••••Landtag Brandenburg Drucksache 2/4073

2. Wahlperiode

Fünfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. April 1996 bis 31. März 1997

Inhaltsverzeichnis Seite

1 Datenschutzrechtliche Entwicklung

1.1 Einleitung

Mit dem 5. Tätigkeitsbericht, dem ich dem Landtag Brandenburg vorlege, gebe ich einen Überblick über die Schwerpunkte meiner Arbeit im Berichtszeitraum 1996/97 und weise auf wichtige Probleme hin.

Die Adressaten dieses Berichts sind in erster Linie die Mitglieder des Landtags, darüber hinaus aber auch die interessierte Öffentlichkeit und nicht zuletzt die Vielzahl öffentlicher Stellen im Flächenland Brandenburg, die ich nach Kräften bei der Einhaltung des Datenschutzes unterstützen möchte, freilich aber auch zu kontrollieren habe. Die Informationsansprüche und Erwartungen sind notwendigerweise unterschiedlicher Art und können in einem solchen Bericht jeweils nur begrenzt berücksichtigt werden. Dies findet seinen Niederschlag vor allem bei der Themenauswahl. Um eine übermäßige Länge des Tätigkeitsberichtes zu vermeiden, wurde auf die Darstellung von Einzelfällen verzichtet, soweit ihnen nicht grundsätzliche Bedeutung zugemessen wurde.

Insgesamt zeichnet sich im Berichtszeitraum eine neue Qualität der Aufgabenwahrnehmung meiner Behörde ab, die nicht mehr schwerpunktmäßig auf die Erörterungen von einzelnen spezialgesetzlichen Vorschriften ausgerichtet ist. Vielmehr wird zunehmend deren praktische verfahrensmäßige Umsetzung in den Vordergrund treten. Die hierzu vorgenommenen Prüfungen datenschutzrechtlicher Vorschriften sowie deren technisch-organisatorische Umsetzung bei Telekommunikationsanlagen, bei Telefonüberwachungsmaßnahmen, in Schulen, in Gewerbe- und in Meldeämtern waren so angelegt, daß sie repräsentativ für die Situation im Land sind. Bei den zuständigen Fachministerien bestand deshalb ein großes Interesse an einer gemeinsamen Auswertung der im Ergebnis der Prüfung festgestellten Mängel bzw. Beanstandungen sowie die Bereitschaft zu Maßnahmen, beispielsweise mit Rundschreiben, zur Problembewältigung landesweit beizutragen. Es ist aber auch zu meiner Freude festzuhalten, daß bei den ins Blickfeld geratenen öffentlichen Stellen, bei denen Mängel festgestellt wurden, große Bereitschaft besteht, diese abzustellen, ohne daß es einer förmlichen Beanstandung bedarf.

Darüber hinaus hat sich in aller Regel bei den Prüfungen meine seit Amtsantritt vertretene Auffassung bestätigt, daß die heute gängige informations- und kommunikationstechnisch unterstützte Verarbeitung personenbezogener Daten und die damit verbundenen Probleme sich nur mit juristischem und technischem Sachverstand lösen lassen. Es wäre wünschenswert, wenn meine Behörde künftig stärker bei der Planung von Automatisierungsprojekten in der öffentlichen Verwaltung beratend herangezogen wird, damit so die effektive Verwendung öffentlicher Mittel in diesem Bereich gefördert werden kann, zumal Nachbesserungen in aller Regel aufwendig und oft nur sehr schwer zu realisieren sind.

Vor allem den Mitgliedern des Landtages danke ich für die vielfache Unterstützung und Aufgeschlossenheit. Den Mitarbeiterinnen und Mitarbeitern meiner Behörde danke ich für ihr beharrliches Engagement, mit dem sie sich für die Belange des Datenschutzes und damit für die Persönlichkeitsrechte der Bürger und Bürgerinnen des Landes Brandenburg eingesetzt haben.

Als Stichtag für den Jahresbericht wurde der 31. März 1997 gewählt.

1.2 Schaffung einzelgesetzlicher Regelungen im Land Brandenburg

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

Die nachfolgende Auflistung von in Kraft getretenen Gesetzen sowie Verordnungen und Verwaltungsvorschriften entspricht der Gliederung des Tätigkeitsberichtes nach dem Ressortprinzip. Eine Gewichtung erfolgt ausschließlich jeweils in dem in der Klammer angegebenen Einzelkapitel.

Gesetze:

- Katastrophenschutzgesetz des Landes Brandenburg (Brandenburgisches Katastrophenschutzgesetz - BbgKatSG) vom 11. Oktober 1996, GVBl. I S. 278

- Gesetz über die Statistik im Land Brandenburg (Brandenburgisches Statistikgesetz - BbgStatG) vom 11. Oktober 1996, GVBl. I S. 294

- Erstes Gesetz zur Änderung des Brandenburgischen Kindertagesstättengesetzes vom 7. Juni 1996, GVBl. I S. 182. (s. unter 5.3.1)

- Zweites Gesetz zur Änderung des Brandenburgischen Hochschulgesetzes vom 22. Mai 1996, GVBl. I S. 173

- Erstes Gesetz zur Änderung des Brandenburgischen Sozialberufsgesetzes vom 26. Juni 1996, GVBl. I S. 202 (s. unter 7.2.1.3)

- Brandenburgisches Architektengesetz (BbgArchG) vom 7. April 1997, GVBl. I S. 20 (s. unter 10.1.1)

Verordnungen und Verwaltungsvorschriften:

- Verordnung zur Dateibeschreibung (DBeschrV) vom 4. September 1996, GVBl. II S. 695 (s. unter 2.2)

- Verfahren zur Erteilung von Unschädlichkeitszeugnissen im Grundstücksverkehr vom 26. September 1996, ABl. S. 987 (s. unter 3.2.2)

- Überwachung der Einhaltung zulässiger Höchstgeschwindigkeiten und der Befolgung von Lichtzeichenanlagen im Straßenverkehr durch die Ordnungsbehörden im Land Brandenburg vom 15. September 1996, ABl. S.962

- Verordnung über die Zulassung zum Vorbereitungsdienst für ein Lehramt Vorbereitungsdienst Zulassungsverordnung (VorbZulV) vom 31. Juli 1996, GVBl. II S. 738
- Erste Verordnung zur Änderung der Ausbildungs- und Prüfungsordnung der Fachschulen vom 17. Dezember 1996,

GVBl. II S. 21

- Verordnung über die Ergänzungsstudien und Ergänzungsprüfungen für Lehrämter an Schulen (Ergänzungsprüfungsverordnung - EPV) vom 25. Juli 1996, GVBl. II S. 605 (s. unter 5.1.2)

- Verordnung über das Ergänzungsstudium und die Ergänzungsprüfung in Sonderpädagogik (Sonderpädagogik-Ergänzungsprüfung - SopEPV) vom 22. Januar 1997, GVBl. II S. 80

- Verordnung über die Berufung der Prüferinnen und Prüfer des Landesprüfungsamtes für Erste und Zweite Staatsprüfungen für Lehrämter an Schulen (Prüferberufungsverordnung - PrüfBerV) vom 25. Juli 1996, GVBl. II S.613 (s. unter 5.1.2)

- Verordnung über das Verfahren der Zustimmung und die Form der Führung ausländischer Grade (AGrV) vom 12. Juni 1996, GVBl. II S. 418

- Verordnung über die Erweiterung der Meldepflicht für übertragbare Krankheiten (SeuchMV) vom 8. Oktober 1996, GVBl. II S. 766 (s. unter 7.3.1.2)

- Verordnung über die Aufgaben des Kinder- und Jugendgesundheitsdienstes der Gesundheitsämter nach § 8 Abs. 2 des Brandenburgischen Gesundheitsdienstgesetzes (Kinder- und Jugend-Gesundheitsdienst-Verordnung - KJGDV) vom 25. Februar 1997, GVBl. II S. 96 (s. unter 7.3.1.3)

1.3 Technisch-organisatorische Maßnahmen bei der Einhaltung des Datenschutzes

1.3.1 Datenschutzfreundliche Technologien

Die stetige Weiterentwicklung der Informations- und Kommunikationstechnik (IuK-Technik), speziell im Bereich vernetzter Systeme und Chipkartenanwendungen, führt derzeit größtenteils noch dazu, daß auch immer mehr personenbezogene Daten erhoben, gespeichert und verknüpft werden. Die Wahrscheinlichkeit, daß Benutzer solcher Systeme elektronische Spuren hinterlassen, steigt rasant. Die damit im Zusammenhang stehende Möglichkeit, daß Persönlichkeitsprofile der Benutzer erstellt werden können, bedeutet für sich genommen schon die Gefahr einer Verletzung des Rechts auf informationelle Selbstbestimmung. Die wohl grundsätzlich angestrebte Nutzung solcher Persönlichkeits- oder Verhaltensprofile kann zunehmend in einer kaum noch kontrollierbaren Weise zur Verletzung der Persönlichkeitsrechte führen.

