zwecke angefertigten Kopien keine personenbezogenen Daten enthalten sind. Für diese Zwecke sind diese Daten nicht erforderlich und ihre Übermittlung wäre ein Verstoß gegen das Sozialgeheimnis gem. § 35 Abs. 1 SGB I. Die Offenbarungsbefugnisse für Sozialdaten sind abschließend in §§ 67 ff. SGB X normiert.

Wünschenswert ist darüber hinaus eine jeweils eindeutige Bezeichnung des Empfängers auf den Ausfertigungen und die Schaffung einer bereichsspezifischen Regelung, die diese Verfahrensweise bestimmt. Gem. § 11 Rettungsdienstgesetz (BbgRettG)[108] wäre dazu das für das Gesundheitswesen zuständige Ministerium auch zum Erlaß einer entsprechenden Rechtsverordnung befugt.

7.2.9 Krebsregistergesetz

Epidemiologische Krebsregister existieren derzeit nur Hamburg, Nordrhein-Westfalen und dem Saarland; in den fünf neuen Bundesländern einschließlich Berlin wird dagegen aufgrund des Krebsregistersicherungsgesetzes[109] das Nationale Krebsregister der DDR bis zum 31.12.1994 weitergeführt. Die Bundesregierung hält dieses Instrumentarium zur Krebsursachenerkennung inzwischen für so wichtig, daß sie 1993 in den Bundesrat einen Entwurf eines Gesetzes über Krebsregister (BR-Drs. 669/93) eingebracht hat. Auf dieser Grundlage sollten die Länder bis zum 01. Januar 1999 stufenweise verpflichtet werden, flächendeckend und einheitlich in ganz Deutschland Krebsregister aufzubauen.

Nach dem derzeitigen Stand konnte sich die Bundesregierung mit ihrem Vorhaben gegenüber den Bundesländern nicht durchsetzen. Krebs stellt i.S.v. Art. 74 Nr. 19 Grundgesetz keine "gemeingefährliche (übertragbare) Krankheit" dar. Dementsprechend stellt ein Krebsregister auch keine "Maßnahme" gegen eine bestimmte Krankheit, sondern im Höchstfall ein geeignetes Informationsmittel zur Gewinnung von Kenntnissen über und zur besseren Verhütung von Krebserkrankungen dar. Darüber hinaus sind auch erhebliche epidemiologische, ethische und datenschutzrechtliche Bedenken gegen die Konzeption des Entwurf geltend gemacht worden.

Da der Wille besteht, eine gesetzliche Grundlage für die Weiterführung des Krebsregisters der neuen Länder und Berlins über den 31.12.1994 hinaus zu schaffen, ist es angebracht, die vorgesehenen Regelungen des angeführten Bundesgesetzentwurfes unter diesem Aspekt zu würdigen:

- Die Führung der Krebsregister sollte auf der Grundlage der Meldeberechtigung des behandelnden Arztes und der Angabe des vollen Namens des Betroffenen an eine Vertrauensstelle basieren. Darüber sollte der Patient vor- oder nachher zu unterrichten sein und konnte seinerseits auch nachträglich Widerspruch einlegen.

- Erst die Vertrauensstelle sollte die Identifizierungsdaten des Betroffenen zweimal verschlüsseln; zunächst mit einem asymmetrischen Chiffrierverfahren und danach mit einem zweiten Verfahren, das eine Wiedergewinnung der Identitätsdaten ausschließt. Allerdings sollte die Vertrauensstelle auch für Forschungszwecke eine Entschlüsselung der Identitätsdaten vornehmen; dazu bedurfte es der Zustimmung des Betroffenen.

108

109 vom 8. Mai 1992, GVBl. I, S. 170
vom 29. Dezember 1992, BGBl. I, S. 2335

- Nur verschlüsselt sollte die Vertrauensstelle die Daten an die eigentliche Registerstelle weitergeben. Diese sollte ihrerseits mit Hilfe der durch die irreversible Verschlüsselung gewonnenen Kontrolldaten und prüfen, ob über den Betroffenen bereits Daten existieren und ergänzt diese gegebenenfalls.

- Das Bundesgesundheitsamt sollte einmal jährlich von der Vertrauensstelle die epidemiologische Daten einschließlich Geschlecht, Monat und Geburtsjahr sowie Wohnort, Staatsangehörigkeit und Angaben zur Berufstätigkeit aller Betroffenen erhalten.

- Außerdem sollte ein Abgleich von epidiologischen Daten und Kontrollnummern zwischen den verschiedenen Vertrauensstellen erfolgen, um Doppelmeldungen in verschiedenen Bundesländern feststellen zu können.

Bisherige Vorstellungen zur Weiterführung des Krebsregisters der neuen Bundesländer einschließlich Berlins favorisieren in wesentlichen Teilen diese im Entwurf eines Bundeskrebsregistergesetz vorgesehene Verfahrensweisen. Abweichend davon soll lediglich die zu schaffende Vertrauensstelle zur Senkung des zu betreibenden Gesamtaufwandes in einem Arbeitsgang die Verschlüsselung der Identitätsdaten und die Bildung der Kontrollnummer sowie die Kodierung der epidemiologischen Daten vornehmen. Aber nicht nur über eine solchermaßen entlastete Registerstelle wird nachgedacht, sondern darüber hinaus wird sogar aus Gründen der Kosteneinsparung eine für Vertrauens- und Registerstelle gemeinsame Verwaltung ernsthaft in Erwägung gezogen. Damit wäre nicht einmal die Forderung der Datenschützer nach strikter organisatorischer und räumlicher Trennung beider Dienststellen eingehalten.
Demgegenüber gibt es dezentrale Verschlüsselungsmodelle, die in Baden-Württemberg bereits erprobt sind und lediglich eine anonymisierte (kodierte) Meldung durch den behandelnden Arzt an das Krebsregister erforderlich machen. Dies hat zur Folge, daß dadurch einerseits nicht in das Vertrauenverhältnis zwischen Arzt und Patienten eingegriffen wird und das andererseits keine Stelle existiert, die technisch in der Lage wäre, alle gemeldeten Krebskranken jederzeit wieder zu reidentifizieren. Eine derartige Verfahrensweise wäre nicht nur datenschutzfreundlich, sondern auch vom Betroffenen vollständig nachvollziehbar und ließe deshalb eine hohe Akzeptanz erwarten.

7.2.10 Transplantationsgesetz

Seit 1979 haben der Bundesregierung und dem Bundesrat mehrere Entwürfe für ein Transplantationsgesetz vorgelegen, die jedoch bereits in den Gesetzgebungsverfahren scheiterten. Die rechtliche Absicherung der von der Transplantation aktiv und passiv Betroffenen basierte in den alten Bundesländern lediglich auf der ausdrücklichen Einwilligung des Spenders. Für die neuen Bundesländern würde mit Inkrafttreten eines Transplantationsgesetzes die große Unsicherheit über die Fortgeltung einzelner Vorschriften des alten DDR-Rechts im Gesundheitsbereich beendet. Durch Art. 9 Abs. 2 Einigungsvertrag i.V.m. Anl. II ist nicht ausdrücklich bestimmt, ob die Verordnung über die Durchführung von Organtransplantationen[110] mit seiner Widerspruchsregelung noch in Kraft ist.

Es ist deshalb erfreulich, berichten zu können, daß nun ein von der Arbeitsgemeinschaft der Leitenden Medizinalbeamten erarbeiteter Entwurf für ein Transplantationsgesetz vorliegt, dem gem. § 3 Abs. 1 die sog. Informationslösung zugrunde liegt; d. h. in erster Linie wird für eine eventuelle Organentnahme der zu Lebzeiten geäußerte oder den Umständen nach zu vermutende Wille des Verstorbenen im Sinne des auch über den Tod hinaus weitergeltenden Persönlichkeitsrechts respektiert. Beim Fehlen einer Willensäußerung oder von

---

110 vom 4. Juli 1985, GBl. d. DDR I, S. 597; geändert am 5. August 1987, GBl. d. DDR I, S. 199

Anhaltspunkten dafür werden Verwandte über die beabsichtigte Organentnahme informiert und erhalten die Möglichkeit, innerhalb einer vereinbarten Frist stellvertretend für den Verstorbenen zu widersprechen. Laut Gesetzesbegründung soll die Organentnahme bei Personen ohne Angehörige oder Lebensgemeinschaft unterbleiben. Das ist ausdrücklich zu begrüßen.

Unklar bleibt nach dem Gesetzentwurf jedoch, wie der Wille des Verstorbenen dokumentiert sein muß, damit er Berücksichtigung findet. Als einzige Möglichkeit hierfür werden Organspendeausweise genannt, die gem. § 2 Abs. 2 durch Einwohnermelde- und Gesundheitsämter bereitzuhalten wären. Da diese zwischenzeitlich verlorengegangen sein können oder zum Zeitpunkt der Todesfeststellung nicht parat sind, ist deren Wert nur als begrenzt einzuschätzen. Insofern macht es Sinn, zusätzliche Möglichkeiten für die eindeutige Willensdokumentation des Verstorbenen in Erwägung zu ziehen.

Für die Organverteilung werden in § 5 des Entwurfs Verfahrensregelungen für Organempfänger und -spender vermischt; insofern ist der Gesetzentwurf nicht normenklar. Es wäre zweckdienlich, getrennte Regelungen für beide Fallgruppen in das Gesetz aufzunehmen, zumal eine Meldung des behandelnden Arztes über seinen organtransplantationsbedürftigen Patienten einer Befugnisnorm bedarf, während die Meldungen über Organspender als Verpflichtung vorgesehen sind, deren Unterlassung gem. § 11 Abs. 1 des Entwurfs eine Ordnungswidrigkeit darstellen würde.

Die getrennte Abhandlung der Organempfänger und -spender wäre auch in bezug auf die Datenübermittlung als notwendig gewesen. Sie erfolgt beim potentiellen Organempfänger als Teil des Behandlungsvertrages und ist daher datenschutzrechtlich als unproblematisch anzusehen. Beim lebenden Organspender bedarf es dafür im Regelfall seiner schriftlichen Einwilligung; diesbezüglich wäre das Gesetz unabdingbar zu ergänzen gewesen. Beim toten Organspender hingegen ist vor allem die genaue Festlegung des Übermittlungszeitpunktes zu fordern. Dies darf bei Information der Verwandten gem. § 3 Abs. 1 erst nach Ablauf der mit den Verwandten vereinbarten Frist erfolgen.

Der Entwurf, der nach Inkrafttreten eine abschließende Regelung wäre, regelt nicht den Umfang der notwendigen Meldungen an die zentrale Stelle (Stiftung Eurotransplant). Innerhalb eines internationalen Datenverbundes kommunizieren als Vertragspartner behandelnde Ärzte und die Stiftung Eurotransplant (für Organempfänger) bzw. Transplantationszentren und die Stiftung Eurotransplant (bei lebenden und toten Organspendern). Die vertraglich vorgesehene Vereinbarung, die in der Stiftung Eurotransplant gespeicherten Daten nach den Vorschriften des Bundesdatenschutzgesetzes zu schützen, wird höchstens partiell greifen, da die Datenübermittlung in einem übernationalem Datenverbund - z. Z. zwischen der Bundesrepublik Deutschland, den Beneluxländern und Österreich - geschieht. Nicht auszuschließen ist, daß sich in Zukunft weitere Länder unter der Regie von Stiftung Eurotransplant an der internationalen Organvermittlung für Transplantationszwecke beteiligen wollen. Selbst wenn es gelingen sollte, die vorgesehene ausschließliche Bezugnahme auf die Vorschriften des Bundesdatenschutzgesetzes gegenüber den beteiligten Ländern durchzusetzen, bedürfte es zusätzlich einer Einigung über eine für diesen übernationalen Datenverbund insgesamt zuständige Kontrollinstanz.

Die Ermächtigung der Länder in § 9 des Entwurfs zum Erlaß von Rechtsverordnungen über die Zusammenarbeit der Krankenhäuser läßt derzeitig nicht erkennen, welche Datenflüsse damit im einzelnen verbunden sein können.

7.3 Soziales

7.3.1 Kita-Beiträge bewegten erneut die Gemüter

Über die Festsetzung von Elternbeiträgen für Kindergartenplätze habe ich bereits in meinem 1. Tätigkeitsbericht unter 7.3 Stellung genommen. Nun ist das Thema erneut in den Schlagzeilen der Presse aufgetaucht. Das Jugendamt einer Stadtverwaltung hatte außer einer Glaubhaftmachung des Familiennettoeinkommens auch noch verlangt, u.a. Angaben zu Unterhaltsleistungen zu machen und dies anhand von Kopien über Gehalts- und Lohnabrechnungen, Lohnersatzleistungen usw. zu belegen. Dies löste bei den betroffenen Eltern Protestaktionen aus. Darüber informierte mich die Presse und bat um meine Stellungnahme.

Die Eltern sind grundsätzlich gem. §§ 97 a Abs. 1 i.V.m. 90 SGB VIII[111], § 17 Abs. 2 (Brandenburgisches) Kita-Gesetz[112] und der städtischen Gebührenordnung verpflichtet, ihr Einkommen im Rahmen des für die Berechnung des Elternbeitrages Erforderlichen preiszugeben. Das für die Beitragsfestsetzung vom Jugendamt zugrundegelegte "monatliche Familiennettoeinkommen" widerspricht aber dem Wortlaut der Gebührenordnung. Danach werden die monatlich bei den Eltern sich ergebenden Einkommensschwankungen nicht berücksichtigt, sondern ist das monatliche Durchschnitts-Nettoeinkommen maßgebend. Zur Ermittlung dieser Bemessungsgrundlage wird das bereinigte Jahreseinkommen der Eltern durch 11 geteilt. Für die Glaubhaftmachung der entsprechenden Angaben genügt es, daß die Eltern dem Jugendamt einmal im Jahr neutrale Bescheinigungen, z. B. Kopien von Einkommenssteuerbescheiden, auf denen die nicht erforderlichen Einzelangaben (z. B. über die Einkommensart) geschwärzt sind, vorlegen.

Deshalb habe ich gegenüber der Stadtverwaltung die monatliche Erhebung des Nettoeinkommens einschließlich seiner Herkunft beanstandet und gefordert, die von den Eltern gleichwohl eingereichten monatlichen Einkommensnachweise zu vernichten. Ferner beanstandete ich die Erhebung von Angaben über den Unterhaltspflichtigen bzw. über diejenigen Kinder, an die ein Erziehungsberechtigter Unterhalt zu zahlen hat, als unzulässig. Ebenfalls unzulässig war die Differenzierung nach Einkommensarten (z. B. Einkommen aus Arbeitsleistungen), da das Jugendamt aus diesen Angaben keine Konsequenzen für die Berechnung zieht und somit diese Angaben zur Gebührenerfassung nicht erforderlich sind. Des weiteren wies ich darauf hin, daß nach der Gebührenordnung keine Verpflichtung zur Angabe der zu leistenden Unterhaltsverpflichtungen besteht. Eine derartige Angabe ist nur zulässig, wenn sie freiwillig erfolgt.

7.3.2 Datenschutz bei der Beratung von Schwangeren

Nach der Entscheidung des Bundesverfassungsgerichts (BVerfG) zur Neuregelung des § 218 Strafgesetzbuch[113] ist die Straffreiheit eines Schwangerschaftsabbruchs dann verfassungsgemäß, wenn die Schwangere zuvor an einer Beratung teilgenommen hat, in der der Versuch unternommen wurden, sie für das Austragen des Kindes zu gewinnen. Dabei stellt das Gericht auf die Verpflichtung des Gesetzgebers ab, die Rechtslage insgesamt so zu gestalten, daß es für die Frau nicht naheliegt, die Beratung gar nicht erst anzunehmen und in die Illegalität auszuweichen. Bis zur Neuregelung der Bestimmungen über den Schwangerschaftsabbruch durch den Gesetzgeber hat das BVerfG deshalb mit Gesetzeskraft angeordnet, daß die schwangere Frau auf ihren Wunsch gegenüber der sie beratenden Person

---

111

112 i.d.F. der Bekanntmachung vom 3. Mai 1993, BGBl. I, S. 637

113 vom 10. Juni 1992, GVBl. I, S. 178

BVerfGE 88, 203; NJW 93, S. 1751 ff.

anonym bleiben kann[114]. Darüber hinaus sind mit der verfassungsgerichtlichen Anordnung folgende Vorgaben verbunden:

- Protokollierung des Beratungsgesprächs ohne Erhebung von Identitätsdaten der zu beratenden Schwangeren,

- Begrenzung der Empfänger der Angaben über den Schwangerschaftsabbruch und die dafür maßgeblichen Gründe.

Zur Umsetzung des Urteils habe ich gegenüber dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen einige datenschutzrechtliche Grundsätze für die Beratung der Schwangeren aufgestellt. Dabei habe ich darauf hingewiesen, daß die auf Wunsch der Schwangeren zu gewährleistende Anonymität der vorgeschriebenen Beratungen nicht durch die namentliche Bescheinigung über die Beratung unterlaufen werden darf.

Die Beratungsstellen haben bei der Beratung Schwangerer aus datenschutzrechtlicher Sicht folgende Grundsätze zu beachten:

- Aushängen von Hinweisen in der Beratungsstelle über das Recht auf anonyme Beratungen,

- Vergabe von Beratungsnummern zur Verwendung für Protokolle und Bescheinigungen,

- Ausstellung der Bescheinigung über vorgeschriebene Beratung durch eine andere als die beratende Person,

- Identifizierung für die Bescheinigung lediglich durch Vorlage des Personalausweises,

- befristete Aufbewahrung der Protokolle in der Beratungsstelle,

- keine namentliche Nennung der an der Beratung beteiligten Personen,

- Verpflichtung der Mitarbeiter in der Beratungsstelle zur Verschwiegenheit,

- keine Feststellung und Beurteilung einer Indikation durch den behandelnden Arzt,

- Verpflichtung zur Verschwiegenheit über die mit Einwilligung der Schwangeren bei der Staatsanwaltschaft erlangten Erkenntnisse, die für einen Antrag auf Leistungen der gesetzlichen Krankenversicherung nach den Beihilfevorschriften von Bedeutung sind.