Ausgehend von der jetzigen Situation, daß vorwiegend technisch-organisatorische Maßnahmen zum Schutz der vorhandenen personenbezogenen Daten realisiert werden und damit der Schutz der Privatsphäre von der Wirksamkeit dieser Maßnahmen abhängt, müssen zukünftig neue Lösungsansätze zum Schutz der Privatsphäre des einzelnen gesucht und gefunden werden. Ausgehend von einer Untersuchung der Datenschutzbeauftragten von Holland und von Ontario (Kanada) zum sogenannten Identity Protector beschäftigt sich der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder mit der Formulierung von Forderungen zur

datenschutzfreundlichen Ausgestaltung von IuK-Technik[1].

Eine wesentliche Forderung zur datenschutzfreundlichen Ausgestaltung ist die Umsetzung der Prinzipien der Datenvermeidung und der Datensparsamkeit. Beim Prinzip der Datenvermeidung wird ein Höchstmaß an Anonymität gewahrt. Als Beispiele sind hier anonyme Zahlungsverfahren zu nennen, bei denen keine personenbezogenen Daten verarbeitet werden. Das Prinzip der Datensparsamkeit bedeutet, daß so wenig personenbezogene Daten wie nur möglich verarbeitet werden. Eine entscheidende Rolle spielen dabei die Anonymisierung, aber auch die Pseudonymisierung personenbezogener Daten. Bei der Pseudonymisierung, als der schwächsten Form der Datensparsamkeit, werden anstatt Identitätsdaten Pseudonyme verwendet. Von einem Pseudonym kann man grundsätzlich keinen unmittelbaren Rückschluß auf die Identifikationsdaten ziehen. Im wesentlichen unterscheidet man drei Klassen von Pseudonymen:

- selbstgenerierte Pseudonyme (der Benutzer generiert sich seine Pseudonyme selbst),

- Referenz-Pseudonyme (die Pseudonyme werden durch Dritte vergeben und der Personenbezug kann nur mit Hilfe einer Referenzliste wieder hergestellt werden),

- Einweg-Pseudonyme (die Pseudonyme werden mittels Einweg-Funktionen aus den personenbezogenen Identitätsdaten gebildet).

Ein praktisches Beispiel zur Verwendung von Einweg-Pseudonymen wird unter 6.1 beschrieben.

1.3.2 Datensparsamkeit bei der Nutzung interner TK-Anlagen

Viele öffentliche Stellen nutzen heute interne Telekommunikationsanlagen (TK-Anlagen) und speichern parallel zum Anbieter der TK-Leistung Verbindungsdaten abgehender Gespräche für eine eigene Gebührendatenverarbeitung mit folgenden Zielen:

- Ermittlung der Telefonkosten zum einen für dienstliche und zum anderen für private Gespräche,

- Aufteilung der dienstlichen Telefonkosten auf mehrere Kostenstellen oder unterschiedliche Nutzer der TK-Anlage,

- Zuordnung der Kosten von privat geführten Telefonaten auf die einzelnen Mitarbeiter,

- Überprüfung der monatlichen Telefonrechnung des Anbieters der Telekommunikationsleistung,

- stichprobenartige Kontrolle der Daten dienstlicher Gespräche hinsichtlich kostenbewußter Inanspruchnahme bzw. mißbräuchlicher Nutzung der TK-Anlage.

Die meisten Hersteller von TK-Anlagen bieten hierfür ein variables zweistufiges Verfahren zur Gebührendatenverarbeitung an. Bei diesem Verfahren werden in einer ersten Stufe alle Verbindungsdaten am Gesprächsende kurzzeitig in einem Verbindungsdatensatz in der TK-Anlage abgelegt. In einem zweiten Schritt werden sie dann in bestimmten Zeitintervallen - mindestens jedoch täglich - an einen separaten Gebührencomputer übermittelt und können dort in vielfältiger Weise

[1] s. Anlage 7

selektiert, ergänzt und ausgewertet werden. Der Gebührencomputer kann in der Regel für abgehende dienstliche und private Gespräche bis zum Ausgleich der Rechnung einen Gebührendatensatz mit folgendem Inhalt speichern, wobei herstellerbedingte Abweichungen möglich sind:

- Datum, Uhrzeit und Dauer des Gesprächs,

- Kennzeichen für den rufenden Teilnehmer (z. B. Nebenstellennummer, Personalnummer, Abrechnungsnummer, Organisationseinheit),

- Rufnummer und ggf. die Vorwahlnummer des angerufenen Teilnehmers, teilweise mit um zwei bis vier Ziffern verkürzter Rufnummer,

- Anzahl der Gebühreneinheiten, meist unterteilt nach einzelnen Gebührenzonen, auf der Grundlage des Gebührenimpulses vom Anbieter der TK-Leistung,

- Kennzeichen für Dienst- oder Privatgespräch,

- ggf. weitere Kennzeichen für Amtsleitung, Art des Verbindungsaufbaus, Art des Dienstes usw.

Während der Gebührenabrechnung erfolgt in den meisten Anlagen eine Zuordnung der Gebührendatensätze zu einer Stammdatendatei, die zum Teil auch als internes Telefonverzeichnis genutzt wird und u. a. folgende Informationen enthält:

- Kennzeichen für die Nebenstelle des rufenden Teilnehmers (z. B. Nebenstellennummer, Personalnummer, Abrechnungsnummer, Organisationseinheit),

- Name, Titel, Dienstbezeichnung,

- Name oder Kurzbezeichnung der Struktureinheit oder des Nutzers,

- Kostenstelle und ggf. weitere Abrechnungsinformationen,

- Nutzungs- oder Abrechnungskennzeichen,

- Gebührenfaktor.

Die einzelnen Hersteller der TK-Anlagen bieten in ihrer Gebührendatenverarbeitung meist ein umfangreiches Spektrum unterschiedlicher Auswertungslisten an, aus denen der Nutzer entsprechend seiner konkreten Bedürfnisse auswählen kann, und heben in ihren Angeboten insbesondere auf die vielfältigen, flexiblen Auswertungsmöglichkeiten ihrer Software für die Gebührendatenverarbeitung ab.

Viele Hersteller von TK-Anlagen lassen den Verbindungsdatensatz bei der Übernahme aus der TK-Anlage in den Gebührencomputer zunächst im wesentlichen unverändert und bilden daraus einen Gebührendatensatz mit annähernd gleichem Inhalt. So entsteht im Gebührencomputer ein Datenbestand mit detaillierten Informationen darüber, wer zu welchem Zeitpunkt wie lange mit welchem Teilnehmer telefoniert hat, der außer zur Gebührenabrechnung und

Kostenkontrolle auch zur individuellen Leistungs- und Verhaltenskontrolle genutzt werden kann. Diese Datenbanken werden in der Regel mindestens bis zum Ausgleich der Fernmelderechnung vorgehalten. Da sich der nicht unbeträchtliche organisatorische Aufwand für die Abrechnung von Privatgesprächen monatlich nicht lohnt, entstehen - abhängig vom Abrechnungszyklus - Speicherfristen von bis zu 6 Monaten und länger. Die übliche Verfahrensweise, bei der zunächst alle Verbindungsdaten gespeichert und bei der Auswertung lediglich bestimmte sensible Daten nicht auf Rechnungen und Listen ausgedruckt werden dürfen, reicht angesichts der umfangreichen Auswertungsmöglichkeiten der Datenbestände zur Unterbindung weiterführender individueller Leistungs- und Verhaltenskontrollen nicht aus.

Das Prinzip der Erforderlichkeit der Daten im Sinne der Datensparsamkeit sollte deshalb bereits bei der Datenspeicherung - spätestens jedoch bei der Übernahme der Daten von der TK-Anlage in den Gebührencomputer - angewandt werden. Die Selektion und Verdichtung der Verbindungsdaten sollte daher unmittelbar nach ihrer Übernahme in den Gebührencomputer erfolgen, die vollständigen Verbindungsdaten sollten danach gelöscht werden. So sind im Gebührencomputer im Regelfall nur noch die Gebühreneinheiten - ggf. fortlaufend addiert - zu speichern und vollständige Verbindungsdatensätze nur dann, wenn sie später auch tatsächlich zur Kostenkontrolle oder zum Nachweis von Privatgesprächen ausgewertet werden.

Für die Zuordnung von Telefongebühren für dienstliche Gespräche auf einzelne Kostenstellen bedarf es keiner Übernahme von Verbindungsdatensätzen in den Gebührencomputer. Lediglich wenn die kostenbewußte Nutzung der TK-Anlage kontrolliert werden soll, wären die Gebührendatensätze für besonders ausgewählte Telefongespräche (z. B. oberhalb einer bestimmten Gebühr) zu speichern.

Um die mißbräuchliche Nutzung dienstlicher Gespräche für private Zwecke zu unterbinden, genügt es, die Verbindungsdaten von stichprobenartig ausgewählten Dienstgesprächen zu speichern und zu überprüfen. Das kann mittels Zufallsgenerator oder durch sonstige zufällige Auswahl zum Beginn des Abrechnungszeitraumes erfolgen.

Für Privatgespräche sollte jedem Nutzer ein Wahlrecht eingeräumt werden, ob die Einzelgebühren oder nur die kumulativen Gesamtgebühren gespeichert werden. Geschieht letzteres, verzichtet der Nutzer jedoch auf die Möglichkeit einer Reklamation der Privatgesprächsabrechnung. Beides läßt sich aber auch datenschutzgerecht kombinieren, indem die Einzelverbindungsdaten lediglich mit verkürzter Zielrufnummer und die hierdurch entstandenen Gebühren ausgedruckt werden.

1.3.3 Verschlüsselung und digitale Unterschrift

Bereits in meinem 3. Tätigkeitsbericht[2] habe ich mich mit kryptographischen Verfahren auseinandergesetzt. Seitdem hat sich auf dem Gebiet der Verschlüsselung eine Menge getan, sei es weil diverse Firmen den am Horizont erscheinenden großen Markt der Verschlüsselungs- und Signaturwerkzeuge entdeckt haben oder weil sich die Politik derzeit intensiv mit dieser Materie auseinandersetzt. Positiv bewerte ich, daß die "Geburt" eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) kurz bevorsteht. Im Entwurf dieses Gesetzes sind u. a. folgende Artikel enthalten:

- Artikel 1: Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG)
- Artikel 2: Gesetz über den Datenschutz bei Telediensten (TDDSG)

[2] s. unter 1.3.5 ff.

- Artikel 3: Gesetz zur digitalen Signatur (Signaturgesetz - SigG)

Weitere Artikel befassen sich mit der Änderung diverser Rechtsvorschriften. In diesem Gesetz werden Rahmenbedingungen für digitale Signaturen definiert, so daß digitale Signaturen als sicher gelten oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können. Es bleibt zu hoffen, daß dieses Gesetz schnellstmöglich verabschiedet wird, um u. a. potentiellen Nutzern den Weg zur Nutzung der digitalen Signatur zu ebenen. Das Signaturgesetz stellt die Voraussetzung für die Anerkennung der Rechtsverbindlichkeit elektronisch gespeicherter Daten, z. B. bei der Übertragung in Netzen, dar.

Allerdings ist anzumerken, daß es auch einflußreiche Interessengruppen in der Bundesrepublik gibt, die eine freie Nutzung kryptographischer Verfahren gesetzlich verbieten wollen. Nach ihrer Auffassung darf nicht der Fall eintreten, daß durch Einführung neuer Technologien - hier Verschlüsselungsverfahren - die Bekämpfung der organisierten Kriminalität eingeschränkt wird. Dabei wird davon ausgegangen, daß auch Strafverfolgungsbehörden bei der verschlüsselten Übertragung von Daten keinen lesbaren Zugriff mehr haben.

Aus meiner Sicht läuft jedoch eine Reglementierung der Nutzung kryptographischer Verfahren ins Leere. Einerseits gibt es heutzutage genügend andere Möglichkeiten - z. B. durch steganographische Verfahren -, Nachrichten versteckt und damit unentdeckt zu übertragen; andererseits wäre eine Reglementierung aus Sicht des Datenschutzes unverhältnismäßig. Nur weil eine Minderheit (Kriminelle) ihre Daten verschlüsselt übertragen könnten, wird der Mehrheit die Nutzung solcher Verfahren erheblich eingeschränkt.

In einem Arbeitspapier der Arbeitsgruppe Kryptographie des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden die "Grenzen und Möglichkeiten der staatlichen Reglementierung des Einsatzes von Verschlüsselungsverfahren"[3] näher erörtert.

1.3.4 Anforderungen zur informationstechnischen Sicherheit bei Chipkartensystemen

[3] s. Anlage 11

Bereits in meinem 2. Tätigkeitsbericht[4] hatte ich mich ausführlich zur datenschutzgerechten Ausgestaltung von Chipkartenanwendungen geäußert. Im Berichtszeitraum ist mit Pilotprojekten begonnen worden, die den zukunftsorientierten Einsatz von Chipkarten betreffen. Für Brandenburg wird das Berliner Projekt "Die Mobilitätskarte" relevant, die sich auch auf das Umland von Berlin erstreckt. Mit dieser Chipkarte soll das bargeldlose Bezahlen in Bus, Bahn und Supermärkten, aber auch in öffentlichen Einrichtungen wie Bädern und Museen, ermöglicht werden. Dieses Projekt werde ich auch weiterhin in bezug auf anonyme Zahlungsverfahren sehr kritisch verfolgen.

Die Arbeitsgruppe "Chipkarten" des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen Anforderungskatalog zur informationstechnischen Sicherheit bei Chipkarten erarbeitet[5]. Die in diesem Katalog definierten Anforderungen richten sich an Entwickler und Hersteller sowie an Betreiber von Chipkartensystemen, aber auch an Nutzer, die zukünftig beabsichtigen, Chipkartenlösungen einzusetzen.

1.3.5 Fernwartung von Informations- und Kommunikationstechnik

Im Berichtszeitraum mußte ich feststellen, daß bei der Durchführung von Fernwartungen teilweise nur ungenügende technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten von den jeweiligen Einrichtungen realisiert wurden (s. unter 7.3.2.4). Obwohl mit § 11 a BbgDSG (allgemeine Regelung) sowie mit § 9 der KHDsV[6] (spezielle Regelungen) Bestimmungen zur Wartung und Fernwartung in Brandenburg existieren, kann das nicht darüber hinwegtäuschen, daß die praktische Umsetzung technisch-organisatorischer Maßnahmen in vielen Fällen nach wie vor als äußerst unbefriedigend anzusehen ist.

In aller Regel wird eine Fernwartung unter Nutzung der allgemein und öffentlich zugänglichen Netze durchgeführt. Die Verantwortlichen der datenverarbeitenden Stelle sollten sich ständig vor Augen halten, welche Gefahren und Risiken bei der Durchführung einer Fernwartung entstehen können. Zum einen kann es zum Verlust der Vertraulichkeit der bei der Fernwartung zu übertragenden Daten kommen, da normalerweise die Daten derzeit überwiegend noch nicht verschlüsselt übertragen werden, zum anderen besteht die Möglichkeit, daß der Auftragnehmer unberechtigterweise auf personenbezogene Daten zugreift.

Schon vor der Einführung eines Fernwartungverfahrens sollte genauestens geprüft werden, ob nicht annähernd adäquate Lösungen für den verfolgten Zweck nutzbar sind. In vielen Fällen ließe sich ohne weiteres auf eine Fernwartung verzichten. So ist es z. B. aus meiner Sicht nicht erforderlich, daß das Einspielen von Software über Fernwartung realisiert wird. Änderungen an der Betriebssystemsoftware sind ebenfalls mit sehr hohen Risiken verbunden, da hierzu normalerweise Systemadministratorrechte benötigt werden, wodurch ein Zugriff auf das gesamte System - und damit auch auf alle personenbezogenen Daten - ermöglicht wird. In vielen Fällen kann auf eine Fernwartung verzichtet werden, indem z. B. Softwareänderungen lokal in das System eingespielt werden.

---

4 s. unter 1.4.2 ff.

5 s. Anlage 12

6 Krankenhausdatenschutzverordnung vom 4. Januar 1996, GVBl. II S. 54

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat 1993 eine Orientierungshilfe[7] zur Wartung und Fernwartung erarbeitet, die auch heute noch volle Gültigkeit hat. Weiterhin werden auch in den derzeit in Erarbeitung befindlichen Vorläufigen Verwaltungsvorschriften zur Durchführung des Brandenburgischen Datenschutzgesetzes (s. unter 2.1) konkrete Anforderungen zur Wartung und Fernwartung definiert. Die zu realisierenden technisch-organisatorischen Maßnahmen sind in einer Dienstanweisung zur Fernwartung festzuschreiben.

1.3.6 Umgang mit Telefax

Schon früher hatte ich mich zum Umgang mit Telefax geäußert[8]. Bei Prüfbesuchen habe ich festgestellt, daß jetzt häufiger als früher PC's mit Faxkarte eingesetzt werden. Oft erfolgt das Faxen aus einem lokalen Computernetz heraus.

Hierzu ist zu sagen: Ist der Fax-PC in ein lokales Netz eingebunden, ist dieses über die Faxkarte grundsätzlich von außen angreifbar und deshalb in bezug auf seine Vertraulichkeit und Verfügbarkeit gefährdet, weil Paßwörter ausgespäht und unbefugte Datenein- und -ausgaben realisiert werden können. Die einfachste Form, sein Hausnetz zu schützen, ist die, einen Fax-PC stets nur als Einzelplatz zu betreiben. Ansonsten wäre es unerläßlich, sämtliche Daten, die im Netz gespeichert und übertragen werden, nach einem anspruchsvollen kryptographischen Verfahren zu verschlüsseln, womit die Vertraulichkeit der Daten gesichert ist.