Das Ministerium hat inzwischen einen Entwurf eines Rundschreibens mit datenschutzrechtlichen Grundsätzen für die Beraterinnen vorgelegt, in dem meine Vorschläge zum Teil Berücksichtigung finden. Ich habe ergänzend empfohlen, die Bestimmung hervorzuheben, daß der Name der Schwangeren nur auf der Bescheinigung über die Beratung sowie auf Vorlagen zur sozialen Unterstützung der Ratsuchenden zu vermerken ist und Kopien von den Bescheinigungen nicht gefertigt werden dürfen. Ferner sollten die Mitarbeiterinnen der Beratungsstellen in besonderer Weise zur Verschwiegenheit verpflichtet werden.

7.3.3 Behinderte - kein Recht auf Datenschutz?

Ein Landratsamt hat die Träger von Wohneinrichtungen für Behinderte im Rahmen der Vorbereitung einer Regionalkonferenz aufgefordert, für eine Belegungsplanung von neu zu

---

114 BVerfGE 88, 203 (211); BGBl. I 1993, S. 821 Ziff. 3 (4)

errichtenden Behindertenwohnstätten Listen über Behinderte mit Name, Vorname, Geburtsdatum, Art der Behinderung und Betreuer zu erstellen und verteilte sie an die Sitzungsteilnehmer. Das Diakonische Werk der Evangelischen Kirche hatte gegen ein derartiges Verfahren "erhebliche ethische und rechtliche Bedenken" und bat mich deshalb um eine "rechtliche Beratung".

Bei der Prüfung des Vorfalls zeigte sich, daß das Landratsamt keine Kenntnis über die für diesen Zweck vom Ministeriums für Arbeit, Gesundheit, Soziales und Frauen herausgegebene Erhebungsbögen hatte. Diese sahen ausdrücklich vor, bei der Erfassung dieses sehr sensiblen Personenkreises für Planungsaufgaben i.S.v. § 31 Bbg DSG lediglich Daten zu Behinderungsart und -grad, Herkunft (Kreis, Ort, Einrichtung) sowie Geschlecht und Alter zu verwenden. Darüber hinaus war dem Landratsamt nicht klar, daß mit einer Weitergabe derartiger Listen eine Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereiches erfolgen würde, die nur unter den in § 16 Bbg DSG genannten restriktiven Voraussetzungen zulässig ist. Diese Voraussetzungen lagen jedoch nicht vor. Dem Landratsamt habe ich empfohlen, für die Erstellung derartiger Listen künftig eine numerische Doppelanonymisierung (Einrichtung/fortlaufende Personenzahl) vorzugeben.

7.3.4 Weitergabe von Sozialdaten im Fall von Kindesmißhandlung

Anfang 1993 bat mich ein Landkreis darum, zur Frage der Zulässigkeit einer Übermittlung von Sozialdaten in Fällen sexuellen Mißbrauchs an Kindern aus datenschutzrechtlicher Sicht Stellung zu nehmen. Dabei war im wesentlichen zu prüfen, ob die Jugendämter berechtigt sind, in derartigen Verdachtsfällen der Staatsanwaltschaft oder der Polizei Mitteilung zu machen und ihnen ggf. auch Unterlagen zur Verfügung zu stellen.

Grundsätzlich unterliegen die Jugendämter als Leistungsträger dem Sozialgeheimnis gem. § 35 Abs. 1 SGB I und dürfen Sozialdaten nicht unbefugt offenbaren. Eine Offenbarung personenbezogener Daten ist gem. § 35 Abs. 2 SGB I nur unter den Voraussetzungen der §§ 67-77 SGB X zulässig. Bei den Vorschriften des Sozialgesetzbuches X handelt es sich um eine abschließende Regelung, nach der eine Offenbarung von Sozialdaten im vorliegenden Fall nur zulässig ist

- bei Vorliegen einer Einwilligung des Betroffenen (§ 67 Nr. 1 SGB X),
- auf richterliche Anordnung (§ 73 Nr. 2 i.V.m. § 72 Abs. 1 Satz 2 SGB X),
- soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch einen Leistungsträger erforderlich ist (§ 69 Abs. 1 Nr. 1 1. Alternative SGB X),
- soweit sie für die Durchführung eines damit zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens erforderlich ist (§ 69 Abs. 1 Nr. 1 2. Alternative SGB X).

Es gehört zu den Aufgaben der Jugendämter, Kinder und Jugendliche vor Gefahren für ihr Wohl zu schützen (§ 1 Abs. 3 SGB VIII) und dazu Mißhandlungen entgegenzuwirken. Daraus folgt jedoch keine Berechtigung der Jugendämter zur Erstattung von Strafanzeigen und zur (eigenmächtigen) Offenbarung von Sozialdaten gegenüber der Staatsanwaltschaft und der Polizei bei Verdacht eines sexuellen Mißbrauchs der Kinder und Jugendlichen. § 69 Abs. 1 Nr. 1 2. Alternative SGB X setzt voraus, daß bereits ein gerichtliches Verfahren anhängig ist. Er begründet daher keine Offenbarungsbefugnis im Rahmen behördlicher Verfahren, auch wenn diese zur Vorbereitung, aus Anlaß oder aufgrund eines gerichtlichen Verfahrens durchgeführt werden. Auf staatsanwaltschaftliche und polizeiliche Ermittlungsverfahren findet diese Vorschrift keine Anwendung.

Ich bin deshalb zu dem Ergebnis gekommen, daß die Jugendämter grundsätzlich nicht berechtigt sind, Sozialdaten der von ihnen betreuten Kinder und Jugendlichen in den Fällen eines möglichen sexuellen Mißbrauchs gegenüber der Staatsanwaltschaft und/oder der Polizei zu offenbaren. Allenfalls scheint es mir möglich zu sein, dem einzelnen Sozialarbeiter in extrem gelagerten Ausnahmefällen - für die nicht angenommen werden kann, daß der Gesetzgeber den in ihnen gegebenen Interessenkonflikt mit den §§ 67 ff. SGB X abschließend regeln wollte - eine Berufung auf den Rechtfertigungsgrund des § 34 Strafgesetzbuch zuzubilligen.

7.3.5 Datenschutz in Adoptionsangelegenheiten

Eine Petentin hatte mich gebeten, zu prüfen, ob es datenschutzrechtlich zulässig sei, daß ein Jugendamt dem Adoptivvater eine Ablichtung des Adoptionsbeschlusses übergibt, obgleich bei der Scheidung der Adoptivmutter das alleinige Sorgerecht für das Adoptivkind übertragen worden war. Die Petentin hielt dies im Hinblick auf den im Adoptionsbeschluß enthaltenen Geburtsnamen des Adoptivkindes und mit Rücksicht auf dessen psychische Situation für nicht datenschutzgerecht.

Zunächst war festzustellen, daß die Tätigkeit des zum Bereich der Jugendhilfe gehörenden Jugendamtes gem. § 61 Abs. 1 SGB VIII[115] insgesamt unter den Schutz des Sozialgeheimnisses fällt. § 67 SGB VIII räumt jedoch auch in Verfahren der Jugendhilfe jedem Betroffenen ein Recht auf Auskunft über die zu seiner Person in Akten oder auf sonstigen Datenträgern gespeicherten Daten ein. Da der Adoptionsbeschluß nicht nur die Rechtsstellung des Kindes dokumentierte, sondern zugleich auch die des Adoptivvaters, handelte es sich um auch auf dessen Person bezogene Daten.

Dem Adoptivvater ging es jedoch nicht um Auskunft, sondern um die Herausgabe einer Ablichtung des Beschlusses. Im Sinne eines erweiterten Auskunftsrechts kann Auskunft grundsätzlich auch durch Übergabe einer Kopie erteilt werden, wenn schutzwürdige Interessen Dritter dadurch nicht beeinträchtigt werden können. Im Hinblick auf § 1758 Abs. 1 des Bürgerlichen Gesetzbuches (BGB), der ausdrücklich eine Offenbarung von Tatsachen untersagt, die geeignet sind, die Annahme und ihre Umstände aufzudecken, lag diese Voraussetzung jedoch nicht vor. Eine Kopie des Adoptionsbeschlusses war vielmehr überaus geeignet, die Annahme des Kindes Dritten gegenüber aufzudecken. Unter diesen Umständen konnte sich ein Anspruch des Adoptivvaters auf eine Ablichtung des Adoptionsbeschlusses aus datenschutzrechtlichen Bestimmungen nicht ergeben, da diese nur die Erteilung einer Auskunft über die zu seiner Person gespeicherten Daten in der Weise zuließen, daß dadurch personenbezogene Daten Dritter nicht offenbart wurden.

Die Petentin war jedoch darauf hinzuweisen, daß sich - unter Berücksichtigung auch der zivilprozessualen Bestimmungen - ein solcher Anspruch aus den Vorschriften des Bürgerlichen Rechts ergeben konnte. So ist beispielsweise gem. § 56e des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG)[116] der Beschluß, durch welchen das Gericht die Annahme als Kind ausspricht, den Annehmenden zuzustellen. Der Adoptionsvater begehrte also nur die Ablichtung einer Urkunde, die ihm als annehmendem Vater ebenso zustand wie der annehmenden Mutter. Außerdem hätte es sein können, daß der Adoptivvater eine Aufhebung des Adoptionsbeschlusses beantragen wollte (vgl. §§ 1759 ff. BGB). Insoweit war nicht zu sehen, weshalb ihm das Jugendamt nicht im Wege einer

---

115

116 vom 26. Juni 1990, BGBl. I, S. 1163

vom 17. Mai 1898, RGBl., i. d. Fassung d. Bekanntmachung vom 20. Mai 1898, RGBl., S. 771, zuletzt geänd. 22. Juli 1993, BGBl. I, S. 1282

pflichtgemäßen Ermessensentscheidung eine Ablichtung sollte zur Verfügung stellen dürfen, auch wenn ein entsprechender Anspruch des Adoptivvaters gegenüber dem Jugendamt nicht bestand und gegen die Adoptivmutter oder an das Gericht hätte gerichtet werden müssen.

Der Petentin war deshalb mitzuteilen, daß das Datenschutzrecht im vorliegenden Fall nicht vor einer etwaigen Gefährdung des Kindeswohls durch einen möglicherweise verantwortungslosen Umgang des Adoptivvaters mit einer Ablichtung des Adoptionsbeschlusses schützen konnte. Insoweit hätte die Adoptivmutter ggf. nur auf etwaige zivilrechtliche Unterlassungsansprüche ihres Kindes zurückgreifen können.

7.3.6 Übermittlung von Kraftfahrzeughalterdaten von der Zulassungsstelle des Straßenverkehrsamtes an das Sozialamt

Ein Landkreis fragte an, ob zur Prüfung der Anspruchsberechtigung bei Sozialhilfeleistungen an Asylbewerber ermittelt werden dürfe, ob sie als Kraftfahrzeughalter bei der Zulassungsstelle des Straßenverkehrsamtes registriert seien.

Da gem. § 88 Bundessozialhilfegesetz (BSHG)[117] das gesamte verwertbare Vermögen, d. h. auch eigene Kraftfahrzeuge, bei der Frage der Sozialhilfeberechtigung zu berücksichtigen ist, war ein Abgleich mit dem Fahrzeugregister grundsätzlich als geeignet zur Überprüfung der Berechtigung anzusehen. Ich habe jedoch festgestellt, daß allerdings das Straßenverkehrsgesetz (StVG)[118] als bereichsspezifische Regelung in § 35 i.V.m. § 32 StVG eine Übermittlung der gespeicherten Halterdaten an Behörden zur Erfüllung der Aufgaben des Empfängers nur zuläßt, soweit dies zugleich im Rahmen der Zweckbestimmung und Aufgabenstellung der Fahrzeugregister erforderlich ist. Da die vom Sozialamt beabsichtigte Prüfung aber weder zu den im Straßenverkehrsgesetz genannten Aufgaben zählte noch zu einem der darin bezeichneten Zwecke erfolgen sollte, wäre eine Übermittlung der gespeicherten Halterdaten unzulässig gewesen.

In gleicher Weise hat sich in diesem Zusammenhang auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 47. Sitzung am 09./10.03.1994 in Potsdam für die Wahrung des Sozialgeheimnisses ausgesprochen (s. Anlage 19).

7.3.7 Erteilung einer Erlaubnis zur Heimbetreibung

Für Personen, die eine Erlaubnis zur Betreibung eines Heimes erlangen wollen, sieht § 6 Heimgesetz[119] eine Überprüfung der Zuverlässigkeit vor. In diesem Zusammenhang wandte sich das Landesamt für Soziales und Versorgung mit der Bitte an das Ministerium für Arbeit, Soziales, Gesundheit und Frauen, unbeschränkte Auskünfte aus dem Bundeszentralregister (BZR) anzufordern und diese an das Landesamt weiterzuleiten. Daraufhin bat mich das Ministerium um Stellungnahme dazu, ob gegen das Weiterleiten der unbeschränkten Registerauskunft aus datenschutzrechtlicher Sicht Einwände beständen.

Ich habe dem Ministerium mitgeteilt, daß das Landesamt für Soziales und Versorgung gem. §

117

118 vom 10. Januar 1991, BGBl. I, S. 94, berichtigt S. 808

vom 19. Dezember 1952, BGBl. I, S. 837, zuletzt geänd. 27.
119 Dezember 1993, BGBl. I, S. 2378

in der Fassung der Bekanntmachung vom 23. April 1990, BGBl. I, 1873

31 Bundeszentralregistergesetz (BZRG)[120] berechtigt sei, für eine bestimmte Person mit deren Kenntnis selbst ein behördliches Führungszeugnis zu beantragen. Dagegen sind nur die im Gesetz enumerativ aufgezählte Behörden - dazu zählen u.a. die obersten Landesbehörden - gem. § 41 Abs. 1 Nr. 2 BZRG privilegiert, eine uneingeschränkte Auskunft aus dem Bundeszentralregister zu erhalten. Auskünfte, die über das behördliche Führungszeugnis hinausgehende Informationen betreffen, dürfen gem. § 43 BZRG deren nachgeordneten oder ihrer Aufsicht unterstehenden Behörden nur mitgeteilt werden, "wenn dies zur Vermeidung von Nachteilen für das Land unerläßlich ist oder wenn anderenfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde".

Dies trifft für den Personenkreis nach § 6 Heimgesetz nicht zu. Ich habe deshalb dem zuständigen Ministerium folgende Vorgehensweise empfohlen: Ergeben sich aus einer uneingeschränkten Registerauskunft Hinweise darauf, daß die betroffene Person zur Betreibung eines Heimes nicht geeignet ist, so sollte nur dies dem Landesamt für Soziales und Versorgung mitgeteilt werden; Einzelangaben aus dem Registerauszug dürfen dagegen nicht übemittelt werden. Mit diesem Verfahren wird ein sachgerechter Ausgleich zwischen dem Anliegen des Heimgesetzes und dem Recht auf informationelle Selbstbestimmung erreicht. Allerdings wird ein Antrag des Ministeriums an das Bundeszentralregister auf unbeschränkte Registerauskunft zur Überprüfung der Zuverlässigkeit des Betreibers gem. § 6 Heimgesetz nur in besonders gelagerten Ausnahmefällen und unter den übrigen Voraussetzungen des § 31 BZRG in Betracht kommen, da ein solcher Registerabgleich vom Heimgesetz grundsätzlich nicht vorgesehen und in der Regel auch nicht erforderlich ist.

7.4. Landesversicherungsanstalt Brandenburg

7.4.1 Angabe von Heilstätten gegenüber dem Arbeitgeber

Arbeitnehmer erhalten bei der Bewilligung einer Kur gem. § 7 Abs. 2 Lohnfortzahlungsgesetz[121] zur Vorlage beim Arbeitgeber zunächst eine allgemeine Bestätigung hierüber und später ein Einberufungsschreiben bzw. die Entlassungsmitteilung. Je nach Abfassung der Formulare (mit und ohne Angabe der Heilstätte) ist es einem Personalarbeiter anhand der Behandlungsstätte bzw. sogar allein aufgrund des Behandlungsortes möglich, Rückschlüsse auf die behandelte Erkrankung zu ziehen.

Eine diesbezügliche Eingabe habe ich zum Anlaß genommen, bei der Landesversicherungsanstalt Brandenburg (LVA) anzuregen, künftig dem Arbeitnehmer auf Wunsch eine neutrale Bescheinigung über Kurbeginn und -ende auszustellen. Sie hat mir daraufhin mitgeteilt, daß ihrerseits bereits beim Verband Deutscher Rentenversicherungsträger ein Antrag auf generelle Änderung des Programms gestellt und damit meinem datenschutzrechtlichen Anliegen Rechnung getragen worden sei.

7.4.2 Erstattungsforderung wegen überzahlter Rentenleistungen

Eine Petentin fragte bei mir an, ob die Landesversicherungsanstalt nach dem Datenschutzgesetz berechtigt sei, "die Fragen laut beigefügtem Vordruck in einer Rentenangelegenheit einzuholen". Auf dem Vordruck fehlte der nach § 12 Abs. 3 Bbg DSG vorgeschriebene Hinweis auf die Rechtsgrundlage der Datenerhebung.

---

120 vom 21. September 1984, BGBl. I, S. 1229, ber. 1985, I, S. 195

121 vom 27. Juli 1969, BGBl. I, S. 946, zuletzt geändert am 20. Dezember 1988, BGBl. I, S. 2477

Im übrigen war, wie sich später herausstellte, der Petentin zuvor mitgeteilt worden, daß der gem. Art. 40 §§ 1 und 2 Rentenüberleitungsgesetz (RÜG)[122] fast ein Jahr lang vorschußweise gezahlte Sozialzuschlag in der Annahme gewährt worden sei, daß ihr monatliches Gesamteinkommen einen vom Gesetz vorgegebenen Beitrag unterschreite. Bei der Erstellung des zwischenzeitlich erlassenen Umwertungs- und Anpassungsbescheids habe sich jedoch diese Zahlungsvoraussetzung nicht bestätigt. Es sei zahlungstechnisch nicht möglich gewesen, die unrechtmäßigen Zahlungen einzustellen. Deshalb war es zu Überzahlungen gekommen, die nunmehr von der Landesversicherungsanstalt Brandenburg gem. § 42 Abs. 2 SGB I zurückgefordert wurden.

Darauf hatte die Petentin zunächst nicht reagiert und deshalb ein Erinnerungsschreiben mit dem oben erwähnten Vordruck erhalten. Dabei wurde sie in einem Anschreiben darauf hingewiesen, daß "bei der Verwirklichung erhobener Erstattungsforderungen" gem. § 24 Abs. 1 SGB X auch die wirtschaftlichen Verhältnisse des Betroffenen zu berücksichtigen seien. Der zugesandte Fragebogen sei für die vom Gesetz dazu vorgesehene Anhörung vor allem bei Härtefällen gedacht.

Dagegen waren aus datenschutzrechtlicher Sicht keine Einwendungen zu erheben. Die LVA mußte, bevor sie den Rückforderungsbescheid gem. § 42 Abs. 2 SGB I erließ, gem. § 24 Abs. 1 SGB X der Petentin Gelegenheit geben, sich zu den für die Rückforderung maßgebelichen Tatsachen zu äußern. Zu diesem Zweck war der Petentin der Fragebogen zugesandt worden, mit dem ihre für den Erstattungsanspruch relevanten wirtschaftlichen Verhältnisse insbesondere im Hinblick auf die Voraussetzungen eines sog. Härtefalls erfragt werden sollten. Die Fragen hielten sich im Rahmen des Erforderlichen. Deshalb war nur zu beanstanden, daß der Fragebogen in formaler Hinsicht nicht den Anforderungen nach § 12 Abs. 3 Bbg DSG entsprach.

8 Umwelt, Naturschutz und Raumordnung

8.1 Bundesumweltinformationsgesetz

Der Rat der Europäischen Gemeinschaft hat am 07. Juni 1990 die Richtlinie 90/313/EG über den freien Zugang zu Informationen über die Umwelt erlassen, die von den Mitgliedsstaaten bis zum 31.12. 1992 in nationales Recht umzusetzen war. Die Richtlinie soll im Interesse eines wirksamen Umweltschutzes für jeden den freien Zugang zu den im Besitz der öffentlichen Verwaltung befindlichen Informationen und die regelmäßige Unterrichtung der Öffentlichkeit über den Zustand der Umwelt sicherstellen. Der vorgenannten Umsetzungspflicht ist der Bundestag bisher nicht nachgekommen. Es liegt derzeit lediglich der im Oktober 93 vom Bundeskabinett beschlossene Entwurf eines Umweltinformationsgesetzes vor.

Da in den Verwaltungsvorgängen der Umweltbehörden eine Vielzahl personenbezogener Daten enthalten sind, ist es Aufgabe des Gesetzgebers, den Anspruch auf freien Zugang zu Umweltinformationen in Einklang zu dem Grundrecht auf informationelles Selbstbestimmungsrecht der betroffenen natürlichen Personen zu bringen. Bei der dabei gebotenen Interessensabwägung wird zu berücksichtigen sein, inwieweit der in den Verwaltungsvorgängen erwähnte Betroffene durch die Offenbarung seiner personenbezogenen Daten in seinen Rechten tangiert wird und in welchem Umfang die Kenntnis gerade der personenbezogenen Daten für die Verfolgung der umweltpolitischen Zielsetzung erforderlich ist. Dabei ist in dem Gesetzesentwurf unter anderem zur Entlastung der Verwaltung vorgesehen, daß Betriebs- und Geschäftsgeheimnisse vom Betriebsinhaber

122 vom 15. Juli 1991, BGBl. I, S. 1606

als solche zu kennzeichnen sind, damit sie von der Verwaltung entsprechend behandelt werden. Diese Kennzeichnungsregelung soll ab dem 01. Januar 1993 gelten, also ab dem Ablauf der Umsetzungsfrist der EG-Richtlinie.

Vor dem Hintergrund der Aufnahme eines allgemeinen Einsichtsnahmerechtes des Bürgers in Behördenakten und andere amtliche Unterlagen[123] sowie eines Zugangsrechts zu Umweltinformationen[124] in der Verfassung des Landes Brandenburg habe ich mich gegenüber dem Minister für Umwelt, Naturschutz und Raumordnung dafür eingesetzt, daß in dem vorliegenden Entwurf des Umweltinformationsgesetzes dem Landesgesetzgeber die Möglichkeit eingeräumt wird, über die Bestimmungen des vorgelegten Gesetzesentwurfs hinausgehende Regelungen zu erlassen. Eine entsprechende Öffnungsklausel sollte eingefügt werden.

Darüber hinaus halte ich die Einrichtung eines Beauftragten für den freien Zugang zu Umweltinformationen für empfehlenswert. Dessen beratende und rechtswahrende Aufgaben könnten dem jeweiligen Landesbeauftragten für Datenschutz übertragen werden.

Zudem ist der Beginn der Kennzeichenregelung des Gesetzesentwurfs zur Vermeidung datenschutzrechtlich unzulässiger Offenbarungen von Betriebs- und Geschäftsgeheimnissen auf den Zeitpunkt des Inkrafttretens des Gesetzes zu verschieben. Da vor dem Inkrafttreten eine Kennzeichnung in der Regel unterblieben ist, besteht ansonsten die Gefahr einer Nichtberücksichtigung der Betriebs- und Geschäftsgeheimnisse durch die Verwaltung.

Der derzeit diesen Bereich regelnde Erlaß des Ministers für Umwelt, Naturschutz und Raumordnung zur Umsetzung der EG-Richtlinie über den freien Umgang zur Information über die Umwelt[125] ist als Übergangsregelung und vorläufige Orientierungshilfe für die schwierige Rechtsabwägung seitens der öffentlichen Stellen des Landes bei der Einsichtsgewährung in Umweltakten zu begrüßen (s. 1. Tätigkeitsbericht unter 9.1). Der Bundesgesetzgeber bleibt jedoch dessen ungeachtet aufgefordert, die erforderliche bundeseinheitliche gesetzliche Grundlage zur Regelung des freien Zugangs zu Informationen über die Umwelt zu schaffen.

8.2 Abfallbegleitscheinverfahren

Zur optimalen Erfassung und Kontrolle der Ströme von besonders überwachungsbedürftigen Abfällen und Reststoffen beteiligt sich das Land Brandenburg gemeinsam mit weiteren 12 Bundesländern an einer Entwicklung eines DV-gestützten Verfahrens für die Sonderabfall- und Reststoffüberwachung (Begleitscheinverfahren).

Dazu werden beim für den Vollzug der Abfall- und Reststoffüberwachungsverordnung (AbfRestÜberwV)[126] zuständigen Landesumweltamt Brandenburg - einschließlich seiner beiden Außenstellen in Frankfurt/Oder und Cottbus - Stammdaten zu den Abfallerzeugern, Beförderern und Abfallentsorgern und -verwertern erhoben. Diese werden mit den bei der Erfassung der Begleitscheine anfallenden Daten abgeglichen. Als Datenaustausch ist dabei vor allem der Austausch sämtlicher Stamm- und Begleitscheindaten zwischen dem

---

123 Verfassung des Landes Brandenburg vom 20. August 1992, GVBl. I, S. 298, Art. 21 Abs. 4 BbgVerf

124 Art. 39 Abs. 7 Satz 2 BbgVerf

125 vom 14. Januar 1993, ABl., S. 462

126 vom 3. April 1990, BGBl. I, S. 648

Landesumweltamt Brandenburg und den genannten Außenstellen in Frankfurt/Oder und Cottbus einerseits und einem länderübergreifenden Austausch der Daten der Begleitscheine sowie wesentlicher Daten zu Entsorgungs- und Verwertungsanlagen zwischen den entsprechenden Knotenstellen - als Datensammel- und Verteilungsstelle - andererseits beabsichtigt. Die Funktion der Knotenstelle hat im Land Brandenburg das Landesumweltamt Potsdam.

Es handelt sich bei dem geplanten "Begleitscheinverfahren" vom Aufbau her um eine konkrete Umsetzung der §§ 13 ff. AbfRestÜberwV. Die besonderen Bedingungen, an die die Weitergabe der Sonderabfalldaten zu knüpfen ist, müssen dabei noch genau definiert werden.

Eine Anmeldung des Verfahrens nach der Dateienregisterverordnung[127] steht noch aus.

8.3 Datenschutzverordnung für den Bereich Immissionsschutz

Mit der Vorlage eines Entwurfes einer Datenschutzverordnung für den Bereich Immissionsschutz Ende August 1993 konnte ich dem Ministerium für Umwelt, Naturschutz und Raumordnung (MUNR) zwar bestätigen, begrüßenswerte detaillierte Ansätze zu einer Datenschutzregelung in einem zunehmend gesellschaftsrelevanten Problemkreis gefunden zu haben. Jedoch nimmt der Entwurf die Vorgaben von § 20 Abs. 1 und 2 Vorschaltgesetz zum Immissionsschutz (LImSchG)[128] lediglich in ihrer Gliederung auf. Die erforderliche materielle Regelung des Rechts auf informationelle Selbstbestimmung, die das Vorschaltgesetz erwähnt, fehlen. Dieses sind

- Einzelnennung der zu verarbeitenden Daten mit Zuordnung zur jeweiligen Zweckbestimmung,

- klare Übermittlungsregelungen betreffend die jeweils beteiligten Behörden bei eindeutiger Zuordnung des jeweiligen Aufgabenzwecks,

- Pflicht der Betroffenen zur Erteilung von Auskünften,

- Auskunftsrechte Betroffener und

- Voraussetzung und Fristen für die Löschung gespeicherter Daten.

So hatte ich eine Reihe von Änderungsvorschlägen und Anmerkungen zu unterbreiten. Hier sollen nur einige wesentliche Kritikpunkte genannt sein:

- Es werden vom Bbg DSG abweichende und daher mißverständliche Begriffe für die einzelnen Datenverarbeitungsschritte verwendet (z. B. "Aufnahme" statt "Speichern").

- Es findet eine unsystematische und bereits insoweit unzulässige Vermischung von Aufgabenzwecken, Datenquellen und Erhebungsanlässen als Rechtfertigung für die Erhebung und Speicherung personenbezogener Daten statt, als das LImSchG eindeutig von einzelnen (unterschiedlichen) Verwendungszwecken ausgeht.

- Es ist für die Wahrnehmung sämtlicher Aufgaben aller für den Immissionsschutz zuständigen Behörden eine Datenspeicherung in einem Gesamtdatenbestand vorgesehen,

---

127

128 vom 19. November 1992, GVBl. II, S. 726
vom 3. März 1992, GVBl. I, S. 78

auf den unüberschaubar zugegriffen werden kann und bei dem Löschungen nur nach unscharfen Kriterien erfolgen sollen. Da der Entwurf im übrigen Detailregelungen zur Löschung bestimmter Daten noch ausklammert, läuft dies auf eine unbegrenzte und insoweit unzulässige Datenvorratsspeicherung hinaus.

- Nicht normenklar und daher unzulässig ist die Ausweitung der Definition für personenbezogene Daten[129] auf Betriebsdaten, sofern diese in "Ausnahmefällen" über Umweltauswirkungen einen Personenbezug zulassen.

- Zu allgemein ist die Befugnis, Informationen über Personen mit besonderen betrieblichen Funktionen wie Immissionsschutz-, Störfall- und Strahlenschutzbeauftrage im Rahmen auch künftiger Arbeitsverhältnisse austauschen zu können, ohne daß zumindest eine Information hierüber an sie vorgesehen ist; in diesem Zusammenhang fehlt auch die Sicherstellung, daß Löschungs- und Sperrfristen an anderer Stelle (etwa im Bundeszentralregister) nicht unterlaufen werden.

- Für den Fall des unterstützenden Einsatzes von privaten Dritten ist lediglich deren Verpflichtung auf das Amtsgeheimnis nach dem Verpflichtungsgesetz vorgesehen. Damit ist jedoch z. B. im Fall der Datenverarbeitung im Auftrag nicht einmal den Erfordernissen gem. § 11 Bbg DSG (Unterwerfungsklausel, Meldepflichten, Duldung von Kontrollmaßnahmen) Rechnung getragen; ein entsprechender Hinweis fehlt.

- Es ist nicht normenklar geregelt, welche Behörde rechtlich nachvollziehbar die Güterabwägung vornimmt, ob bedarfsweise Informationen an die Öffentlichkeit personenbezogen oder in anonymisierter Form, vorgenommen werden, "wenn das Interesse des Betroffenen am Schutz seiner Persönlichkeit das öffentliche Interesse sowie die Interessen Dritter an einer vollständigen Bekanntgabe der personenbezogenen Daten überwiegt".

- Die vorgesehene Dokumentation von Übermittlungen von Akten muß durch ein adäquates Verfahren bei Dateien (Protokollierung) ergänzt werden.

- Es ist der "Bedarfsmangel" als Kriterium für eine Löschung von personenbezogenen Daten vorgesehen. Dies birgt - ungeachtet der Unbestimmtheit des Begriffs - die Gefahr einer unerlaubten Vorratshaltung von Daten, entspricht nicht dem Erforderlichkeitsprinzip und ist daher unzulässig.

- Die Stellen, denen personenbezogene Daten übermittelt worden sind, sollen von deren Löschung oder Sperrung nur dann unterrichtet werden, wenn dies nicht "einen erheblichen Aufwand erfordern würde". Dies stellt kein hinreichendes Regulativ zu dem bei der Erhebung und Speicherung ohne weiteres betriebenen erheblichen Aufwand dar.

- Es ist vorgesehen, daß die Auskunftserteilung an Betroffene von der Zustimmung der Staatsanwaltschaft und Polizei abhängig gemacht wird, wenn die personenbezogenen Daten von dort stammen. Dies ist nicht hinnehmbar. Da diese Daten erlaubt im Bereich des Umweltschutzes genutzt werden (sollen), muß sichergestellt sein, daß diese Behörden auch die rechtlich nachprüfbare Güterabwägung vornehmen.

Wegen der Vielzahl auch grundsätzlicher datenschutzrechtlicher Bedenken gegen den vorgelegten Entwurf hatte ich angeboten, Details auch in direktem Gedankenaustausch zu besprechen. Ein erstes Gespräch beim MUNR im November 1993 zeigte, daß damals dort noch verhältnismäßig geringe Neigung bestand, meinen Anregungen und Empfehlungen zu

---

129 vgl. § 3 Abs. 1 Bbg DSG

folgen. Weitere schriftliche Einlassungen in der Angelegenheit liegen mir bislang nicht vor.

9 Ernährung, Landwirtschaft und Forsten

9.1 Das integrierte Verwaltungs- und Kontrollsystem

Das integrierte Verwaltungs- und Kontrollsystem (InVeKos) der Europäischen Union (EU) soll dazu dienen, einen Mißbrauch von EG-Fördermitteln im Agrarbereich festzustellen und zu verhindern. Zu diesem Zweck hat die EU ihre Mitgliedsstaaten dazu verpflichtet, in jedem Mitgliedsland eine Datenbank nach einheitlichen Kriterien zu errichten, in der alle Landwirte erfaßt werden, die an bestimmten Förderungsmaßnahmen teilnehmen. Bestandteil dieser Datenbank ist insbesondere eine lückenlose Erfassung der Flächen der betroffenen Landwirte und der Flächenutzungsart (u.a. Ölsaaten, Getreide, Mais und Brachland) über mehrere Jahre; ferner werden Daten zur wirtschaftlichen Situation der Betriebe erfaßt. Alle förderungsrelevanten Informationen werden automatisiert verarbeitet. Die landwirtschaftlichen Flächen müssen nach einheitlichen Kriterien so bezeichnet werden, daß eine Kontrolle der angegebenen Nutzungsarten auch durch einen Vergleich mit Satellitenaufnahmen möglich wird. Nach Auskunft des Ministeriums für Ernährung, Landwirtschaft und Forsten (MELF) ist allerdings eine Satellitenüberwachung in Brandenburg nicht geplant. Die Überprüfungen sollen auf Feldkontrollen vor Ort beschränkt bleiben. Die EU macht die Bewilligung von Mitteln von der Einführung und Anwendung des InVeKos in den Mitgliedsstaaten abhängig.

Da im Bereich der EU ein Landwirt schwerlich ohne die Inanspruchnahme von Fördermitteln der EU wird existieren können, wird das integrierte Verwaltungs- und Kontrollsystem im Ergebnis zu einer lückenlosen Erfassung der Landwirte in einer Datenbank führen.