Damit ist allerdings noch nichts über die Schutzwürdigkeit der Daten gesagt, die ein Fax-PC versendet oder empfängt, und zwar unabhängig davon, ob er als Netzkomponente oder als Einzelplatz eingerichtet ist. Daten, die einer besonderen Geheimhaltung unterliegen, dürfen nur verschlüsselt gefaxt werden. Falls eine derartige Verschlüsselungseinrichtung nicht zur Verfügung steht, muß man auf eine Faxübertragung verzichten und ein anderes Verfahren für eine sichere Datenübermittlung wählen.

Aber auch die klassischen Faxgeräte sind durch unbefugte Ausspähung bedroht, wenn sie über eine Fernwartungsfunktion verfügen. Unter Umständen ist dem Anwender nicht einmal bewußt, daß sein Gerät eine solche Funktion besitzt, weil in dem mitgelieferten Handbuch nicht darauf hingewiesen wird. Auf jeden Fall ist im normalen Dienstbetrieb eine vorhandene Fernwartungsfunktion unbedingt zu deaktivieren.

Zu der hier geschilderten Problematik haben die Datenschutzbeauftragten des Bundes und der Länder kürzlich eine Empfehlung verabschiedet[9].

1.3.7 Regelungen für die Sicherheit bei Türen und Fenstern

Öffentliche Stellen, die selbst oder im Auftrag einer anderen öffentlichen Stelle personenbezogene Daten verarbeiten, sind nach § 10 Abs. 2 Satz 1 Nr. 1 BbgDSG gesetzlich verpflichtet, geeignete Maßnahmen zu treffen, um Unbefugten den Zugang zu den Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle). Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich dabei nach der Sensibilität der gespeicherten Daten, deren Zuordnung im

---

7 s. Anlage 9

8 s. 2. Tätigkeitsbericht unter 1.4.4 sowie Anlage 2

9 s. Anlage 8

Schutzstufenkonzept dargestellt ist.

Für die Durchführung baulicher Maßnahmen zur Zugangskontrolle sind eine Reihe von DIN-Vorschriften ergangen. Da es wiederholt Anfragen zu den Normen von Türen und Fenstern gab, möchte ich hier auf die wichtigsten DIN-Vorschriften zum Einbruchschutz hinweisen:

- DIN V 18054 Einbruchhemmende Fenster
- DIN V 18103 Einbruchhemmende Türen
- DIN 52290 Angriffhemmende Verglasung

Einbruchhemmend bedeutet, daß Türen oder Fenster in geschlossenem und verriegeltem Zustand Einbruchversuche mit körperlicher Gewalt für eine bestimmte Widerstandszeit verhindern. Sie werden entsprechend ihrer einbruchhemmenden Wirkung in folgende Widerstandsklassen eingestuft:

Türen	Fenster	Verglasung	Widerstandszeit in Minuten
-	EF 0	A 3	≥ 5
ET 1	EF 1	B 1	≥ 5
ET 2	EF 2	B 2	≥ 7
ET 3	EF 3	B 3	≥ 10

In der folgenden Tabelle wird bei den Widerstandsklassen für Türen der Tätertyp und mutmaßliche Vorgehensweisen zugeordnet. Für die Praxis bietet die Zuordnung lediglich einen Anhalt. Somit kann entsprechend der einzuschätzenden Risikosituation und der Lage des Objektes die gewünschte Widerstandsklasse ausgewählt werden.

Widerstands-klasse	Tätertyp Mutmaßliche Vorgehensweise
ET 1	Einbrecher ohne bzw. mit nur sehr geringem Werkzeug; er versucht, in erster Linie durch den Einsatz körperlicher Gewalt einzudringen: Gegentreten, Gegenspringen, Schulterwurf oder ähnliches
ET 2	wie bei Widerstandsklasse 1; der Einbrecher benutzt zusätzlich einfache Hebelwerkzeuge
ET 3	wie bei Widerstandsklasse 2; erfahrener Einbrecher; benutzt vorwiegend Werkzeug - Hebelwerkzeuge, Keile, kleinere Schlagwerkzeuge -, jedoch ohne den Einsatz von Elektrowerkzeugen

Die einbruchhemmende Wirkung ist jedoch immer relativ. Eine absolute Sicherheit gegen Einbrüche allein durch Verwendung dieser geprüften Türen und Fenster gibt es nicht. Hat ein erfahrener Einbrecher genügend Zeit, ist er mit

Spezialwerkzeug ausgestattet und kann er beliebig viel Lärm machen, dann bieten selbst Türen und Fenster der Widerstandsklasse 3 keinen Schutz mehr. Jede öffentliche Stelle muß deshalb abhängig von den territorialen Bedingungen und den zu erwartenden Gefahren selbst eine geeignete Lösung zur Sicherung von Türen und Fenstern finden und dabei in Betracht ziehen, ob eventuell zusätzliche Maßnahmen (z. B. Aufschalten einer Alarmanlage zur Polizei o. ä.) ergriffen werden. Hinweise, welche Kombinationen von Sicherungsmaßnahmen wirkungsvoll sind, können auch die polizeilichen Beratungsstellen geben.

1.4 Angleichung des BDSG an die EU-Datenschutzrichtlinie

Im Herbst 1995 ist die EU-Datenschutzrichtlinie[10] verabschiedet worden, die eine Umsetzung in das nationale Recht der Mitgliedsstaaten bis Ende 1998 erfordert. Inzwischen hat das Bundesinnenministerium Anfang des Jahres einen Entwurf vorgelegt, mit dem das BDSG an die Erfordernisse der Richtlinie angeglichen werden soll.

Wer die EU-Datenschutzrichtlinie zur Kenntnis genommen hat und daraufhin die Hoffnung schöpfte, daß die erforderliche Umsetzung in nationales Recht nun zum Anlaß genommen würde, die gesetzliche Ausformung des Datenschutzes in ein modernes, gutgegliedertes, den Anforderungen der fortschreitenden Technik und der veränderten Gesellschaft genügendes Datenschutzgesetz einzuarbeiten, der sieht sich enttäuscht. Der Referentenentwurf (Stand: 14.01.1997) führt zwar zahlreiche kleinere Änderungen ein, eine Neugestaltung des Gesetzes ist dabei aber nicht herausgekommen. In der Begründung des Gesetzentwurfes ist ausdrücklich vermerkt, daß mit der Novellierung nicht mehr als die Umsetzung der Datenschutzrichtlinie geleistet werden soll.

- Trennung zwischen öffentlichem und nicht-öffentlichem Bereich noch nicht überwunden

Nach dem Entwurf kann die Trennung zwischen öffentlichem und nicht-öffentlichem Bereich auch nach der Novellierung des BDSG erhalten bleiben, selbst wenn dies dem Wortlaut der Richtlinie nicht entspricht; in der Richtlinie wird diese Trennung gerade nicht vorgenommen. Eine Aufhebung der Trennung wäre jedoch ein Gebot der Stunde gewesen, ist es doch erklärter und überall zu beobachtender Trend, öffentliche Aufgaben an nicht-öffentliche Auftragnehmer zu geben und öffentliche Einrichtungen in private Rechtsformen zu gießen. Die Aufrechterhaltung der Trennung der gesetzlichen Vorgaben zwischen öffentlichen und nicht-öffentlichen Stellen ist bereits jetzt ein Anachronismus.

- Verankerung der Funktion des internen Datenschutzbeauftragten

Ungeachtet der den privaten Bereich betreffenden Regelungen wird es durch den neu eingefügten § 4 f des Entwurfs künftig auch in den öffentlichen Stellen des Bundes, die personenbezogene Daten automatisiert verarbeiten, einen (internen) Datenschutzbeauftragten geben.

- Datenschutz durch Begriffsdefinitionen

Die Vorschriften zum Datenschutz können auf sehr unterschiedliche Art und Weise eingehalten und die Einhaltung garantiert werden. Hierbei kommt den Begriffsbestimmungen besondere Bedeutung zu. Einer dieser Wege ist die Fiktion, daß bei Datenverarbeitung im Auftrag der Auftraggeber für die Einhaltung des Datenschutzes verantwortlich bleibt, obwohl er gar nicht an und bei der Verarbeitung beteiligt ist. Der Begriff "Verarbeiten" ist in § 3 des Entwurfs definiert und

[10] ABl. der EG (ABlEG) Nr. L 281 vom 23. November 1995, S. 31

umschrieben. Danach umfaßt er das Speichern, Verändern, Übermitteln, Sperren und Löschen. Gesondert genannt werden "Erheben" und "Nutzen". Damit soll dem Vorschlag der Datenschutzbeauftragten leider nicht gefolgt werden, die Begriffe "Erheben" und "Nutzen" in das "Verarbeiten" zu integrieren.