Grundsätzlich sind auch aus datenschutzrechtlicher Sicht keine Einwendungen dagegen zu begründen, daß die Bewilligung von Subventionen in kaum noch vorstellbarer Größenordnung durch die EU mit wirksamen Kontrollen gegen den Subventionsmißbrauch und -betrug einhergehen sollen. Es ist jedoch nicht zu übersehen, daß die EU mit dem integrierten Verwaltungs- und Kontrollsystem den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet hat, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot widersprechen kann, da insbesondere die einschlägigen Verordnungen der EU[130] für die Kontrolldichte lediglich ein Mindestmaß an Kontrollen, jedoch keine Obergrenze festsetzen. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 46. Konferenz am 26./27. Oktober 1993 in Berlin in einer Entschließung zum integrierten Verwaltungs- und Kontrollsystem hingewiesen und geeignete systembeschränkende Maßnahmen zur Vermeidung unverhältnismäßiger Einschränkungen des Rechts auf informationelle Selbstbestimmung der betroffenen Landwirte gefordert (s. Anlage 12).

Aus datenschutzrechtlicher Sicht ist insbesondere zu beanstanden, daß die vielfältigen detaillierten und unübersichtlichen Regelungen der EU zu InVeKos keinesfalls dem verfassungsrechtlichen Gebot der Normenklarheit entsprechen. Eine weitere verfassungsrechtliche Problematik ergibt sich daraus, daß mit InVeKos eine planmäßige Datenerhebung auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken

---

130 VO (EWG) Nr. 3508/92 des Rates vom 27. November 1992 (ABl. der Europäischen Gemeinschaften Nr. L 355/1 vom 5. Dezember 1992) und VO (EWG) Nr. 3887/92 der Kommission vom 23. Dezember 1992 (ABl. der Europäischen Gemeinschaften Nr. L 391/36 vom 31. Dezember 1992)

betrieben wird, die nach den Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil[131] unzulässig ist.

Da reduzierte, das heißt auf das Maß des jeweils tatsächlich Erforderlichen beschränkte Angaben der Landwirte in den Förderanträgen zu einer Minderung oder gänzlichen Ablehnung der Beihilfen durch die EU führen, ergibt sich die insgesamt unbefriedigende Situation, daß auch die Landwirte in Brandenburg nur wählen können zwischen einem Verzicht auf die für sie notwendigen Beihilfen der EU und einer übermäßigen Beeinträchtigung ihres Grundrechts auf informationelle Selbstbestimmung.

Anlaß bestand darauf hinzuweisen, daß nach Maßgabe der oben genannten InVeKos-Verordnungen der EU sich die Kontrollkompetenzen der EU auf die Kontrolle der Einführung des integrierten Verwaltungs- und Kontrollsystems in den Ländern beschränken. Eine Kontrolle der einzelnen Landwirte in Brandenburg kann nur durch die brandenburgischen Behörden erfolgen. Hinzuweisen war auch darauf, daß im Rahmen des InVeKos die Übermittlung erhobener personenbezogener Daten an die EU nur in aggregierter Form erfolgen darf.

Bei der Umsetzung der InVeKos-Verordnungen der EU im Land Brandenburg war zunächst zu beanstanden, daß ich vom Ministerium für Ernährung, Landwirtschaft und Forsten an der Erstellung des technischen Konzepts und seiner Umsetzung nicht beteiligt worden war. In der Folge hat jedoch die weitere Zusammenarbeit mit dem Ministerium eine ausgesprochen positive und sachdienliche Entwicklung genommen.

Das *technische Konzept, das zur Umsetzung von InVeKos in Brandenburg* zur Anwendung kommt, läßt sich zusammengefaßt wie folgt beschreiben:

Die automatisierte Verarbeitung der Anträge und die Vorbereitung der Auszahlung der Fördermittel erfolgt nach einem einheitlichen Konzept mit dem modular entwickelten Programmsystem PROFIL in zwei Stufen ("PROFIL-Amt" und "PROFIL-Land"). Die landwirtschaftlichen Betriebe stellen ihre Anträge bei den zuständigen Kreisverwaltungen. Hier erfolgt die Datenerfassung, eine Plausibilitätskontrolle und eine Bearbeitung bis zur Bewilligung der Fördermittel (Bescheid). Die Daten werden auf Disketten ausgegeben und über Kurierdienst dem Landesamt für Ernährung, Landwirtschaft und Flurneuordnung (LELF) zugestellt. Das LELF aggregiert die Daten aller Kreise, bereitet die Zahlbarmachung an die Bundeskasse vor, führt Auswertungen durch und ermittelt statistische Daten, die auch an das Bundesamt für Ernährung und Forsten übermittelt werden.

In den Kreisämtern und im LELF liegen Dienstanweisungen vor, die für Transparenz, modifizierte Zugriffsmöglichkeiten und den Schutz der personenbezogenen Daten bei der Datenverarbeitung sorgen sollen. Bei den Programmen wurde Wert auf differenzierte Nutzung je nach Aufgabengebiet (z.B. Erfasser, Fertigmelder, Systemverwalter) gelegt. Die Programmentwicklungen sind z.Z. noch nicht abgeschlossen. Nach dem bisherigen Stand läßt sich das technische Konzept der praktischen Umsetzung des InVeKos im Land Brandenburg jedoch insgesamt als grundsätzlich vertretbar beurteilen. Allerdings ist bislang eine umfassende datenschutzrechtliche Überprüfung des eingesetzten automatisierten Datenverarbeitungssystems durch meine Behörde nicht erfolgt. Lediglich eine erste Prüfung der automatisierten Datenverarbeitung (vernetzte DOS-PC unter Novell Netware) und eine stichprobenartige Einsicht in die Erfassungsunterlagen und Prüflisten für Klein- und Großerzeuger in einem Landkreis gaben mir keine Veranlassung zu wesentlichen Beanstandungen.

---

131 BVerfGE 65, 1 (46)

Auch bei der Gestaltung der Formulare für den Antrag auf Agrarförderung 1994 bin ich hinzugezogen worden. Es ging im wesentlichen darum, durch entsprechende Hinweise zu den maßgeblichen Bestimmungen des Brandenburgischen Datenschutzgesetzes die Datenerhebung nach Prinzip, Verfahren und Zweck für den Antragsteller so transparent wie möglich zu gestalten.

9.2 Tierseuchenkasse

Mit Inkrafttreten des Gesetzes zur Ausführung des Tierseuchengesetzes (AGTierSGBbg)[132] wird auch im Land Brandenburg eine Tierseuchenkasse für zu zahlende Entschädigungsleistungen aufgebaut, an die gem. § 1 Abs. 1 der Verordnung zur Durchführung dieses Gesetzes (DVO-AGTierSGBbg)[133] alle Besitzer von Pferden, Rindern, Schweinen, Schafen, Ziegen und Geflügel als Pflichteinrichtung jährlich Beiträge entsprechend ihrem Viehbestand zu entrichten haben. Hierbei sind die Ämter und amtsfreien Gemeinden gem. § 6 Abs. 3 AGTierSGBbg zur Mitwirkung in Bezug auf die Erhebung, Speicherung und Übermittlung von Namen und Adressen der Tierbesitzer an die Tierseuchenkasse verpflichtet. Daraufhin werden die Tierbesitzer von der Tierseuchenkasse zur Festlegung von Beiträgen angeschrieben und dazu um Mitteilung ihrer Tierbestände gem. § 1 Abs. 2 und 3 der Verordnung über die Beiträge an die Tierseuchenkasse des Landes Brandenburg (TSK-Beitrags-VOBbg)[134] veranlaßt. Das Meldeformular der Tierseuchenkasse enthält keinen Vermerk über die gesetzliche Grundlage der Erhebung und ist damit datenschutzrechtlich zu beanstanden.

Auf Nachfragen meinerseits zum Meldeverfahren hat das Ministerium für Ernährung, Landwirtschaft und Forsten eingeräumt, daß die Speicherung von Namen und Adressen der Tierbesitzer in den Ämtern und amtsfreien Gemeinden über die Erstmeldung an die Tierseuchenkasse hinaus nicht notwendig wäre. Die Mitwirkungspflicht gem. § 6 Abs. 3 AGTierSGBbg beträfe ausschließlich die Aufbauphase der Tierseuchenkasse und später nur noch die Öffentlichkeitsarbeit in Form von ortsüblichen, allgemeinen Bekanntmachungen zur jährlichen Tierbestandsmeldung. Daher könnten einmal erhobene Daten gem. § 19 Abs. 2 Satz 1 Buchst. b Bbg DSG wieder gelöscht werden. Desgleichen wurde eingeräumt, daß wenn gem. § 1 Abs. 3 TSK-Beitrags-VOBbg Fehlmeldungen bei der Tierseuchenkasse eingehen, die Daten von Tierbesitzern gem. § 19 Abs. 2 Satz 1 Buchst. b Bbg DSG zu löschen seien. Bei einer Novellierung des AGTierSGBbg und der DVO-AGTierSGBbg wäre eine diesbezügliche Klarstellung angebracht.

9.3 Übermittlung einer Betriebsliste landwirtschaftlicher Betriebe

Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MAGSF) hatte das Ministerium für Landwirtschaft, Ernährung und Forsten (MELF) um die Übermittlung einer Betriebsliste landwirtschaftlicher Betriebe gebeten, die es zur Ausübung arbeitsschutzrechtlicher Befugnisse verwenden wollte. Das MELF bat mich daraufhin um eine datenschutzrechtliche Beurteilung des Übermittlungsbegehrens.

Bei meiner Stellungnahme bin ich zu dem Ergebnis gekommen, daß eine Übermittlung der Betriebsliste unzulässig wäre. Gemäß § 14 Abs. 1 Satz 1 Bbg DSG ist die Übermittlung personenbezogener Daten an andere öffentliche Stellen nur zulässig, wenn sie zur

---

[132]

[133] vom 2. März 1993, GVBl. I, S. 58

[134] vom 8. April 1993, GVBl. II, S. 204
vom 8. April 1993, GVBl. II, S. 206

rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und darüber hinaus die weiteren Voraussetzungen des § 13 Abs. 1 Satz 2 oder 3 oder des Abs. 2 Satz 1 Bbg DSG vorliegen.

Da die Übermittlung nicht der Erfüllung von Aufgaben des MELF dienen sollte, war nur zu prüfen, ob sie zur rechtmäßigen Erfüllung der Aufgaben des MAGSF erforderlich war. Bereits dies war zu verneinen, denn selbst wenn die Betriebsliste zur Erfüllung der in § 139 b Gewerbeordnung (GewO)[135] gesetzlich bestimmten Aufgaben erforderlich gewesen wäre, so weist doch diese Bestimmung die dort bezeichneten Aufgaben nicht dem Ministerium, sondern den Gewerbeaufsichtsbehörden, im gegebenen Fall den Ämtern für Arbeitsschutz und Sicherheitstechnik, zu. Gemäß § 4 der Verordnung über die Gewerbeaufsichtsbehörden[136] führt das MAGSF lediglich die Dienst- und Fachaufsicht über die Gewerbeaufsichtsbehörden. Im übrigen wäre gemäß dem Grundsatz der unmittelbaren Datenerhebung beim Betroffenen mit seiner Kenntnis (§ 12 Abs. 2 Bbg DSG) sowie den entsprechenden Wertungen der Regelungen in § 139 b Abs. 5 a und 7 GewO auch eine Übermittlung der Liste an die Ämter für Arbeitsschutz und Sicherheitstechnik nicht zulässig gewesen.

Das MELF hat mir mitgeteilt, daß entsprechend meiner Stellungnahme eine Übermittlung der Betriebsliste nicht erfolgt sei.

9.4 Pflanzenschutzsachkundeverordnung

Nach § 9 des Pflanzenschutzgesetzes[137] sind gewerbliche Anwender von Pflanzenschutzmitteln verpflichtet, vor Beginn ihrer Tätigkeit diese der zuständigen Landesbehörde anzuzeigen. Für das Land Brandenburg ist dafür gemäß § 1 der Brandenburgischen Pflanzenschutzsachkundeverordnung[138] das Landesamt für Ernährung, Landwirtschaft und Flurneuordnung (LELF) zuständig.

Das Ministerium für Ernährung, Landwirtschaft und Forsten hatte mich gebeten, das Formblatt der Anzeige und den Aufbau des Registers bezüglich der Verwendung von personenbezogenen Daten zu beurteilen. Der Hinweis der Behörde auf dem Formblatt zur automatisierten Speicherung der Daten zum Zweck der Registerführung wurde auf meine Empfehlung hin präzisiert. Die Streichung von personenbezogenen Daten aus dem Register bei Unternehmen, die ihre anzeigepflichtige Tätigkeit eingestellt haben, wurde auf mein Anraten in dem Entwurf der "Verwaltungsvorschrift für die Führung eines Registers zur Erfassung von Unternehmen, die Pflanzenschutzmittel für andere anwenden" geregelt. Damit bestanden aus datenschutzrechtlicher Sicht keine Bedenken mehr gegen diese Verwaltungsvorschrift.

10 Stadtentwicklung, Wohnen und Verkehr

---

135 Neubekanntmachung der GewO vom 1. Januar 1978, BGBl. I, S. 97 i. d. seit 1. Januar 1987 gültigen Fassung

136 vom 5. September 1990, GBl. d. DDR I, S. 1433

137 vom 15. September 1986, BGBl. I, S. 1505, zuletzt geänd. am 26. Januar 1993, BGBl. I, S. 278

138 vom 13. September 1993, GVBl. II, S. 638

10.1 Wohnungsbauförderung

Im Rahmen der Beratungen des Entwurfs eines Wohnungsbauförderungsgesetzes 1994 bestehen Überlegungen zu einer Ausgestaltung einer einkommensabhängigen Wohnungsbauförderung. Dabei ist die Erhebung und Verarbeitung von personenbezogenen Daten in einem Dreiecksverhältnis zwischen Mieter-Vermieter-Wohnungsfinanzierungsstelle geplant. So ist vorgesehen, daß der Staat an den Vermieter eine Aufwendungshilfe oder Zusatzförderung zahlt. Die Höhe der erforderlichen Aufwendungshilfen soll nach den jeweiligen Einkommensverhältnissen errechnet und die Zusatzförderung an den Vermieter monatlich ausgezahlt werden. Der Vermieter kann dabei aus der Höhe der Zahlungen Rückschlüsse auf das Einkommen und die Einkommensentwicklung seines Mieters ziehen. Einzelheiten der Datenbekanntgabe und Übermittlung sollen diesbezüglich in einer Vereinbarung mit dem Mieter geregelt werden.

Eine solche einkommensabhängige Wohnungsbauförderung erscheint im Hinblick auf den Schutz der personenbezogenen Daten des Mieters äußerst bedenklich. So muß schon die Zweckmäßigkeit und Erforderlichkeit einer derart umfassenden, immer wiederkehrenden Datenerhebung und Datenverarbeitung angesichts des Verwaltungsaufwandes, der zur Festlegung der ortsüblichen Vergleichsmiete und sozialverträglichen Wohnungskostenbelastung und zur Erhebung der Einkommen der Mieter betrieben werden muß, bezweifelt werden.

Kernproblem des geplanten Vorhabens ist jedoch, daß der Vermieter aus der Höhe der an ihn überwiesenen Förderung einen datenschutzrechtlich abzulehnenden Einblick in die Einkommensverhältnisse seiner Mieter (und deren Mitbewohner - soweit deren Einkommen bei der Berechnung mit berücksichtigt wird -) erhält, der über das für die Durchführung des Mietverhältnisses erforderliche Maß hinausgeht und mit möglichen Nachteilen für den Mieter verbunden ist.

Ebenso genügt die vorgesehene Vereinbarung mit dem Mieter über die Verarbeitung seiner personenbezogenen Daten nicht der für eine solche Einwilligung zu fordernden Freiwilligkeit. Denn im Hinblick auf die derzeitige Wohnungsnot und die existenzielle Bedeutung des Wohnraumes befindet sich der Mieter beim Abschluß der vorgesehenen Vereinbarung in einer faktischen Zwangssituation, die eine freiwillige Einverständniserklärung in die Verarbeitung seiner personenbezogenen Daten ausschließt.

Gegenüber dem Ministerium für Stadtentwicklung, Wohnen und Verkehr habe ich die Berücksichtigung dieser datenschutzrechtlichen Bedenken gegen eine derartige einkommensabhängige Wohnungsbauförderung, insbesondere bei der Beratung des Entwurfs eines Wohnungsbauförderungsgesetzes 1994, gefordert.

10.2 Bauaufsichtsämter in Bedrängnis

Im Berichtszeitraum hatte sich eine Kreisverwaltung an mich gewandt, weil sie in Zweifel war, ob die Bekanntgabe von erteilten Baugenehmigungen an Baustellenverlage rechtens sei. Hintergrund der Anfrage war, daß bestimmte Baustellenverlage (Baustelleninformationsdienste) die Bauaufsichtsämter der Kreisverwaltungen damit unter Druck setzten, daß sie auf andere Ämter verwiesen, die ihnen die gewünschten Unterlagen bereits gegen Kostenentschädigung überlassen hätten und daß sie im Verweigerungsfall mit Schadensersatzforderungen drohten. Das Gesetz über die Bauordnung (BauO)[139] enthält keine entsprechende bereichsspezifische Regelung für die Datenübermittlung der erteilten

---

139 vom 20. Juli 1990, GBl. d. DDR I, S. 929

Baugenehmigungen, so daß als Rechtsgrundlage im vorliegenden Fall das Brandenburgische Datenschutzgesetz in Betracht kommen kann.

Grundsätzlich ist eine Datenübermittlung nach § 4 Abs. 1 Bbg DSG nur zulässig, wenn das Bbg DSG oder ein anderes Gesetz sie erlaubt oder wenn der Betroffene eingewilligt hat. Für die Übermittlung von Baugenehmigungen und die in ihnen enthaltenen personenbezogenen Daten an Privatfirmen sind die Voraussetzungen nach § 16 Abs. 1 Buchst. d, der einzig hier in Betracht kommenden Rechtsgrundlage, nicht erfüllt. Nach dieser Bestimmung ist die Datenübermittlung an nicht-öffentliche Stellen zulässig, wenn der Empfänger ein berechtigtes Interesse an der Datenübermittlung geltend macht und der Betroffene dem nicht widersprochen hat.

Die Datenübermittlung der erteilten Bauherrengenehmigungen ist daher unter den Voraussetzungen des § 4 Abs. 1 Buchst. b und Abs. 2 Bbg DSG mit Einwilligung des Betroffenen zulässig. Eine Einwilligung des Betroffenen liegt vor, wenn dieser auf dem Bauantragsformular angekreuzt hat, daß er damit einverstanden ist, daß personenbezogene Daten über ihn an Dritte, z. B. Baustelleninformationsdienste, weitergegeben werden. Im Fall einer Einwilligung des Betroffenen ist vor der Übermittlung zu prüfen, ob der Empfänger den Voraussetzungen, die das Bauantragsformular an ihn stellt, entspricht.

In denjenigen Fällen, in denen Betroffene auf ihren Bauantragsformularen angekreuzt haben, daß sie mit einer Übermittlung nicht einverstanden sind, sowie in den Fällen, in denen nichts angekreuzt wurde, muß die Übermittlung unterbleiben, da nach § 4 Abs. 2 Bbg DSG die Einwilligung der Schriftform bedarf. Kreuzt der Betroffene weder "ja" noch "nein" an, äußert er überhaupt keinen Willen, so daß ein wesentliches Merkmal einer Willenserklärung fehlt. Daraus folgt, daß auch in diesen Fällen nicht übermittelt werden darf.

Die Überprüfung der Bauantragsformulare ergab, daß bei einem Formular nicht eindeutig ersichtlich ist, an wen die Daten übermittelt werden. Ich habe angeregt, nur ein Formular zu verwenden, dem der Antragsteller entnehmen kann, an wen die Daten übermittelt werden, wenn er mittels Ankreuzen seine Zustimmung zur Übermittlung erteilt.

Die Überprüfung der Bekanntgabe von erteilten Baugenehmigungen an einen Baustelleninformationsdienst in einem Bauaufsichtsamt ergab, daß das Verfahren nicht zu beanstanden war. Das Bauaufsichtsamt hat nur diejenigen Bauanträge übermittelt, auf denen die Einwilligung ausdrücklich vermerkt war. Durch Einblick in die Gewerbeanmeldung hat das Bauaufsichtsamt darüber hinaus geprüft, ob der Baustelleninformationsdienst den Anforderungen entsprach.

11 Finanzen

11.1 Telekommunikationsverbund der obersten Landesbehörden

Im März 1993 wandte sich die Arbeitsgemeinschaft der Haupt- und Personalräte der Landesregierung, des Landtages und des Landesrechnungshofes mit der Bitte an mich, zu dem Entwurf einer Dienstvereinbarung über die Nutzung der ISDN-Telekommunikationsanlage des Telekommunikationsverbundes der obersten Landesbehörden (DV) Stellung zu nehmen, weil sie darin erhebliche Möglichkeiten zur Personen- und Leistungskontrolle gegeben sahen. Erst dies veranlaßte das Finanzministerium, an mich heranzutreten und mich noch für eine aktive Mitwirkung bei der Erstellung und Verabschiedung eines Erlasses einer Verwaltungsvorschrift über die Errichtung und Benutzung dienstlichen Telekommunikationsanlagen für die Verwaltung des Landes

Brandenburg (DAV)[140] und der DV zu gewinnen.

Was war geschehen? Nach längerer Planungs- und fast abgeschlossener Bauphase sollte im April 1993 ein Telekommunikationsverbund der obersten Landesbehörden, der im wesentlichen alle in Potsdam ansässigen Ministerien der Landesregierung und die Staatskanzlei miteinander verbindet, in Betrieb genommen werden. Das Finanzministerium war mit der Ausarbeitung der DAV und DV beauftragt worden und noch vor Inbetriebnahme des Telekommunikationsverbundes sollten beide in Kraft gesetzt werden. Den zuständigen Mitarbeitern war nicht bekannt, daß gem. § 23 Abs. 2 Bbg DSG meine Behörde über Planungen des Landes zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten ist, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen. Dabei verstehe ich unter einer rechtzeitigen Unterrichtung eine durchgehende Einbeziehung von Beginn der Planungsphase an. Daß dies Sinn macht, wird an diesem Beispiel deutlich. Die Versäumnisse des Finanzministeriums hatten für die Steuerzahler des Landes Brandenburg finanzielle Folgen. So mußten beispielsweise aufgrund unumgänglicher nachträglicher Forderungen aus der Sicht des Datenschutzes nicht nur Änderungen in der Software zur Gebührendatenverarbeitung vorgenommen werden, sondern auch Teile der bereits gekauften Hardware (wie beispielsweise die technischen Einrichtungen zur Drohanrufaufzeichnung) mußten ungenutzt bleiben, da ihre Inbetriebnahme wegen fehlender gesetzlicher Grundlagen nicht datenschutzgerecht gewesen wäre.

Nach sehr zeitaufwendigen, jedoch letztendlich fruchtbaren Gesprächen in erster Linie mit den zuständigen Mitarbeitern des Finanzministeriums, aber auch mit Vertretern der Haupt- und Personalräte der Landesregierung, des Landtages und des Landesrechnungshofes sowie verantwortlichen Vertretern des Auftragnehmers für den TK-Verbund lagen im August 1993 Entwürfe der DAV und DV vor, die weitgehend dem personenbezogenen Datenschutz Rechnung tragen. Im wesentlichen waren folgende Änderungen erreicht worden:

- Die Gebührendatenverarbeitung wurde dahingehend verändert, daß bei Dienstgesprächen keine Speicherung von Verbindungsdaten mehr erfolgt, sondern nur noch die Gebühren je Kostenstelle ermittelt werden.

- Bei der Abrechnung von Privatgesprächen besteht für den Einzelnen die Möglichkeit, je Nebenstelle zu wählen, ob alle Verbindungsdaten mit der um die letzten drei Ziffern verkürzten Zielrufnummer oder nur die Gesamtgebühren gespeichert werden.

- Zur Überprüfung von Dienstgesprächen dürfen nur die Verbindungsdaten von ausgewählten Nebenstellen und Stichproben registriert werden, die im voraus zufällig ausgewählt worden sind.

- Das Leistungsmerkmal "Aufschalten" darf nur von der Telefonzentrale genutzt werden. Die ursprünglich geplante Zuweisung dieses Leistungsmerkmals auch für Minister, Staatssekretäre und Abteilungsleiter wurde gestrichen.

- Die vorhandenen technischen Einrichtungen zur Drohanrufaufzeichnung werden nicht in Betrieb genommen.

11.2 Kündigung wegen angeblicher Verletzung des Datenschutzes

Gelegentlich tritt der Fall auf, daß versucht wird, unter dem Deckmantel des Datenschutzes Probleme zu lösen, die mit ihm nichts zu tun haben. In einer Sparkasse war einer

140 vom 30. November 1993, ABl., S. 1775

Mitarbeiterin mit der Begründung gekündigt worden, sie hätte bei der Dateneingabe in den Rechner Sicherheitsbestimmungen des Datenschutzes verletzt. Dieser Vorwurf veranlaßte die Mitarbeiterin, sich an mich zu wenden.

Anhand der Rechnerprotokolle konnte ich keine Datenschutzverletzungen durch die Petentin feststellen. Die Geschäftsführung mußte zugeben, daß die der ehemaligen Mitarbeiterin vorgeworfenen Verstöße gegen den Datenschutz nicht gerechtfertigt sind. Auch enthielt der zwischenzeitlich abgeschlossene Vergleich bezüglich ihrer Beurteilung nur positive Äußerungen.

11.3 Aus dem Bereich der Ämter zur Regelung offener Vermögensfragen

11.3.1 Regelungen zur Datenverarbeitung

Klärungsbedürftig waren in mehreren Fällen die Befugnisse der Ämter zur Regelung von offenen Vermögensfragen (ÄROV) sowie der Anspruchssteller zur Verarbeitung personenbezogener Daten nach § 31 Vermögensgesetz (VermG)[141].

So war darauf hinzuweisen, daß § 31 Abs. 2 VermG nur die Übermittlung personenbezogener Daten von den Vermögensämtern an Verfahrensbeteiligte regelt, d. h. an solche Personen und Stellen, deren rechtliche Interessen durch den Ausgang des Restitutionsverfahrens berührt werden können und die deshalb im Falle eines Prozesses von dem Gericht gem. §§ 63, 65 Verwaltungsgerichtsordnung (VwGO)[142] beigeladen werden könnten. Eine Übermittlung an andere öffentliche oder private Stellen wird durch diese Bestimmung nicht zugelassen.

Als unzulässig war deshalb insbesondere auch die Übermittlung von Angaben über Restitutionsanträge an die *Lastenausgleichsämter* zu beurteilen, zu denen diese die Vermögensämter in Brandenburg mehrfach aufgefordert haben. Eine Rechtsgrundlage dafür soll erst mit der nach Art. 10 Ziff. 12 des Entwurfs eines Entschädigungs- und Ausgleichsleistungsgesetzes beabsichtigten Ergänzung des § 27 VermG geschaffen werden. Nach der bis heute gültigen Gesetzeslage sind die Lastenausgleichsämter nach Maßgabe der Regelung im Lastenausgleichsgesetz (LAG)[143] darauf verwiesen, sich gemäß dem Grundsatz der unmittelbaren Datenerhebung beim Betroffenen mit dessen Kenntnis an die Betroffenen selbst zu wenden. Lediglich im Ausnahmefall ist eine Übermittlung personenbezogener Daten an die Lastenausgleichsämter gem. § 14 Abs. 1 Satz 1 in Verbindung mit § 13 Abs. 2 Satz 1 Buchst. c Bbg DSG dann zulässig, wenn sich für die ÄROV aus dem einzelnen Ersuchen der Lastenausgleichsämter ohne weiteres ergibt, daß der Betroffene gegenüber dem Lastenausgleichsamt unzutreffende Angaben gemacht haben muß. Dies kann grundsätzlich nur dann der Fall sein, wenn sich aus dem Ersuchen der Lastenausgleichsämter ergibt, daß von dort bereits bei dem Betroffenen angefragt wurde.

Das Landesamt zur Regelung offener Vermögensfragen (LAROV) hat inzwischen die ÄROV angewiesen, bis zu einem Inkrafttreten der Neufassung des § 27 VermG - außer in extrem gelagerten Ausnahmefällen wie offensichtlichen Betrugsversuchen o.ä. - keine personenbezogenen Daten an die Lastenausgleichsämter zu übermitteln.

141

142 vom 3. August 1992, BGBl. I, 1446

143 i.d. Fassung der Bekanntmachung vom 19. März 1991, BGBl. I, S. 686, zuletzt geänd. 11. Januar 1993, BGBl. I, S. 50 vom 1. Oktober 1969, BGBl. I, S. 1909, zuletzt geänd. 21. Dezember 1992, BGBl. I, S. 2094

Als auch vom LAROV selbst so bezeichnete "rechtlich nicht haltbare Praxis" war die Verwendung eines Formschreibens zu beanstanden, mit dem ein AROV u. a. einer *Wohnungsbaugesellschaft* mitteilte, bei der Durchführung des Verwaltungsverfahrens entsprechend dem Gesetz zur Regelung offener Vermögensfragen sei gem. § 31 Abs. 4 VermG das Vermögensamt berechtigt, vom Rechtsträger bzw. staatlichen Verwalter umfassende Auskunft über das Grundstück zu fordern. Zur Erreichung dieses Zweckes sei es erforderlich, daß den Bevollmächtigten der Antragsteller Zutritt zu dem Grundstück und Einsicht in die Verwaltungsunterlagen gewährt werde. In einem Fall baten die Anspruchsteller auf der Grundlage dieses Schreibens die Wohnungsbaugesellschaft um Kopien der für das betroffene Grundstück abgeschlossenen Mietverträge.

Diese Vorgehensweise widersprach gerade dem Wortlaut und dem Regelungszweck des § 31 Abs. 3 und 4 VermG. Danach haben die Anspruchssteller im Restitutionsverfahren nur über das AROV - dem der Gesetzgeber dadurch bewußt eine Filterfunktion zugewiesen hat - Anspruch auf Auskunft über alle Informationen, die zur Durchsetzung ihrer Ansprüche nach dem Vermögensgesetz erforderlich sind. Der Auskunftsanspruch der Anspruchssteller richtet sich somit nur gegen das AROV. Der Auskunftsanspruch des AROV gegenüber dem gegenwärtigen Rechtsträger (§ 31 Abs. 4 VermG) kann wegen der vom Gesetzgeber gewollten Filterfunktion des AROV nur von diesem selbst und nur in der Weise geltend gemacht werden, daß Auskunft an das Vermögensamt verlangt wird. Nur dann, wenn ein Antrag auf Rückgabe eines Unternehmens gestellt wurde, hat die Behörde dem Anspruchssteller eine Begehung der Geschäftsräume und Einsicht in alle Geschäftsunterlagen zu gewähren, die für seinen Antrag von Bedeutung sein können.

Der Wohnungsbaugesellschaft war deshalb zu empfehlen, mit Hinweis auf die mangelnde Berechtigung der Anspruchssteller gem. § 31 Abs. 3 und 4 VermG die Übermittlung personenbezogener Daten abzulehnen, zumal sie dadurch gegen ihre vertraglichen Verpflichtungen gegenüber ihren Mietern verstoßen hätte.

Der dargestellten Rechtslage widerspricht auch die verbreitete Praxis der ÄROV, bereits aus verfahrensökonomischen Gründen dem Anspruchssteller Auskunft meist in der Weise zu erteilen, daß es ihm Einsicht in die Akten gewährt oder Ablichtungen aus diesen zur Verfügung stellt.

Zwar ist dies auch aus datenschutzrechtlicher Sicht nicht grundsätzlich unzulässig. Denn zum einen hat der Gesetzgeber mit der Regelung in § 31 Abs. 3 Satz 1 VermG nicht das *Recht auf Akteneinsicht* ausschließen oder einschränken, sondern vielmehr den Informationsanspruch insgesamt und ggf. auch über ein bloßes Akteneinsichtsrecht hinaus erweitern wollen. Ferner ist zu berücksichtigen, daß die Vorgänge beim AROV im Falle eines Verwaltungsrechtsstreits zu den dem Gericht vorzulegenden Akten gehören würden, in die der Anpruchsteller dann als Prozeßbeteiligter gem. § 100 Abs. 1 VwGO Einsicht nehmen könnte, und daß die Regelung im § 31 Abs. 3 Satz 1 VermG nicht beabsichtigt, den Anspruchsteller auf den Rechtsweg zu verweisen. Und schließlich ist auch der Aspekt der gebotenen "Waffengleichheit" zwischen Antragsteller und betroffenem Rechtsträger zu sehen: Nach Maßgabe von § 31 Abs. 2 und Abs. 7 VermG in Verbindung mit § 29 Verwaltungsverfahrensgesetz (VwVfG)[144] steht auch dem betroffenen Rechtsträger ein Akteneinsichtsrecht zu. Ein Grund für eine Ungleichbehandlung wäre insoweit nicht ersichtlich.

Damit ergibt sich jedoch für die Regelung in § 31 Abs. 3 und 7 VermG zugleich, daß der Gesetzgeber mit ihr in Ansehung des Rechts auf Akteneinsicht auch keine Besserstellung des Anspruchsstellers beabsichtigt hat, sondern dessen Rechtsstellung nur insoweit erweitert

144 vom 26. Februar 1993, GVBl. I, S. 26

wurde, als ihm zusätzlich zu seinem Akteneinsichtsrecht ein darüber hinausgehender Anspruch auf Auskunft durch das AROV über alle zur Durchsetzung seines Restitutionsanspruchs erforderlichen Informationen eingeräumt wurde. Dies bedeutet: § 31 Abs. 3 Satz 1 VermG bestimmt in Hinblick auf das Akteneinsichtsrecht des Anspruchsstellers nichts anderes als § 29 VwVfG, auf den § 31 Abs. 7 somit uneingeschränkt verweist. Daraus folgt, daß auch im Restitutionsverfahren Umfang und Inhalt des Akteneinsichtsrechts für alle Verfahrensbeteiligte in gleicher Weise nach § 29 VwVfG zu bestimmen sind.

Nach § 29 Abs. 1 Satz 1 VwVfG besteht das Recht auf Einsicht in die das Verfahren betreffenden Akten jedoch grundsätzlich nur insoweit, als deren Kenntnis zur Geltendmachung oder Verteidigung der rechtlichen Interessen dessen, der die Einsicht begehrt, erforderlich ist. Ferner können nach Maßgabe von § 29 Abs. 2 Satz 1 VwVfG auch in diesem Fall die berechtigten Interessen anderer Verfahrensbeteiligter oder dritter Personen der Akteneinsicht entgegenstehen.