Es wäre nun zu erwarten gewesen, daß in der eigentlichen Regelung der Datenverarbeitung im Auftrag, in § 11 des Entwurfs, neben den Begriffen "Verarbeiten" und "Nutzen" auch das "Erheben" genannt würde. Obwohl dies nicht geschehen ist, bleibt es unbestreitbar, daß auch das Erheben von Daten "im Auftrag" erfolgen kann.

Der Begriff "Entscheidung" steht im Zentrum von § 6 a des Entwurfs, wonach Einzelentscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen, nicht auch ausschließlich auf Informationen oder Kenntnisse gestützt werden dürfen, die automatisiert gewonnen werden. Auch diese Vorschrift ist eine direkte Umsetzung einer Vorgabe der Richtlinie.

- Übermittlungen in andere Länder - Unterrichtungspflichten

Regelungen, die einen "Europäischen" Datenschutz ermöglichen, werden ergänzt durch solche, die die Übermittlung personenbezogener Daten in Drittländer betreffen (§ 4 b und 4 c des Entwurfs). Es wird sich zeigen, ob das von der Richtlinie anvisierte Niveau des Datenschutzes erreicht oder gehalten werden kann, vor allem deshalb, weil ja bereits das Gesetz zahlreiche Ausnahmen vorsieht, die zusätzlich ergänzt werden durch eine Ermächtigung für die Aufsichtsbehörde, weitere generelle oder besondere Ausnahmen von datenschutzrechtlichen Schutzbestimmungen zuzulassen. Der Entwurf selbst verweist auf vertragliche Regelungen. In der Begründung ist jedoch klargestellt, daß derartige Vertragsklauseln der Aufsichtsbehörde zur Genehmigung vorzulegen sind.

Zu der Sicherung eines staatenübergreifenden Datenschutzes gehören auch Unterrichtungsverpflichtungen, die gesetzlich verankert werden sollen. Hierzu sind allerdings noch zahlreiche untergesetzliche Vorschriften erforderlich, damit der hohe Anspruch umgesetzt werden kann. Die Formulierung "Die ... zuständigen Stellen unterrichten die zuständigen Stellen der übrigen Mitgliedstaaten der Europäischen Union .... über Dritte ..., die kein angemessenes Datenschutzniveau gewährleisten und über die ... erteilten Genehmigungen ..." ist derart vage, daß die Vorschrift aus sich heraus nicht umsetzbar sein dürfte.

- Novellierungsbedarf in den Ländern

Unabhängig vom Novellierungserfordernis des BDSG müssen auch die Landesdatenschutzgesetze an die EU-Datenschutzrichtlinie angepaßt werden. In den Landesdatenschutzgesetzen wird vor allem die Pflicht zum Bestellen von internen (örtlichen) Datenschutzbeauftragten zu verankern sein, und zwar für alle öffentlichen Stellen, mit Ausnahme derjenigen, die personenbezogene Daten ausschließlich für eigene Zwecke verarbeiten.
Außerdem ist es besonders wichtig, das sog. "outsourcing", das Verlagern öffentlicher Aufgaben auf private Stellen, (weltweit) zu regeln. Insbesondere das zunehmend zu beobachtende Verlagern von Kommunalaufgaben bedarf dringend detaillierter landesgesetzlicher Regelungen.

1.5 Landtag

1.5.1 LT-Drs. ../....

Landtagsdrucksachen geben gelegentlich Anlaß, sich mit datenschutzrechtlichen Anliegen auseinanderzusetzen. So sind im Zusammenhang mit parlamentarischen Initiativen, wie z. B. Kleinen Anfragen, aber auch in Verbindung mit der Rechnungslegung der Fraktionen, gem. § 10 Fraktionsgesetz (FraktG)[11] Namensnennungen vorgekommen. Soweit ich davon Kenntnis erhielt, bin ich an die Fraktionsvorsitzenden herangetreten und habe diese ersucht, künftig Abhilfe zu schaffen.

Das parlamentarische Interesse, bestimmte Sachverhalte aufzuklären oder darüber zu informieren, wird selbstverständlich durch datenschutzrechtliche Regelungen nicht verhindert. Art. 56 Verfassung des Landes Brandenburg[12] garantiert den Mitgliedern des Landtags des Landes Brandenburg einen allgemeinen Informationszugang sowie ein uneingeschränktes Fragerecht und verpflichtet die Landesregierung zur Auskunftserteilung, es sei denn, daß dem ein überwiegendes öffentliches oder privates Interesse an der Geheimhaltung entgegensteht. Allerdings schreibt auch die Brandenburgische Verfassung in Art. 11 das Recht auf informationelle Selbstbestimmung fest. Wo verfassungsrechtlich geschützte Rechtsgüter aufeinandertreffen, ist ein Ausgleich dergestalt herbeizuführen, daß jedes von ihnen "an Wirklichkeit gewinnt". Dies gilt um so mehr, wenn der Name von Betroffenen im Zusammenhang mit Lebenssachverhalten genannt wird, die diese im allgemeinen nicht einer breiten Öffentlichkeit zugänglich machen wollen. Selbst wenn Namen in solchen Fällen bereits an anderer Stelle öffentlich bekannt gemacht worden sind, kann auch dies nicht einen erneuten Eingriff in das Persönlichkeitsrecht rechtfertigen. Daher regte ich an, lediglich die Anfangsbuchstaben des Vor- und Nachnamens anzugeben, wenn überhaupt Personenangaben unerläßlich sind, um einen Sachverhalt eindeutig einzugrenzen. Dieses Verfahren dürfte in aller Regel ausreichen, der Landesregierung zu ermöglichen, ihrer Auskunftspflicht nachzukommen.

Bei den Vorlagen der Fraktionen, wie z. B. dem Rechnungslegungsbericht gem. § 11 FraktG, ist der Landtagspräsident lediglich zu deren Veröffentlichung verpflichtet. Eine inhaltliche Prüfung durch ihn könnte sich allenfalls auf die Einhaltung der gesetzlich vorgeschriebenen Mindestanforderungen erstrecken, nicht jedoch auf eine darüber hinausgehende unerlaubte Offenlegung von personenbezogenen Daten.

1.5.2 Rederecht des Landesbeauftragten für den Datenschutz vor dem Landtag

Es hat sich im Berichtszeitraum gezeigt, daß "Unklarheiten" über die Befugnisse des Landesbeauftragten für den Datenschutz bestehen, im Landtag Brandenburg das Wort zu ergreifen. Dazu vertrete ich die Auffassung, daß dem Landesbeauftragten für den Datenschutz das Rederecht vor dem Plenum zusteht und stütze sie auf folgende Auslegung der Verfassung des Landes Brandenburg und des Brandenburgischen Datenschutzgesetzes.

Das Brandenburgische Datenschutzgesetz sieht in § 23 Abs. 5 das Rederecht für den Landesbeauftragten für den Datenschutz vor. Die später verabschiedete Landesverfassung erwähnt diesbezüglich im Art. 66 Abs. 2 nur die Mitglieder des Landtages und die Landesregierung. Einschlägiger Artikel der Verfassung des Landes Brandenburg für den Landesbeauftragten für den Datenschutz ist jedoch Art. 74. Neben seinen Aufgaben, das Grundrecht auf Datenschutz zu wahren, finden sich hierin einige Vorgaben für das Amt, den Amtsinhaber und dessen Rechte und Pflichten. Wesentlicher ist in diesem Zusammenhang Abs. 3, nach dem das Nähere ein Gesetz regelt. Dies stellt eine Ermächtigung an den Gesetzgeber dar, die Verfassungsvorgabe auszufüllen. Diese Aufforderung ist der Gesetzgeber in § 23 Abs. 5 Satz 1 BbgDSG nachgekommen, der dem Landesbeauftragten das Recht explizit verankert. Dies ist durch die Novellierung des

---

[11] vom 29. März 1994, GVBl. I S. 80

[12] vom 20. August 1992, GVBl. I S. 298, geänd. d. Art. 2 d. NVG vom 27. Juni 1995, GVBl. I S. 150

Brandenburgischen Datenschutzgesetzes noch einmal ausdrücklich bestätigt worden. Dem kann auch nicht die Geschäftsordnung des Landtages als innerparlamentarische Regelung (eine autonome Satzung und im Rang unterhalb des Gesetzes stehend) entgegengehalten werden.

1.6 Staatskanzlei

1.6.1 Rundfunkstaatsvertrag

Das Land Brandenburg befindet sich zur Zeit in Verhandlungen mit dem Land Berlin mit dem Ziel, eine Novellierung des "Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks" zu erreichen. Die Staatskanzlei übersandte mir deshalb Anfang Oktober 1996 den Entwurf mit der Bitte um Durchsicht und Stellungnahme.