Für die Akteneinsicht des Anspruchsstellers im Restitutionsverfahren bedeutet dies: Das AROV darf ihm Einsicht nur in solche Unterlagen gewähren, die für die Durchsetzung seines Restitutionsanspruchs von Bedeutung sind. Sind in diesen Unterlagen mit anspruchsrelevanten Informationen weitere personenbezogene Daten derart verbunden, daß eine Trennung nicht möglich ist oder vom AROV nicht vorgenommen wird, so darf das AROV dem Anspruchssteller grundsätzlich nur Auskunft erteilen. Die Gewährung von Akteneinsicht ist in diesen Fällen nur zulässig, wenn keine Anhaltspunkte dafür bestehen, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden könnten. Dies wird jedoch nur ausnahmsweise der Fall sein, denn grundsätzlich ist davon auszugehen, daß der Betroffene mit einer Bekanntgabe seiner personenbezogenen Daten, die er dem AROV zur Verteidigung seiner Rechte mitgeteilt hat, an den Anspruchssteller nicht einverstanden ist, sondern sie lediglich im Umfang der Anspruchberechtigung des Anspruchsstellers duldet. Diese Berechtigung wird jedoch durch das rechtliche Interesse des Anspruchsstellers gem. § 31 Abs. 3 Satz 1 VermG begrenzt. Jede Weitergabe personenbezogener Daten durch die ÄROV an den Anspruchssteller über die Grenzen seiner Berechtigung hinaus, die ohne Einwilligung der Betroffenen gem. § 4 Abs. 2 Bbg DSG erfolgt, ist deshalb eine rechtswidrige Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung, die der Betroffene nicht hinzunehmen braucht.

Die Praxis der ÄROV bei der Gewährung von Akteneinsicht steht deshalb mit den genannten Vorschriften über den Datenschutz nicht in Einklang. Aus datenschutzrechtlicher Sicht ist daher zu fordern, daß den ÄROV die Rechtslage und ihre entsprechenden Verpflichtungen gem. § 31 Abs.3, 4 und 7 VermG noch einmal erläutert und sie nachdrücklich zur Wahrung der rechtlichen Grenzen des Akteneinsichtsrechts angewiesen werden. Dabei wird zu betonen sein, daß auch bei der Gewährung von Akteneinsicht Zweckmäßigkeitsaspekte nur im Rahmen der durch das Gesetz bestimmten Rechtmäßigkeit berücksichtigt werden können und insbesondere auch der Gesichtspunkt der Verfahrensökonomie nicht dazu führen darf, daß die vom Gesetzgeber ausdrücklich gewollte Filterfunktion der ÄROV bei der Information der Anspruchssteller im Restitutionsverfahren nicht ausgeübt wird.

Hintergrund dieser datenschutzrechtlichen Prüfung waren *Eingaben*, denen als Sachverhalt zugrunde lag, daß zumeist - veranlaßt durch die nach § 31 Abs. 2 VermG erfolgende Unterrichtung über den Restitutionsantrag - die betroffenen Rechtsträger, insbesondere die gegenwärtigen Mieter der Wohnungen, gegenüber dem AROV zu dem Antrag Stellung genommen und dabei oft zahlreiche und sehr persönliche Informationen aus ihrem privaten Lebensbereich mitgeteilt hatten. Diese dem AROV praktisch aufgedrängten "Familiengeschichten" können regelmäßig von den für den Restitutionsanspruch relevanten Angaben nicht getrennt werden und gelangen deshalb bei einer Gewährung von Akteneinsicht auch dem Anspruchsteller zur Kenntnis. Kommt es dann später - z.B. gem. § 31 Abs 5 VermG - zu Verhandlungen zwischen den Beteiligten, so sind die Betroffenen

häufig unangenehm vom Kenntnisstand des Antragstellers überrascht. Wie oben dargelegt, hätte dem Anspruchsteller in diesen Fällen regelmäßig nur Auskunft erteilt, nicht jedoch Akteneinsicht gewährt werden dürfen. Anläßlich einer Eingabe habe ich diese Problematik bereits vor längerer Zeit an das Landesamt zur Regelung offener Vermögensfragen herangetragen. Eine Stellungnahme des LAROV ist jedoch bislang nicht erfolgt.

In einem anderen Fall hatte die Wohnungsbaugesellschaft die Mieterin aufgefordert, den Mietzins künftig nicht mehr an sie, sondern an die Alteigentümerin zu zahlen, der das Grundstück bestandskräftig rückübertragen worden sei. Gegenüber der Eigentümerin berief sich die Mieterin auf eine Empfehlung des Ministeriums für Stadtentwicklung, Wohnen und Verkehr und machte die Zahlung der Miete davon abhängig, daß ihr die Eigentümerin den Rückübertragungsbescheid vorlege. Die Eigentümerin beschwerte sich bei mir über die von der Gemeinde verbreitete Empfehlung des Ministeriums. Den Bescheid des AROV wollte sie ihrer Mieterin nicht vorlegen, da in ihm eine Vielzahl personenbezogener Angaben enthalten sei, die die Mieterin nichts angingen. Ich habe der Petentin mitgeteilt, daß das Verlangen der Mieterin nach einem Nachweis ihrer Berechtigung grundsätzlich berechtigt sei, und habe ihr empfohlen, sich von dem AROV eine Bescheinigung ausstellen zu lassen, in der lediglich die bestandskräftige Rückübertragung des Eigentums bestätigt wird. Eine Rückfrage beim LAROV zur Regelung offener Vermögensfragen ergab, daß dieses Verfahren auch der verwaltungsinternen Weisungslage entspricht.

In einer weiteren Stellungnahme, die auf die Anfrage eines Trägers der Sozialversicherung hin erfolgte, war eine Befugnis des AROV zur Übermittlung personenbezogener Daten, die die anfragende *Krankenkasse* zur Ermittlung ihrer beitragspflichtigen Mitglieder nutzen wollte, zu verneinen, da es dafür an einer Rechtsgrundlage fehlt. Der nicht in meinem Zuständigkeitsbereich ansässige Träger der Sozialversicherung hat mir zwischenzeitlich mitgeteilt, daß weitere Anfragen seiner Einrichtung an die ÄROV in Brandenburg nicht erfolgten, da sie bereits aus anderen Gründen auch gar nicht erforderlich seien.

11.3.2 Technisch-organisatorische Mängel

Anläßlich von Kontrollbesuchen bei zwei ÄROV war festzustellen, daß die Sicherheitsmaßnahmen dort insgesamt unzureichend waren. So fehlte es beispielsweise an einer angemessenen Außensicherung wie z. B. einer Ausstattung von Fenstern und Türen mit einbruchshemmenden Materialien oder einer Installation von Alarmanlagen. Ferner fehlten verschließbare Schränke zur Lagerung der Vorgänge bei den Sachbearbeitern, Schutzvorkehrungen gegen unbefugtes Betreten der Arbeitsräume in den Ämtern sowie eine verschließbare brandsichere Lagerungsmöglichkeit für die regelmäßig gefertigten Sicherheitsabzüge von der Datenbank. Es gab keine Dienstvorschrift zur Verarbeitung personenbezogener Daten. Die Mitarbeiter waren nicht auf das Datengeheimnis gem. § 6 Bbg DSG verpflichtet. Dieser Umstand wog um so schwerer, als festzustellen war, daß die Zuverlässigkeit der Mitarbeiter praktisch den einzigen Schutz vor einer mißbräuchlichen Verwendung der personenbezogenen Daten in den Ämtern darstellte. So hatte aus den genannten Gründen faktisch jeder Mitarbeiter Zugang zu allen Akten. Ferner konnte jeder Nutzer nach Eingabe eines persönlichen Paßwortes über seinen eigenen Arbeitsplatzcomputer auf alle in der zentralen Datenbank enthaltenen Informationen zugreifen. Das System registrierte in einer Protokolldatei die An- und Abmeldungen der Nutzer. Im Gebrauch der Datenbestände unterlagen die Sachbearbeiter deshalb praktisch keinerlei Einschränkungen.

Nicht alle dieser Mängel können auf die vorgefundenen Bedingungen des Aufbaus der Verwaltungen und auf die schleppende Bewilligung der für die gebotenen Sicherungsmaßnahmen erforderlichen Mittel zurückgeführt werden. Mitverantwortlich zu machen ist vielmehr auch die Einstellung, daß man sich so einen "Luxus" wie Datenschutz bei der Regelung offener Vermögensfragen nicht leisten könne.

Ferner ist das automatisierte Datenverarbeitungssystem zur Erfassung vermögensrechtlicher

Ansprüche (EVA), das allen ÄROV zur Anwendung vorgegeben wurde, als maßgebliche Quelle der angesprochenen Mängel bei der automatisierten Datenverarbeitung in den Ämtern zu nennen. Es läßt eine Behebung der Mängel durch das einzelne AROV nicht zu.

Die Auswirkungen ungenügender organisatorischer Vorkehrungen bei nie auszuschließendem menschlichen Versagen mag folgender Fall illustrieren: Ein Antragsteller hatte bei einem Vermögensamt in der regelmäßigen Sprechstunde des dort eingerichteten Tagesdienstes im Nachgang zu seinem Restitutionsantrag einen Erbschein nachgereicht. Er hatte das Dokument in einen Briefumschlag gesteckt, den er unverschlossen ließ. Auf dem Umschlag war der Inhalt, das Geschäftszeichen des Vermögensamtes, unter dem sein Antrag dort geführt wurde, sowie die Adresse des von ihm zur Rückgabe angemeldeten Objekts vermerkt. Der Umschlag wurde zur Ausgangspost gegeben und so schließlich von der Post der erstaunten Mieterin des Gebäudes zugestellt.

12 Aus der eigenen Behörde

- *Dienststelle*

Durch die zur Verfügung gestellten Sachmittel konnte im Laufe des Jahres 1993 die büromäßige Ausstattung meiner Behörde nahezu abgeschlossen werden. Der aufgeschlossenen parlamentarischen Unterstützung sowie der verständnisvollen Haltung des Ministeriums der Finanzen gegenüber den durch die Aufgabenstellung bedingten besonderen Ausstattungserfordernissen ist es zu verdanken, daß die erforderlichen Investitionsmittel bereitstanden, um jeden Arbeitsplatz dv-mäßig auszustatten und mit ausreichender Drucktechnik versehen zu können. Darüber hinaus kann das System durch entsprechende Hard- und Software auch als internes Aktensuch- und Archivierungssystem genutzt werden.

Durch Minderausgaben bei den Sachmitteln konnte eine moderne interne Telefonanlage angeschafft werden, die insbesondere dadurch notwendig wurde, da der Dienststelle zunächst nur ein analoger Telefonanschluß einschließlich Fax zur Verfügung stand. Damit sind wir - abgesehen von gelegentlichen geländebedingten Schalt- und Leitungspannen und Fehlschaltungen im Bereich der Telekom - zumindest telefonisch und per Telefax gut erreichbar.

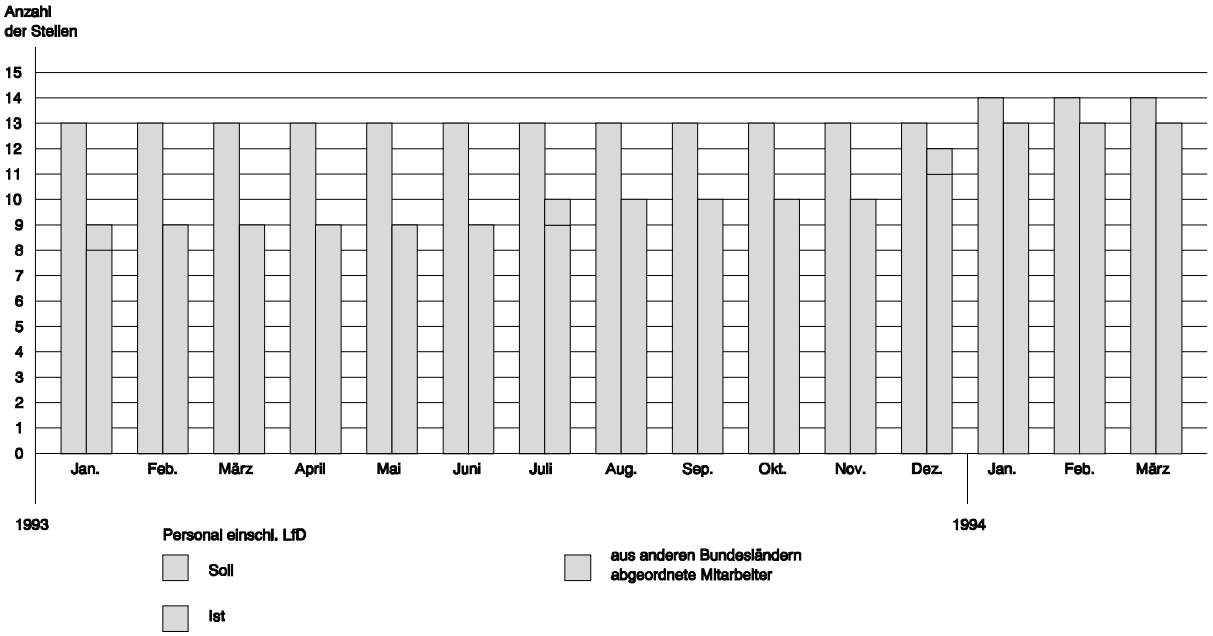
Im übrigen stellt die Erreichbarkeit meiner Behörde jedoch weiterhin ein großes Problem dar. Auch eine intensive Öffentlichkeitsarbeit konnte bislang kaum bewirken, daß sich die Bürger persönlich nach Kleinmachnow aufmachten, immerhin über 15 km entfernt von ihrer Landeshauptstadt. Dies geht zu Lasten des Anspruchs und des Ansehens einer "Bürgerbehörde". Auch umgekehrt sind für meine Mitarbeiter und mich die notwendigen Kontakte zum Landtag und den Ministerien des Landes Brandenburg in Potsdam mit hohen Reisekosten und großen Zeitverlusten verbunden. Immerhin hat der Minister der Finanzen gesprächsweise sein Verständnis für meine diesbezüglichen Sorgen geäußert und mir eine wunschgemäße Unterbringung meiner Behörde in Aussicht gestellt, sobald nach Fertigstellung verschiedener Bauprojekte der Landesregierung wieder Büroraumkapazitäten in Potsdam zur Verfügung stehen.

Ein große Erleichterung stellt angesichts dieser Gegebenheiten die Einbindung meiner Behörde in den Kurierdienst des Innenministeriums dar; so kann der gesamte behördeninterne Schriftverkehr mit den Ministerien sowie mit dem Landtag problemlos abgewickelt werden.

- *Personalsituation*

Über lange Zeit weniger günstig stellte sich die Personalentwicklung in meiner Behörde dar. Dazu trug (nicht zuletzt) auch die nicht in allen Fällen sachgerechte Stellenbewertung bei. Dennoch konnten inzwischen die letzten beiden der bereits im Haushaltsjahr 1993 zur Verfügung stehenden Referentenstellen besetzt werden. Dabei wirkte es sich positiv aus, daß der Finanzminister zugestimmt hatte, daß in Gleichbehandlung mit den Bediensteten der Landtagsverwaltung auch den in meiner Behörde beschäftigten Beamten und Angestellten die sog. Ministerialzulage gezahlt werden kann.

Personalentwicklung



Eine vom Präsidenten des Landtages ausgehende Empfehlung an die Landesregierung und an die Fraktionen des Landtags zur Einrichtung meiner Behörde als oberste Landesbehörde ist bisher ohne Erfolg geblieben. Das bedeutet, daß meine Haushaltsmittel weiterhin im Kapitel 01 030 Bestandteil des Einzelplanes 01 des Landtags gem. § 22 Abs. 4 Satz 4 Bbg DSG sind, der Landtag mit seinen unmittelbar für seinen Haushalt zuständigen Gremien sich aber außerstande sieht, Entscheidungen insbesondere bezüglich meines Personalbedarfs zu treffen. Allerdings wird mir vom Präsidenten des Landtages fairerweise eingeräumt, in den Verhandlungen über den Haushalt 1995 gemeinsam mit den Vertretern der Landtagsverwaltung mein Kapitel gegenüber dem Finanzministerium vertreten zu können. Eine Lösung des Grundsatzproblems kann allerdings wirklich nur durch eine eindeutige Definition des Rechtsstatus meiner Behörde erreicht werden.

- *Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder*

Einer langjährigen Praxis folgend ist dem Landesbeauftragten für den Datenschutz Brandenburg entsprechend der alphabetischen Reihenfolge turnusgemäß der Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 1994 zugefallen. So kam mir die dankbare Aufgabe zu, die Konferenz zu ihrer 47. Sitzung am 09./10. März 1994 zum ersten Mal in ein neues Bundesland einzuladen. Dank der Unterstützung durch die Landtagsverwaltung, die mir auch die technischen Einrichtungen und besten Räumlichkeiten des Landtags zur Verfügung stellte, war es mir möglich, die Konferenz in angemessenem Rahmen in der Landeshauptstadt Potsdam durchführen zu können. Dies hat ebenso zum Erfolg der Konferenz beigetragen wie ein festlicher Abendempfang des Präsidenten des Landtages.

Schwerpunktmäßig beschäftigte sich die Konferenz mit einer Standortbestimmung des Datenschutzes 10 Jahre nach dem Volkszählungsurteil, dem europaweiten Datenaustausch, dem Interessenausgleich zwischen Bekämpfung der Kriminalität und dem Schutz vor Übergriffen des Staates auf das Persönlichkeitsrecht Unbeteiligter sowie die Verhältnismäßigkeit der Überprüfung von sozialen Leistungen. Die Beschlüsse der

Konferenz sind als Anlagen 16 bis 21 dem Tätigkeitsbericht beigefügt. Die 48. Konferenz der Datenschutzbeauf-tragten des Bundes und der Länder wird - wiederum in Brandenburg - am 28./29. September 1994 stattfinden.