Da inzwischen der dritte Runkfunkänderungsstaatsvertrag verabschiedet worden ist, sollen einige von diesem abhängige Änderungen in dem Staatsvertrag berücksichtigt und darüber hinaus weitere neue Komponenten in den Staatsvertrag eingearbeitet und der Datenschutz ausdrücklich geregelt werden:

- Der Entwurf ist darauf ausgerichtet, daß in Angelegenheiten des Datenschutzes das Berliner Datenschutzgesetz gelten und der Berliner Datenschutzbeauftragte im Zusammenhang mit dem Rundfunkstaatsvertrag die Kontrolle übernehmen soll. Diese einseitig auf Berlin ausgerichtete Lösung ist aus meiner Sicht nicht folgerichtig, da es doch um die gleichwertige Zusammenarbeit zweier Bundesländer geht. Ich habe daher in bezug auf die Kontrollkompetenz vorgeschlagen, diese - in Anlehnung an die vorgesehene Rechtsaufsicht - in einem zweijährigen Turnus im Wechsel dem LfD Berlin und mir zu übertragen. Die Anwendung des in Berlin anzuwendenden Datenschutzrechts halte ich hingegen für sinnvoll, da insoweit aus Gründen der Rechtssicherheit weder ein Wechsel noch eine regionale Aufteilung der Geltung einer bestimmten Rechtsvorschrift in Frage kommen kann.
- Aber auch die Vorschriften für den Datenschutz im engeren Sinne sollten verbessert werden. So sind die Löschungsfristen für die Vorhaltung von Abrechnungsdaten ganz konkret festzulegen und eine klare Regelung zur Berichtspflicht in den Tätigkeitsberichten der Rundfunkanstalten zu treffen.

Die Landesregierung hat zwar zunächst meine Anregung aufgegriffen, diese haben sich jedoch im Staatsvertrag selbst nicht durchsetzen lasssen, so daß jetzt das Territorialprinzip für die datenschutzrechtliche Kontrollkompetenzen gelten soll.

1.6.2 Teilnehmerlisten bei Veranstaltungen der Brandenburgischen Landeszentrale für politische Bildung

Bei Veranstaltungen, die durch die Brandenburgische Zentralstelle für politische Bildung (BLZpB) gefördert werden, wurden die Teilnehmer gebeten, sich mit voller Anschrift in die Teilnehmerliste einzutragen. Eine Petentin empfand die Vorgehensweise als "Adreßsammelwut" und wandte sich an mich.

Derartige Veranstaltungen werden aus öffentlichen Mitteln gefördert. Die BLZpB ist als Bewilligungsbehörde zur Nachprüfung über die Verwendung der Mittel verpflichtet. Dazu muß nachvollziehbar sein, wer an den Veranstaltungen teilgenommen hat. Ich regte an, auf die Angabe der vollständigen Adresse zu verzichten, da die Angabe des Wohnortes zum Nachweis ausreicht, daß es sich bei dem Teilnehmer "X" einer von der BLZpB geförderten Veranstaltung um einen Bürger Brandenburgs (ja/nein) im Alter über/unter 18 Jahre - jeweils durch die eigenhändige Unterschrift bestätigt - handelt.

Die BLZpB teilt meine Bedenken, daß die Erhebung der Anschrift insbesondere bei Tages- und Abendveranstaltungen nicht unbedingt erforderlich sein muß. Deshalb wird sie zukünftig in diesen Fällen prüfen, ob ein Verzicht auf die Erhebung gegenüber dem Zuwendungsempfänger als Ausnahme im Bewilligungsbescheid zugelassen werden kann. Des weiteren will die BLZpB Teilnehmerlisten mit dem Zusatz versehen, daß sie nur für abrechnungstechnische Zwecke benötigt und anschließend dem Veranstalter zurückgereicht werden. Zum anderen stellte die BLZpB mir eine Neufassung der Förderichtlinie unter Berücksichtigung der bisher mit ihr gemachten Erfahrungen in Aussicht.

Unterdessen hat mir die BLZpB dazu einen Entwurf einschließlich eines überarbeiteten Formulars der Teilnehmerliste zugesandt. In dieser sind die Angaben (Alter, Beruf und Anschrift) der Teilnehmer an einer Abend- oder Tagesveranstaltung nicht einzutragen. Erforderlich ist die Angabe des Wohnsitzes der Teilnehmer, um eine Bewertung der Teilnehmerstruktur nach Abschluß der Veranstaltungen vornehmen zu können. Insbesondere bei landesübergreifenden Maßnahmen, wenn eine Kooperation mit der Bundeszentrale für politische Bildung vorliegt, ist der Nachweis über Teilnehmer von mindestens drei verschiedenen Ländern nach der Richtlinie des Bundesministeriums des Innern[13] erforderlich. Bei Veranstaltungen mit Übernachtungen ist ferner eine Bestätigung über die Dauer und den Ort der geförderten Übernachtung vorzulegen, um den entstandenen Aufwand anerkennen zu können. Diesem Entwurf der Richtlinie habe ich zugestimmt.

1.6.3 Kontrolle des TK-Verbundes der obersten Landesbehörden

[13] vom 7. Juni 1994, GMBl. S. 457

Im Berichtszeitraum habe ich den im Jahre 1993 in Betrieb gegangenen Telekommunikations-Verbund (TK-Verbund) der obersten Landesbehörden[14] geprüft. Diesem sind alle Standorte der Landesregierung Brandenburg im Territorium Potsdam angeschlossen. Der Zentrale der TK-Anlage, die über Schnittstellen Zugriff auf die Teilrechner in den einzelnen Standorten erhält, obliegt die Steuerung, Verwaltung und Gebührenabrechnung für das Gesamtsystem. Dazu muß eine Vielzahl umfangreicher zentraler Dateien - meist mit personenbezogenen Daten - angelegt, gepflegt und in vielfältiger Weise ausgewertet und miteinander verknüpft werden. Die Zentrale wird bei der Staatskanzlei betrieben. Ein Personalbestand von insgesamt 12 Mitarbeitern sichert die Vermittlung von Gesprächen, die Wartung und Pflege der Hard- und Software, die Gebührendatenverarbeitung und die Gebührenabrechnung.

Die Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher TK-Anlagen für die Verwaltung des Landes Brandenburg (Dienstanschlußvorschrift - DAV)[15] und eine Musterdienstvereinbarung über die Nutzung der ISDN-TK-Anlage des TK-Verbundes der obersten Landesbehörden des Landes Brandenburg (Musterdienstvereinbarung) bilden die rechtlichen Grundlagen für ihren Betrieb. Der Musterdienstvereinbarung, die jede Ressortleitung gleichlautend mit ihrem Personalrat auf der Grundlage des § 65 Ziff. 2 PersVG[16] abschloß, bedurfte es, um einen einheitlichen Betrieb des TK-Verbundes zu gewährleisten.

Die Zielstellung der Prüfung in der Zentrale des TK-Verbundes bestand in der Kontrolle der Einhaltung der für alle Ressorts identischen allgemeinen Rahmenbedingungen sowie der o. g. Rechtsgrundlagen für den Betrieb der TK-Anlage.

Im folgenden können nur einige Schwerpunkte aus dem Prüfbericht dargelegt werden, den ich der Staatskanzlei als verantwortliche Betreiberin des TK-Verbundes, allen am TK-Verbund beteiligten obersten Landesbehörden und gem. Anlage 2 Abs. 6 Musterdienstvereinbarung den zuständigen Personalräten übermittelt habe (Im übrigen verweise ich auf meine Ausführungen zur Datensparsamkeit bei der Nutzung interner TK-Anlagen unter 1.3.2.).

1.6.3.1 Zentrale Gebührendatenverarbeitung

Das Gesamtsystem der Gebührendatenverarbeitung besteht aus einem Gebührenrechner in der Zentrale des TK-Verbundes und 10 weiteren Nebenrechnern in den einzelnen Standorten.

In einer ersten Verarbeitungsstufe werden die Verbindungsdaten für jedes gebührenpflichtige Einzelgespräch in sog. Verbindungsdatensätzen an den einzelnen Standorten bis zu ihrer Übernahme in den zentralen Gebührenrechner zwischengespeichert. Diese Übernahme erfolgt vom Standort 1 (Staatskanzlei) sofort nach Gesprächsende und von den anderen 10 Standorten in der Regel automatisch nachts über Modem-Leitungen.

Entgegen den Bestimmungen in Pkt. 3.1.1 Abs. 3 DAV - in dem auf die Erforderlichkeit der vorzuhaltenden Daten abgestellt wird - beinhaltet der Verbindungsdatensatz, der für die Dauer von zwei Monaten für jedes gebührenpflichtige Dienst- und Privatgespräch gespeichert wird, nach der Übertragung zum zentralen Gebührenrechner noch folgende Informationen:

- Nummer des rufenden Teilnehmers,

---

[14] s. 2. Tätigkeitsbericht unter 11.1 und 3. Tätigkeitsbericht unter 10.3

[15] Runderlaß des Ministeriums des Finanzen Nr. 17 - 01340 - 180/93 am 30. November 1993, ABl. 1993 S. 1775

[16] Personalvertretungsgesetz für das Land Brandenburg vom 15. September 1993, GVBl. I S. 358

- Nummer des gerufenen Teilnehmers (Bei Dienstgesprächen wird seit Mai 1996 die volle Rufnummer durch Sterne überschrieben. Bei Privatgesprächen werden die letzten drei Ziffern der Rufnummer durch Sterne überschrieben. Bei zu überprüfenden Dienstgesprächen wird die volle Vorwahl- und Rufnummer dargestellt.),

- Gesprächsdatum,

- Beginn der Verbindung,

- Ende der Verbindung,

- Gesprächsdauer in Sekunden,

- Gebühreneinheiten (werden von der Telekom geliefert),

- verschiedene Kennzeichen (für Dienst- oder Privatgespräche, für die Art des Verbindungsaufbaus, für die Amtsleitung, für die Art des Dienstes usw.).