- *Fortbildungsveranstaltungen*

In Zusammenarbeit mit dem Landesamt für Datenverarbeitung und Statistik hat meine Behörde im Berichtszeitraum zweimal eintägige Fortbildungsveranstaltungen zu grundsätzlichen Fragen des Datenschutzes für Mitarbeiter des öffentlichen Dienst ausgerichtet. Gemessen an dem Bedarf auf diesem Gebiet im Land Brandenburg ist das freilich nur "ein Tropfen auf den heißen Stein". Eine nach meinen bisherigen Erfahrungen dringend zu wünschende Verstärkung der Fortbildung der Mitarbeiter im öffentlichen Dienst auch im Bereich der datenschutzrechtlichen Regelungen kann jedoch von meiner Behörde weder organisatorisch noch personell geleistet werden. Ich würde es allerdings begrüßen und im Rahmen meiner Möglichkeiten tatkräftig unterstützen, wenn jährlich - wie das in anderen Bundesländern ge- schieht - seitens des Landtages oder der Fortbildungseinrichtungen des öffentlichen Dienstes zumindest für die behördlichen Datenschutzbeauftragten der Kommunen ein "Datenschutz-tag" eingeführt werden würde.

Kleinmachnow, den 13.05.1994

Dr. sc. Dietmar Bleyl
Der Landesbeauftragte für den Datenschutz

Datenschutzrechtliche Anforderungen beim Einsatz von Laptops und Notebooks

Laptops, Notebooks u. ä. Computer sind auf Grund ihrer Mobilität und des Fehlens eines geordneten Arbeitsplatzes gegenüber herkömmlichen PC zusätzlichen Bedrohungen ausgesetzt, wie etwa: leichter Diebstahl, höhere Gefahr der Zweckentfremdung, leichtere Zerstörbarkeit, unbefugte Bildschirmeinsicht, schwer kontrollierbare Datenübermittlung. Durch organisatorische und technische Maßnahmen des Datenschutzes kann man diesen Gefahren begegnen:

Organisatorische Maßnahmen:
- Die Anschaffung dieser Geräte durch die Behörde sollte nach einheitlichen Gesichtspunkten erfolgen.
- Die Geräte sind wie alle PC in das Geräteverzeichnis einzutragen.
- Die Geräteverwaltung sollte zentral bei dem Systemverantwortlichen der Behörde organisiert sein.
- Der Einsatz von Anwendungsprogrammen erfolgt wie üblich nach dem Freigabeverfahren.
- Der Geräteeinsatz wird durch Dienstanweisung geregelt.

Technische Maßnahmen:
- Gegen Hardwaremanipulationen können die Geräte verplombt werden.
- Ein Gerät sollte an einen Nutzer gebunden werden. Ist dies nicht möglich, muß jeder vorher festgelegte Mitarbeiter mit eigenem Paßwort arbeiten können.
- Die Sicherheitssoftware muß die Paßworte verschlüsselt abspeichern.
- Wichtige Aktivitäten am Gerät einschließlich gescheiterter Zugriffsversuche sind durch die Sicherheitssoftware automatisch nicht-manipulierbar zu protokollieren.
- Die Auswertung des Protokolls sollte insbesondere dem behördlichen Datenschutzbeauftragten zustehen, allerdings nur zur Beobachtung des Datenschutzes.
- Der Zugriff auf das Betriebssystem ist auszuschließen.
- Die Schnittstellen sollten grundsätzlich wegen unkontrollierbarem Datenaustausch gesperrt werden, ebenso das Diskettenlaufwerk.
- Sensible personenbezogene Daten sind auf der Festplatte zu verschlüsseln, so daß bei Diebstahl des Geräts kein Auslesen dieser Daten möglich ist.
- Problematisch, aber im Einzelfall hinnehmbar ist die Notwendigkeit, Daten über ein Netz übertragen zu müssen, etwa über Telefonleitung mittels Modem. In diesem Fall müssen beide Teilnehmer die Berechtigung der Datenübermittlung des anderen Partners überprüfen.
- Ist die Nutzung des Diskettenlaufwerks zur Datenausgabe unumgänglich, müssen die Daten wie auf der Festplatte verschlüsselt und die Funktion des Laufwerks auf die Ausgabe beschränkt werden.

Regeln beim Umgang mit Telefaxgeräte

Da es eine Fülle von Risiken für die Einhaltung der Vertraulichkeit gibt, wenn man mit Telefax-Geräten arbeitet, sollten bei der praktischen Arbeit mit diesen Geräten folgende technischen und organisatorischen Regeln eingehalten werden:

- Als Verantwortlicher für die Einhaltung des Datenschutzes muß man als Absender wenigstens den Sicherheitsstandard des Briefversands einhalten.
- Da das Telefaxen ebenso wie das Telefonieren abhörbar ist, sind grundsätzlich personenbezogene Daten, die als sehr sensibel einzustufen sind bzw. einem Berufs- oder Amtsgeheimnis unterliegen (gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen, arbeitsrechtliche Verhältnisse, Steuerdaten, Sozialdaten, psychologische Daten, Unterbringung in Anstalten, Betreuungen, Wahlausschlüsse, Paßversagungsgründe), nicht zu faxen.
- Telefaxgeräte sind so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder gesendeter Telefax-Schreiben erhalten können.
- Beim Faxen sind alle technischen Sicherheitseinrichtungen des Faxgeräts zu nutzen, dies trifft insbesondere für die Anzeige des erreichten Geräts zu. Bei erkennbaren Fehlern oder Störungen ist die Sendung sofort abzubrechen.
- Vor einer Sendung sollte man sich vergewissern, ob der Adressat noch unter der bekannten Anschluß-Nummer erreichbar ist.
- Bei sensiblen Daten sollte man vorher mit dem Empfänger telefonieren und eine Sendezeit absprechen.
- Bevor erstmals personenbezogene Daten gesendet werden, sollte man sicher sein, daß der Empfänger tatsächlich Maßnahmen getroffen hat, die sicherstellen, daß diese Daten nur an den Empfangsberechtigten gelangen.
- In der Behörde muß eine schriftliche Dienstanweisung zur Bedienung des Faxgeräts vorliegen.
- Jede Übermittlung einer Telekopie ist durch das Vorblatt der Behörde, die Angabe der Kopienanzahl, durch den Verifikationsstempel auf dem Original und durch die Ablage der Protokolle sorgfältig zu dokumentieren.
- Beim Verkauf eines gebrauchten Telefaxgerätes ist zu beachten, daß gespeicherte Vermittlungs- und Inhaltsdaten tatsächlich gelöscht sind.
- Es ist auch zu bedenken, daß eine von einem Standardfaxgerät ordentlich gesendete und dokumentierte Telekopie nicht in jedem Fall vor Gericht einen Beweiswert hat.

Entschließung

der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 23./24. März 1992 in Stuttgart

zum

Arbeitnehmerdatenschutz

I. Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunft-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie - losgelöst vom Erhebungszweck - für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z.B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u.ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II. Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers - auch durch Befragen des Arbeitnehmers oder Bewerbers - nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist

der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.

3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z.B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zu Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm - soweit erforderlich - nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.

8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.

9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. I Abs. 4) eingewilligt hat.

Entschließung

der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 28. April 1992 in Stuttgart

zum

Grundrecht auf Datenschutz

(gegen die Stimme Bayerns)

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

- für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,

- der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,

- der Grundrechtskatalog dem technologischen Wandel angepaßt und

- die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

> "Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

   - Stärkung der Grundrechte aus Art. 10 und 13 GG im Hinblick auf neue Überwachungstechniken

   - Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)

- Instrumente zur Technikfolgenabschätzung.

Entschließung

der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 28. April 1992 in Stuttgart

zur

Neuregelung des Asylverfahrens (BT-Drs. 12/2062) vom 28. April 1992

(gegen die Stimme Bayerns)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und

2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1.:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern - bis auf wenige Ausnahmen - Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder - gleichgültig ob Deutscher oder Ausländer - muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber - also nicht bloß diejenige einzelner oder bestimmter Gruppen - zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

Bei der zentralen Auswertung der Fingerabdrucke von Asylbewerbern durch das Bundeskriminalamt muß - ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird - unbedingt folgendes sichergestellt sein:

- Fingerabdrucke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt

erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sogenannten Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben:

Mit der bevorstehenden Einführung von AFIS - einem neuen automatisierten Fingerabdruckverfahren - sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte - über das Trennungsgebot des § 16 Abs. 4 hinaus - die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht - wie es der Gesetzentwurf aber vorsieht - praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Entschließung

der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 1./2. Oktober 1992 in Stuttgart

zum

Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen - auch wenn sie von einem Dienstapparat aus geführt werden - unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.
Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen - insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind - umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TKAnlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z.B. bei Feuerwehr und Rettungsdiensten).
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten

gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Entschließung

der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 1./2. Oktober 1992 in Stuttgart

zum

Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung
der gesetzlichen Krankenversicherung
Gesundheits-Strukturgesetz 1993 - (BR-Drs. 560/92)

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u.a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserung des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.
- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.
- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie - auch zur Abrechnung - im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.
- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbögen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

Entschließung

der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 1./2. Oktober 1992 in Stuttgart

zum

"Lauschangriff"

(gegen die Stimme Bayerns)

Die Datenschutzbeauftragten des Bundes und der Länder erklären:

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. "Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung - insbesondere heimlicher - entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.
2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.
3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Entschließung

der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 16./17. Februar 1993 in Berlin

zur

Richtlinie des Rates vom 07. Juni 1990 über den freien Zugang
zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zum

Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom
und bei der europaweiten Liberalisierung des Telefonnetzes
und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. 8. 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zur

Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z.B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z.B. die übertragenen Daten anwendungsseitig verschlüsselt.
Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten - personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in

solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zum

Integrierten Verwaltungs- und Kontrollsystem
(InVeKoS)
(Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;

- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;

- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;

- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z.B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs z.B. zur Besteuerung).

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zu

kartengestützten Zahlungssystemen im Öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im Öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im Öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zu

regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten
und die Gebühreneinzugszentrale (GEZ)

(gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Entschließung

der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 1993 in Berlin

zur

Gefährdung der Vertraulichkeit der Funkkommunikation
von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z.B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. März 1994 in Potsdam

zu

Chipkarten im Gesundheitswesen[145)]

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf

---

145) Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.

- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. März 1994 in Potsdam

zur

Informationsverarbeitung im Strafverfahren [1)]

(bei Stimmenthaltung Bayerns)

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Ingesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

---

1) Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X

ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. März 1994 in Potsdam

zum

Ausländerzentralregistergesetz [1)]

(gegen die Stimme Bayerns)

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 02. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen

---

[1)] Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. März 1994 in Potsdam

zum

Abbau des Sozialdatenschutzes [1)]

(gegen die Stimme Bayerns)

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der einzelne mündige Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeits-loser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

[1)] Baden-Württemberg war in der Sitzung nicht vertreten, trägt den Beschluß jedoch inhaltlich mit.

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. März 1994 in Potsdam

zum

Gesetzentwurf der Bundesregierung zur Neuordnung
des Postwesens und der Telekommunikation [1)]

(Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der
dafür erforderlichen Änderung des Grundgesetzes
(BR-Drs. 114/94 = BT-Drs. 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf

---

[1)] Baden-Württemberg war in der Sitzung nicht, Sachsen bei der Beschlußfassung nicht mehr vertreten; beide tragen den Beschluß jedoch inhaltlich mit.

Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat

- bei Stimmenthaltung Bayerns und in Abwesenheit Baden-Württembergs - die folgende

Bestandsaufnahme

über die Situation des Datenschutzes "10 Jahre nach dem Volkszählungsurteil"

zustimmend zur Kenntnis genommen.

Nach Ablauf von über 10 Jahren seit der Verkündung des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz am 15. Dezember 1983 sieht sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, eine Bestandsaufnahme der Situation vorzulegen, in der sich der Datenschutz derzeit befindet.

Entwicklung nach dem Volkszählungsurteil:

Bereits unmittelbar nach Inkrafttreten der Datenschutzgesetze in Bund und Ländern war die Frage heftig diskutiert worden, welchen Rang der Datenschutz gegenüber anderen Rechtsgütern habe. Befürwortern der Auffassung, dem Datenschutz komme Grundrechtsqualität zu, standen zurückhaltendere Stimmen gegenüber, die die Subsidiarität des Datenschutzes betonten.

Das Volkszählungsurteil hat den Datenschutz zu einer elementaren Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens erklärt und den Grundrechtscharakter der informationellen Selbstbestimmung festgeschrieben. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Damit wurde klargestellt, daß der Datenschutz unter den Bedingungen der modernen Datenverarbeitung das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen den einzelnen und den Institutionen in Staat und Gesellschaft ist. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bestätigt.

Danach ist von dem verfassungsrechtlichen Grundsatz auszugehen, daß die Entscheidung über die Preisgabe und Verwendung personenbezogener Daten zuallererst beim Betroffenen selbst liegt. Einschränkungen der individuellen Dispositionsfreiheit sind für die Rechts- und Gesellschaftsordnung von so wesentlicher Bedeutung, daß sie nur auf einer gesetzlichen Grundlage zulässig sind. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zeckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d.h. vor den Augen der Öffentlichkeit zu entscheiden.

Bei der Regelung des Informationsumgangs ist von den individuellen Freiheitsrechten auszugehen; doch darf und muß der Gesetzgeber selbstverständlich berücksichtigen, daß der einzelne in vielfältiger Weise auf den Schutz und die Hilfe des Staates angewiesen ist und daß die Tätigkeit des Staates kontrollierbar sein muß. In gesetzlich klar vorgegebenen Fällen ist daher die Verwendung personenbezogener Daten auch ohne selbstbestimmte Mitwirkung des Betroffenen erforderlich.

Das Grundrechtsverständnis mit der Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine

kritische Bilanz zu ziehen.

Nach der Entscheidung des Bundesverfassungsgerichts sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtlicher Fortschritt hart umkämpft werden.

Neben einer grundlegenden Novellierung der Datenschutzgesetze in Bund und Ländern wurden Spezialbestimmungen in zahlreichen Sondermaterien geschaffen. Auf der Ebene des Bundes zählen dazu:

- einzelne Bücher des Sozialgesetzbuches,
- das Personalaktenrecht für Beamte,
- das Straßenverkehrsrecht,
- die Gesetze über die Nachrichtendienste des Bundes,
- das Telekommunikationsrecht.

Besonderer Handlungsbedarf für die Verwirklichung der informationellen Selbstbestimmung entstand durch die deutsche Einigung. Dabei stellt die Aufarbeitung der Hinterlassenschaft des Staatssicherheitsdienstes der ehemaligen DDR auch für den Datenschutz eine besondere Herausforderung dar.

Noch weitergehend ist der Umfang der datenschutzrechtlichen Neuregelungen in den Ländern, in denen die Vorgaben des Bundesverfassungsgerichtes teilweise konsequenter umgesetzt wurden als im Bund.

Diese Verrechtlichungswelle hat auch Kritik hervorgerufen:

In Dutzenden von Gesetzen ist nunmehr das "Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle bereits aus normenklaren Gründen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen. Eine weitergehende Kritik stellt in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war. Geäußert wurde auch die Annahme, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten habe und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpassung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze behindert würden.

Dem muß allerdings entgegen gehalten werden, daß die Fülle und Kompliziertheit der Datenverarbeitung in den verschiedensten Verwaltungsbereichen für die Regelungsdichte verantwortlich ist. Sie ist eine Konsequenz des Umstands, daß in allen Verwaltungsbereichen der - zunehmend automatisierten - Informationsverarbeitung immer mehr Bedeutung zukommt: Eine notwendige Folge der Entwicklung hin zu "Informationsgesellschaft".

Ein weiterer Grund für die Komplexität der Gesetzgebung liegt darin, daß die Gesetze häufig nicht darauf abzielen, die Rechtsposition des Bürgers zu stärken, sondern vielmehr Verarbeitung personenbezogener Daten zu ermöglichen, oft über das Maß hinaus, das bislang zulässig war. Viele Vorschriften sind so derart allgemein und umfassend zugunsten der Eingriffsseite formuliert, daß es schwerfällt, sie als "Datenschutzgesetze" im eigentlichen Sinn zu verstehen. Wann immer Verwaltungen sich durch den Datenschutz behindert glaubten, ertönte der Ruf nach dem Gesetzgeber, der - zugunsten der Verwaltung - korrigierend eingreifen soll.

Trotz alledem blieb der Datenschutz in wesentlichen Bereichen ungeregelt. Auf Bundesebene gibt es z.B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des

Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten, der Bundespolizeibehörden, des Ausländerzentralregisters oder - am gravierensten - des gesamten Strafverfahrens.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, diese Lücken umgehend und im Sinne der informationellen Selbstbestimmung zu schließen.

Zur aktuellen Situation:

Die derzeitige Situation des Datenschutzes wird von den beiden großen Themenbereichen geprägt, die die Innenpolitik beherrschen: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Diese Felder ängstigen die Menschen und stärken die Kontrollbedürfnisse des Staates. Auf beiden Gebieten wird die vermeintliche Lösung darin gesucht, daß die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich ausgeweitet und auf der anderen Seite die Rechte der Bürger entsprechend eingeschränkt werden.

Auf dem Gebiet der **Strafverfolgung** haben sich bisher die Ermittlungen auf den Beschuldigten konzentriert und die prozessuale Aufklärung geschah im wesentlichen offen.

Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Ermittlungsverfahren ist nicht mehr Aufklärung eines konkreten Tatverdachts, sondern flächendeckende Sammlung personenbezogener Daten. Der Staat hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung.

Im Bereich der **Wirtschafts- und Sozialordnung** wird auf besonders drastische Weise versucht, durch die Einführung neuer Übewachungsverfahren eine Kostenminderung zu erreichen. Die Daten werden einerseits genutzt, durch Plafondierungen und Wirtschaftlichkeitsuntersuchungen eine Kostendämpfung zu erreichen (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder eine angeblich mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung).

Auf den Datenschutz wirkt sich dabei die Tendenz aus, weg von einer angeblichen egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Individualrechte werden vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt. Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht.

Hinzu kommt, daß das reine Verwaltungsinteresse, das Bestreben nach größtmöglicher Perfektion und Einzelfallgerechtigkeit ein immer größeres Gewicht erhält. Je mehr Perfektion die Verwaltung angestrebt, desto mehr Daten muß sie erheben, nutzen, abgleichen oder sonst verarbeiten. Das Gespür für den "Mut zur Lücke" geht verloren. Kennzeichend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.

Besonders gern wird zur Intensivierung der Kontrolle die Wunderwaffe des Datenabgleichs genutzt. Perfektion und Korrektheit lassen sich dadurch auf bequeme Weise erreichen: Auf Knopfdruck lassen sich die verschiedensten Kontrollmechanismen in Gang bringen, ohne daß sich die Behörde unmittelbar mit dem einzelnen Bürger auseinandersetzen muß. Mühelos ist die Prüfung von Zehntausenden in kürzester Frist möglich.

Wird der Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, ungebremst fortgesetzt, könnte sich aus einer Unsumme von

automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereich erfaßt, der "gläserne Bürger" ergeben. Selbst wenn jeder einzelne Abgleich und Kontrollvorgang für sich eine gewisse Berechtigung haben sollte, trägt er bei zu einem umfassenden Netz von Überwachungs- und Überprüfungsmöglichkeiten. Jeder Bürger wird dabei potentiell zum Verdächtigen, dessen korrektes Verhalten ist zu überprüfen gilt. Damit ändert sich das Verhältnis des Bürgers zum Staat auf grundlegende Weise.

Wie dem begegnen?

Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Fundament im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn 10 Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen würde. Daß die erforderliche Mehrheit in Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich.

Die verfassungsrechtliche Verbesserung bei einer derartigen Grundgesetzänderung bestünde auch darin, daß bei jedem Gesetzentwurf von Anfang an die Berücksichtigung des Grundrechts auf Datenschutz zu prüfen wäre. Eine Einschränkung des Grundrechts müßte künftig durch ausdrückliche Erwähnung im Gesetz unter Angabe des neuen Grundgesetzartikels kenntlich gemacht werden (sog. Zitiergebot nach Art. 19 GG); anderenfalls wäre das Gesetz nichtig. Dies wäre ein erheblicher "Mehrwert" zugunsten der Bürger.

Für die weitere Ausgestaltung des einfachen Datenschutzrechts sollten folgende Erwägungen zugrunde gelegt werden:

In der Informationsgesellschaft ist der effektive Schutz der personenbezogenen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Der Bürger kann seine Freiheit zur Kommunikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt.

Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch **materielle Freiheitsräume** garantieren müssen. Dies bedeutet, daß bei der Frage, ob der einzelne einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange belastende Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, jeweils strenge Maßstäbe angelegt werden müssen. Hierfür ist eine neue Grenzziehung für Eingriffe in das Recht auf informationelle Selbstbestimmung erforderlich:
Der Begriff des "überwiegenden Allgemeininteresses", der alleine einen Eingriff in die informationelle Selbstbestimmung rechtfertigt, ist inhaltlich mehr aufzufüllen und mehr als bisher im Lichte der informationellen Selbstbestimmung zu interpretieren. In konkreten Konfliktfällen darf die Freiheitssicherung der Bürger gegenüber effektiver Staatstätigkeit nicht ins Hintertreffen geraten.

Für das Bundesverfassungsgericht ist die Beteiligung **unabhängiger Datenschutzbeauftragter** wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten im Interesse eines vorgezogenen Rechtsschutzes von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung. Dies gilt insbesondere in den Bereichen, in denen ein Auskunfts- oder Einsichtsanspruch des Bürgers nicht oder nur unvollständig besteht. Daraus folgt, daß Rolle und Kompetenzen der Datenschutzbeauftragten

auch im Hinblick auf effektivere Eingriffsmöglichkeiten gestärkt werden müssen. Versuche, die Kontrollmöglichkeiten der Datenschutzbeauftragten zu beschränken, muß schärfstens widersprochen werden.

Datenschutzrechtliche Verstöße gehen meist aus Unkenntnis und mangelndem Problembewußtsein seitens der öffentlichen Stellen zurück. **Aus- und Fortbildung** in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in der Schule, Rechts- und Informatikstudium in den Hochschulen) sowie den Fortbildungsveranstaltungen an der öffentlichen Verwaltung als obligatorisches Fach zu verankern.

Die **Datenverarbeitungstechniken** haben sich gegenüber der Zeit des Volkszählungsurteils geradzu revolutionär verändert. Der Umsetzung des Volkszählungsurteils durch die Schaffung der eigenen Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch organisatorischer Maßnahmen zur Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitunsprozesses selbst richten. Dies bedeutet nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue informationstechnische Entwicklungen (Miniaturisierung der Rechner, Chipkarten, neue Vernetzungstechniken), sondern auch neuer komplexer Anwendungsformen (z.B. im Bereich des Zahlungsverkehrs, der Straßenbenutzung oder der Textverarbeitung).

Die **Europäische Union** wird zunehmend zur Informations- und Datengemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen - und damit auch für persönliche Daten - nicht zu Nachteilen für den einzelnen führt.

Innerhalb von Deutschland wirft die **Integration der neuen und der alten Bundesländer** nach wie vor Probleme auf. Nach wie vor besteht die Neigung, über Bürger aus den neuen Bundesländern erheblich mehr Daten zu erheben und unter erleichterten Bedingungen Daten zu verarbeiten als dies in den alten Ländern der Fall wäre.

Die Notwendigkeit für Übergangsregelungen in den neuen Bundesländern wird nicht bestritten; die Eingriffe in Persönlichkeitsrechte müssen aber dennoch verhältnismäßig, erforderlich und darüber hinaus zeitbefristet sein. Aus dem Einigungsprozeß herrührende Sonderregelungen und Verwaltungsvorschriften sind nicht festzuschreiben, sondern auch im Sinne der informationellen Selbstbestimmung schrittweise abzubauen.

Einrichtung _____

Aufnahmebeleg

Bitte in **Druckbuchstaben** schreiben. Stark umrandete Felder **nicht** ausfüllen. Die Angaben zu den schraffierten Feldern sind freiwillig. Bitte lesen Sie hierzu die **Anmerkungen auf der Rückseite**.

Aufnahme-Nr.	Aufnahme-Tag	Uhrzeit	Station

Patient/in: Zu- und Vorname				
Straße und Hausnummer			PLZ und Wohnort	
Geburts-Datum	Geburts-Name		Geburts-Ort	
bitte ankreuzen weiblich ☐ männlich ☐	Konfession		Familienstand	Nationalität

Hauptversicherte/ter: Zu- und Vorname Wenn identisch mit Patientendaten, hier nur ankreuzen. ☐		

Beruf und Arbeitgeber (bei Arbeitsunfall unbedingt angeben)
Hausarzt
Einweisender Arzt
Dringende Nachricht an: (z.B. Name, Anschrift, Telefon)

Krankenkasse oder Zahlungspflichtiger (Bitte genaue Anschrift angeben. Evtl. auch Versicherungsnummer etc.)

Müssen Sie in diesem Jahr noch Ihrer Zahlungspflicht nachkommen? ja ☐ nein ☐

bitte ankreuzen

Hinweis: Die noch zu leistenden Zahlungen wollen Sie unbedingt in jedem Fall vor Verlassen des Krankenhauses in unsere Aufnahme einzahlen.

Ich bin damit einverstanden, daß meine Personalien (Familienname, Vorname, Wohnanschrift, Aufnahmeantrag, Station, und Zimmer-Nr.) an die Informationszentrale (der Einrichtung) übermittelt werden, um Besuchern auf Nachfrage Auskunft erteilen zu können.
Das Informationsblatt - Hinweise auf die Datenverarbeitung im Krankenhaus - habe ich erhalten.

☐ Ich bin damit einverstanden ☐ Ich bin damit nicht einverstanden

_____ _____

Ort, Datum

Unterschrift der Patientin / des Patienten
oder der gesetzlichen Vertreterin / des Vertreters

Anmerkungen

Konfession

Wenn Sie hier einen Eintrag vornehmen, wird Ihre Religionsgemeinschaft über Ihren Aufenthalt in unserer Klinik informiert. Übermittelt werden Name, Anschrift, Geburtsdatum, Aufnahmetag und Zimmernummer.

Beruf, Arbeitgeber

Sie erleichtern Ihrer Krankenkasse die Arbeit, wenn Sie trotz Freiwilligkeit Angaben machen. Sollten Sie aufgrund **eines Arbeitsunfalls** bei uns sein, so **müssen** Sie Angaben machen.

Hausarzt

Ihr behandelnder Krankenhausarzt möchte evtl. Rücksprache mit Ihrem Hausarzt nehmen. Sie erleichtern ihm die Arbeit, wenn Sie ihren Hausarzt benennen.

Dringende Nachrichten, Telefon-Nr.

Wenn Sie wollen, können Sie hier Angaben über einen nächsten Angehörigen oder eine andere Vertrauensperson machen, die notfalls informiert werden soll.

Stichwortverzeichnis:

(Berichtszeitraum der Jahresberichte: I = März bis Dezember 1992; II = bis März 1994; /Seitenangabe)

Abkürzungsverzeichnis

a. F.	=	alte Fassung
AbfRestÜberwV	=	Abfall- und Reststoffüberwachungsverordnung
ABl.	=	Amtsblatt
Abs.	=	Absatz
Abschn.	=	Abschnitt
ADV	=	Automatische Datenverarbeitung
AFIS	=	Automatisierte Fingerabdruck-Identfizierungssystem
AfNS	=	Amt für Nationale Sicherheit
AG	=	Ausführungsgesetz
AGTierSGBbg	=	Gesetz zur Ausführung des Tierseuchengesetzes
AK	=	Arbeitskreis
Anl.	=	Anlage
AO	=	Abgabenordnung
AOK	=	Allgemeine Ortskrankenkasse
AOV	=	Amt zur Regelung offener Vermögensfragen
Art.	=	Artikel
AUT	=	Anonymous Unliked-Testing
AVA	=	automatisierte Vorgangsauswertung
AVB	=	Allgemeine Vertragsbestimmungen
BAnz.	=	Bundesanzeiger
BArchG	=	Bundesarchivgesetz
Bbg DSG	=	Brandenburgisches Datenschutzgesetz
Bbg.	=	Brandenburgisch(es)
BbgArchG	=	Archivgesetz
BbgGDG	=	Gesundheitsdienstgesetz
BbgRettG	=	Rettungsdienstgesetz
BDSG	=	Bundesdatenschutzgesetz
BfD	=	Bundesbeauftragter für den Datenschutz
BfV	=	Bundesamt für Verfassungsschutz
BGB	=	Bürgerliches Gesetzbuch

BGBl.	=	Bundesgesetzblatt
BGS	=	Bundesgrenzschutz
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BLHA	=	Brandenburgisches Landeshauptarchiv
BMI	=	Bundeministerium des Innern
BND	=	Bundesnachrichtendienst
BOS	=	Behörden und Organisationen mit Sicherheitsaufgaben
BR-Drs.	=	Bundesrats-Drucksachen
BRRG	=	Beamtenrechtsrahmengesetz
BSHG	=	Bundessozialhilfegesetz
BStU	=	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
Buchst.	=	Buchstabe
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BZR	=	Bundeszentralregister
BZRÄG	=	Bundeszentralregisteränderungsgestz
BZRG	=	Bundeszentralregistergesetz
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DDR-GBl.	=	DDR-Gesetzblatt
DIV	=	Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin
DORA	=	Dialogorientertes Recherche- und Auskunftssystem
DRegVOBbg	=	Dateiregisterverordnung
DRFZ	=	Deutsches Rheuma-Forschungszentrum
DRK	=	Deutsches Rotes Kreuz
Dtsch. Ärztebl.	=	Deutsches Ärzteblatt
DuD	=	Zeitschrift "Datenschutz und Datensicherung"
DV	=	Dienstvereinbarung über die Nutzung der ISDN-Telekommunikationsanlage des Telekommunikationsverbundes der obersten Landesbehörden
DVO	=	Durchführungsverordnung
e. V.	=	eingetragener Verein
EDV	=	Elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft

EURO-ISDN	=	Europäisches ISDN
EVertr.	=	Einigungsvertrag
EWG	=	Europäische Wirtschaftsgemeinschaft
Fa-Blätter	=	Fingerabdruck-Blätter
ff.	=	folgende
FH	=	Fachhochschule
gem.	=	gemäß
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
GK	=	Gemeinschaftskommentar
GLKA	=	Gemeinsames Kriminalamt der fünf neuen Länder
GSF	=	Gesellschaft für Strahlen- und Umweltforschung
GVBl.	=	Gesetz- und Verordnungsblatt
G10	=	Gesetz zu Artikel 10 Grundgesetz
HebBOBbg	=	Berufsordnung der Hebammen und Entbindungspfleger des Landes Brandenburg
HebGBbg	=	Landeshebammengesetz
HeilBerG	=	Heilberufsgesetz
i. d. F. vom	=	in der Fassung vom
IMK	=	Innenministerkonferenz
INPOL	=	Informationssytem der Polizei
InVeKoS	=	Integriertes Verwaltungs- und Kontrollsystem
i.V.m.	=	in Verbindung mit
i.S.v.	=	im Sinne von
ISD	=	Internationaler Suchdienst
ISDN	=	Integrated Services Digital Network (dienste-integrierendes Digitalnetz)
KAN	=	Kriminalaktennachweis
Kap.	=	Kapitel
KJHG	=	Kinder- und Jugendhilfegesetz
KPMD-S	=	Kriminalpolizeiliche Meldedienst - Staatsschutz
KpS	=	Kriminalpolizeiliche personenbezogene Sammlung
KTA	=	Kriminaltaktische Anfrage
KVK	=	Krankenversichertenkarte
LAN	=	Local Area Network (lokales, örtliches Netz, Grundstücksnetz)
LAROV	=	Landesamt zur Regelung offener Vermögensfragen
LBG	=	Landesbeamtengesetz

LASA	=	Landesagentur für Struktur und Arbeit
LfD	=	Landesbeauftragter für den Datenschutz
LfV	=	Landesamt für Verfassungsschutz
LGG	=	Landesgleichstellungsgesetz
LImSchG	=	Vorschaltgesetz zum Immissionsschutz
LKA	=	Landeskriminalamt
LKHG	=	Landeskrankenhausgesetz
MAGSF	=	Ministerium für Arbeit, Gesundheit, Soziales und Frauen
Maut	=	Gebühr für Straßen- und Brückenbenutzung (österr.)
MBJS	=	Ministerium für Bildung, Jugend und Sport
MeldeDÜVAV	=	Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MELF	=	Ministerium für Ernährung, Landwirtschaft und Forsten
MfS	=	Ministerium für Staatssicherheit (der DDR)
MODACOM	=	Mobile Data Communications (Dienst der DBP TELEKOM zur mobilen Datenkommunikation)
MUNR	=	Ministerium für Umwelt, Naturschutz und Raumordnung
n. F.	=	neue Fassung
NJW	=	Neue Juristische Wochenschrift
NVA	=	Nationale Volksarmee
PAG	=	Gesetz über die Aufgaben und Befugnisse der Polizei
PAuswG	=	Personalausweisgesetz
PC	=	Personalcomputer
PDB	=	Personendatenbank
PersVG	=	Landespersonalvertretungsgesetz
PHW	=	personenbezogener Hinweis
PKK	=	Parlamentarische Kontrollkommission
Pkt.	=	Punkt
PKZ	=	Personenkennziffer
POG	=	Polizeiorganisationsgesetz
PP	=	Polizeipräsidium
PTNeuOG	=	Postneuordnungsgesetz
Rd.-Nr.	=	Randnummer
RGBL.	=	Reichsgesetzblatt
RÜG	=	Rentenüberleitungsgesetz
RVO	=	Reichsversicherungsordnung
Sachgeb.	=	Sachgebiet

SED-UnBerG	=	Erstes SED-Unrechtsbereinigungsgesetz
SGB	=	Sozialgesetzbuch
SMAD	=	Sowjetische Militäradministration
StA	=	Staatsanwaltschaft
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StrRehaG	=	Strafrechtliches Rehabilitierungsgesetz
StUG	=	Stasi-Unterlagen-Gesetz
StVÄG	=	Strafverfahrensänderungsgesetz
TK	=	Telekommunikation
TSK	=	Tierseuchenkasse
UIG	=	Umweltinformationsgesetz
VerfSchG	=	Verfassungsschutzgesetz
VermG	=	Vermögensgesetz
VO PP	=	Verordnung über die Polizeipräsidien
VPKA	=	Volkspolizeikreisamt
VV	=	Verwaltungsvorschrift
VwGO	=	Verwaltungsgerichtsordnung
WAN	=	Wide Area Network (weites Netz, Fernverkehrsnetz)
ZER	=	Zentrales Einwohnerregister
ZERV	=	Zentrale Ermittlungsstelle von Regierungs- und Vereinigungskriminalität
Ziff.	=	Ziffer
ZIS	=	Zentrale Informationsstelle Sporteinsätze
ZKA	=	Zentrales Kriminalamt