Die Datei der Verbindungsdaten wird zur Gebührenermittlung mit einer Datei "Stammdaten" verknüpft. Sie enthält u. a. folgende Informationen:

- Nummer des rufenden Teilnehmers,

- Kostenstelle,

- Bemerkung 1 (bei zu überprüfenden Dienstgesprächen mit einem "Stern" versehen),

- Gebührenfaktor,

- Name, Vorname, Abteilung lang, Abteilung kurz, Ort (Diese Felder sind nur bei vorübergehenden Fremdnutzern des TK-Verbundes, z. B. Baufirmen und Pressevertreter, belegt.).

Damit werden mit dem derzeit praktizierten Verfahren der Gebührendatenverarbeitung weit mehr Daten als erforderlich gespeichert. Darüber hinaus wird für jedes gebührenpflichtige Einzelgespräch ein derartiger Verbindungsdatensatz sogar mit der vollständigen Zielrufnummer bis zur automatischen Übernahme in den zentralen Gebührencomputer zwischengespeichert. Nur vom Standort 1 (Staatskanzlei) erfolgt die Übernahme der Verbindungsdaten sofort nach Gesprächsende. Selbst nach der Übernahme in den zentralen Gebührencomputer bleiben alle Verbindungsdatensätze vollständig erhalten, lediglich die Zielrufnummer wird teilweise modifiziert.

1.6.3.2 Speicherung von Verbindungsdaten für Dienstgespräche

Da zur Gebührenermittlung am Monatsende nur die von der Telekom gelieferten Gesprächseinheiten benötigt und ausgewertet werden, sind die übrigen Daten (Gesprächsdatum; Beginn, Ende und Dauer des Gespräches) nicht mehr erforderlich und dürfen auch nicht über das Ende einer Verbindung hinaus gespeichert werden. Es ist insoweit nicht nachvollziehbar, weshalb bei der Übernahme der Gebührendatensätze in den zentralen Gebührencomputer nicht bereits

eine Akkumulation der Gebühren für die einzelnen Kostenstellen erfolgt und die Gebührendatensätze danach gelöscht werden.

1.6.3.3 Speicherung von Verbindungsdaten für Privatgespräche

Gem. § 6 Abs. 3 Musterdienstanweisung haben die Mitarbeiter der obersten Landesbehörden die Möglichkeit zu wählen, ob sie die in Rechnungstellung ihrer privat geführten Telefonate als Einzel- (verkürzt um die letzten drei Ziffern der Zielnummer) oder Gesamtgebührennachweis - und damit ohne Reklamationsmöglichkeit - wünschen.

Bei der Umsetzung dieser Wahlmöglichkeit im TK-Verbund werden aber zunächst für jedes Privatgespräch die unter Ziff. 1 genannten Informationen gespeichert und erst danach erfolgt die Auswahl, ob diese überhaupt für den Ausdruck eines Einzelverbindungsnachweises erforderlich sind. Die Bestimmungen in der Musterdienstvereinbarung dienen aber gerade dem Ziel, daß Mitarbeiter unter Verzicht auf einen Einzelverbindungsnachweis und das Reklamationsrecht bei der Abrechnung von Privatgesprächen die Speicherung der Verbindungsdaten durch den Arbeitgeber verhindern können.

Während der Einzelgebührennachweis am Monatsende den Mitarbeitern direkt von der Staatskanzlei zugestellt wird, erhalten die Ressorts zusätzlich einen Ausdruck, der für jeden Gesprächsteilnehmer die Informationen Rufnummer des Teilnehmers, Anzahl der geführten Gespräche, Gesprächsdauer, Einheiten und Betrag enthält. Diese Vorgehensweise ist durch die Bestimmungen in Pkt. 3.2.4 DAV nicht abgedeckt.

Bei konsequenter Umsetzung des Gebots der Datensparsamkeit (s. unter 1.3.2) würde zu Abrechnungszwecken der Ausdruck der Teilnehmer-Nr. des Mitarbeiters und des monatlichen kumulativen Gesamtbetrages für den jeweiligen Teilnehmer völlig ausreichen. Bei den übrigen gespeicherten Daten besteht ständig die Gefahr, daß sie zur Verhaltenskontrolle der Mitarbeiter - beispielsweise bzgl. ihrer während der Dienstzeit privat geführten Orts- oder Ferngespräche - herangezogen werden. Eben dies sollte durch die Bestimmungen der Dienstanschlußvorschrift und der Musterdienstanweisung aber ausgeschlossen werden.

1.6.3.4 Überprüfung der Daten von dienstlichen Gesprächen

Eine mißbräuchliche Nutzung des dienstlichen Telefonanschlusses liegt u. a. dann vor, wenn ein Mitarbeiter ein Privatgespräch führt, es aber nicht als ein solches kennzeichnet, und demzufolge die Kosten dafür seinem Arbeitgeber anlastet.

Um dem entgegenzuwirken und damit zugleich eine vollständige Überwachung des TK-Verhaltens von Beschäftigten zu vermeiden, sieht § 7 Musterdienstvereinbarung eine stichprobenartige Kontrolle dienstlicher Gespräche vor. Nur in diesem engbegrenzten Rahmen ist es erlaubt, die komplette Rufnummer des angerufenen Teilnehmers zu speichern, auszudrucken und anschließend einer geeigneten Überprüfung zu unterziehen.

Das derzeitige Kontrollverfahren von Dienstgesprächen in der Staatskanzlei entspricht zwar den Festlegungen der Dienstanschlußvorschrift und der Musterdienstvereinbarung. Die vorliegende Kontrollmethode birgt - bedingt durch die Art der Datenspeicherung - allerdings erhebliche datenschutzrechtliche Risiken. So ist es möglich, durch den Eintrag des Zeichens "Stern" im Feld Bemerkung 1 der Datei Stammdaten aller Beschäftigten eine komplette Überprüfung aller dienstlichen Telefongespräche vorzunehmen. Dies muß unbedingt durch zusätzliche technische und organisatorische Maßnahmen ausgeschlossen werden, um den Forderungen in § 2 Abs. 2 Musterdienstvereinbarung zu entsprechen.

1.6.3.5 Verhinderung von Anwesenheit-, Verhaltens- und Leistungskontrollen

Nach § 2 Abs. 1 Musterdienstvereinbarung ist eine Durchführung von Anwesenheit-, Verhaltens- und Leistungskontrollen nicht zulässig und sowohl technisch als auch organisatorisch auszuschließen.

Diese Vorschrift wird nicht ausreichend nachdrücklich umgesetzt. Die Staatskanzlei als Betreiberin verpflichtet sich lediglich dazu, keine Anwesenheit-, Verhaltens- und Leistungskontrollen vorzunehmen; der Datenbestand und das organisatorische Umfeld lassen aber immer noch zu, daß derartige Kontrollen - mit geringem Aufwand und für den Nutzer sogar unbemerkt - nachträglich eingeführt werden können (fehlende Rücknahmefestigkeit). Es fehlt an einer technisch-organisatorischen Untermauerung der Verpflichtung.

Hier erwarte ich in Umsetzung des § 2 Abs. 1 Musterdienstvereinbarung, daß geeignete technisch-organisatorische Maßnahmen getroffen werden, die mit relativ hoher Sicherheit gerade derartige Kontrollen ausschließen. Dazu müssen die Systemkomponenten so umgestaltet werden, daß die Datenschutzfunktionen stabil sind und nicht einseitig durch den Systembetreiber oder Dritte zurückgenommen oder unterlaufen werden können. Insoweit habe ich in meinem Prüfbericht zusätzliche Sicherheitsmaßnahmen zur Verhinderung von Anwesenheit-, Verhaltens- und Leistungskontrollen u. a. in folgenden Bereichen gefordert:

- Bei der Vergabe von Leistungsmerkmalen durch den Systemadministrator sind unberechtigte bzw. versehentliche Veränderungen weitestgehend auszuschließen; das kann beispielsweise durch eine generelle Sperrung der nicht zulässigen besonders kritischen Leistungsmerkmale erfolgen.

- Der Umfang der Überprüfung dienstlicher Gespräche sollte durch Festlegung einer nicht überwindbaren Obergrenze in der Software beschränkt werden.

- Der Ausdruck von Auswertungslisten, der mit der derzeitig zur Gebührendatenverarbeitung verwendeten Software möglich, laut Dienstanschlußvorschrift aber unzulässig ist, muß durch die Technikgestaltung ausgeschlossen werden.

- Insgesamt sollte durch eine andere Organisation der Datenspeicherung, die nicht mehr davon ausgeht, daß für jedes Einzelgespräch ein Gebührendatensatz angelegt wird, das Potential für mögliche Verhaltens- und Leistungskontrollen abgebaut werden.

1.6.3.6 Paßwörter für die Datensicherheit

Die Mitarbeiter in der Zentrale des TK-Verbundes greifen mit Hilfe der Telefondatenverwaltung auf die TK-Anlagen der übrigen 10 Standorte zu, um u. a. die Leistungsmerkmale abzufragen oder zu aktualisieren. Dazu sind die meisten Standorte über ein Modem von der Zentrale aus erreichbar. Um das Eindringen Unbefugter zu verhindern, muß sich der Benutzer durch sein persönliches, geheimgehaltenes Paßwort zu erkennen geben, wobei die Zuverlässigkeit der Authentizität mit der Geheimhaltung des Paßwortes steht und fällt. Da im TK-Verbund u. a. auch mit von den Herstellerfirmen fest vorgegebenen und nicht veränderbaren Paßwörtern gearbeitet wird, bieten diese Benutzerpaßwörter praktisch keine Sicherheit und stellen eine Art "Alibifunktion" dar. Wie zusätzlich festgestellt, können nach fehlerhaften Programmabläufen sogar fremde Nutzer ohne Kenntnis des Paßwortes auf die Anlage zugreifen.

1.6.3.7 Geheimgehaltene Dateibeschreibungen

In Vorbereitung meiner Prüfung bat ich gem. § 26 Abs. 1 BbgDSG die Staatskanzlei um Zusendung der Dateibeschreibung und des Verzeichnisses der Geräte, wie dies in § 8 BbgDSG vorgeschrieben ist. Mit dem Hinweis: "Unter Berücksichtigung der Geheimhaltungsbestimmungen bitten wir um Verständnis, daß spezifische Dokumente vor Ort zur Einsichtnahme vorliegen.", wurde mir die vorherige Zustellung dieser Unterlagen verweigert. Abgesehen davon, daß sie vor der Novellierung des Brandenburgischen Datenschutzgesetzes gem. § 24 Abs. 1 BbgDSG dem Landesbeauftragten für den Datenschutz zur Führung des Dateienregisters zur Verfügung gestellt hätten werden müssen, kann ich keine datenschutzrechtlichen Gründe für die Geheimhaltung dieser Unterlagen erkennen, da sie lediglich die Beschreibung der einzelnen Datenfelder enthalten.

Während der Kontrolle stellte sich schließlich heraus, daß auch vor Ort keine Dateibeschreibung vorlag. Die Prüftätigkeit meiner Behörde hat sich dadurch wesentlich erschwert. Als meine Mitarbeiter versuchten, die Dateien anhand von Bildschirmanzeigen zu beschreiben, stellten sie fest, daß auch bei der verantwortlichen Betreiberin des TK-Verbundes kein eindeutiger Überblick über die genaue Belegung einiger Datenfelder bestand. Unter diesen Umständen dürfte es für die Staatskanzlei schwerlich möglich sein, den Verpflichtungen nachzukommen, die in § 10 Abs. 1 BbgDSG den öffentlichen Stellen des Landes Brandenburg hinsichtlich der Ausführung der Vorschriften dieses Gesetzes auferlegt werden.

1.6.3.8 Erste Stellungnahme der Staatskanzlei

Alle Verstöße gegen die Dienstanschlußvorschrift und Musterdienstvereinbarung habe ich gem. § 25 Abs. 1 Nr. 1 BbgDSG förmlich beanstandet. In einer ersten Stellungnahme hierzu zieht sich die Staatskanzlei als verantwortliche Betreiberin des TK-Verbundes auf den Standpunkt zurück, daß sie entsprechend der DAV und der Dienstvereinbarung arbeite und daß sich die von mir beanstandeten Positionen nicht verändern ließen, da dies die vom Hersteller gelieferte Softwarevariante nicht zulasse. Dies ist für mich nicht nachvollziehbar, da die Software ja gerade aufgrund einer im Jahre 1993 in Auftrag gegebenen Anpassung mit dem Inhalt der Dienstanschlußvorschrift und der Dienstvereinbarung in Übereinstimmung gebracht werden sollte. Erfreulicherweise schließt die Staatskanzlei eine weitere Softwareanpassung aber nicht aus.

Die Staatskanzlei hat mich allerdings auch wissen lassen, daß sie - zusammen mit den Personalräten der Ressorts - prüfen will, ob die Musterdienstvereinbarung einschließlich der Anlagen noch den aktuellen Erfordernissen entspricht oder ggf. präzisiert werden sollte. Ich hoffe, daß damit keine Anpassung der Musterdienstvereinbarung an die zur Zeit verwendete Software zur Gebührendatenverarbeitung beabsichtigt ist.

2 Allgemeiner Datenschutz

2.1 Änderungen der Vorläufigen Verwaltungsvorschrift zur Durchführung des Brandenburgischen Datenschutzgesetzes

Im Zuge der Novellierung des Brandenburgischen Datenschutzgesetzes[17] hat das Ministerium des Innern (MI) im Berichtszeitraum einen Entwurf zur Änderung der Vorläufigen Verwaltungsvorschrift zur Durchführung des

[17] s. 4. Tätigkeitsbericht unter 2.1

Brandenburgischen Datenschutzgesetzes (Vorl. VV zum BbgDSG)[18] vorgelegt.

Die Neufassung und Ergänzung der Vorläufigen Verwaltungsvorschrift soll den brandenburgischen Behörden vor allem den Umgang mit den Vorschriften über die Datenverarbeitung im Auftrag gem. § 11 BbgDSG und mit der neu in das Datenschutzgesetz aufgenommenen Regelung der Wartung und Fernwartung von Datenverarbeitungsanlagen gem. § 11 a BbgDSG erleichtern. Die Umsetzung dieser Vorschriften des Datenschutzgesetzes und insbesondere die Einhaltung der technisch-organisatorischen Sicherheitsmaßnahmen bei der Fernwartung (s. unter 1.3.5) hatten in der Vergangenheit den öffentlichen Stellen erhebliche Probleme bereitet. In diesem Zusammenhang habe ich dem MI konkrete Vorschläge zur Gestaltung und Formulierung der Ausführungsbestimmungen zu beiden Vorschriften unterbreitet, die erfreulicherweise ohne inhaltliche Änderungen in den Entwurf übernommen worden sind.

[18] vom 24. Januar 1995, ABl. S. 134; s. 3. Tätigkeitsbericht unter 2.2

Nachdem die Aufnahme einer Regelung über den behördlichen Datenschutzbeauftragten in das Brandenburgische Datenschutzgesetz aus "Kostengründen" gescheitert ist[19] und die Entscheidung über die Bestellung eines behördlichen Datenschutzbeauftragten nach dem Willen des Gesetzgebers weiterhin den öffentlichen Stellen überlassen bleiben soll, halte ich es für angebracht, die bereits bestehenden Ausführungsbestimmungen in der Vorläufigen Verwaltungsvorschrift zu ergänzen und den Aufgabenbereich des Datenschutzverantwortlichen zu konkretisieren, um dessen Stellung innerhalb der Behörden zu stärken. So liegt es vor allen Dingen auch im Interesse der jeweiligen öffentlichen Stelle, wenn der Datenschutzverantwortliche die Behörde nicht nur in ihren datenschutzrechtlichen Bemühungen unterstützt und berät, sondern auch die Einhaltung der Mindestanforderungen des Datenschutzgesetzes durch die Behörde und ihre Mitarbeiter weitgehend selbständig kontrolliert. Es ist meines Erachtens weiterhin erforderlich festzuschreiben, daß der Datenschutzverantwortliche über die ausreichende Sach- und Fachkunde verfügt bzw. sich diese umgehend aneignet, seine Bestellung schriftlich erfolgt und die Behörde die ihm obliegenden Aufgaben genau bezeichnet. Es sollte überdies durch entsprechende organisatorische Maßnahmen sichergestellt werden, daß der Datenschutzverantwortliche seine Vorschläge und Bedenken unmittelbar der Leitung der öffentlichen Stelle vortragen kann. Darüber hinaus habe ich mich für die Aufnahme eines Benachteiligungsverbotes und einer speziellen Regelung der Weisungsfreiheit ausgesprochen, da nur auf diese Weise die Unabhängigkeit des Datenschutzverantwortlichen als Grundlage für eine objektive und von sachlichen Argumenten geleitete Aufgabenerfüllung im Interesse des Datenschutzes gewährleistet werden kann. Auch dazu habe ich dem MI entsprechende Vorschläge unterbreitet.

Daneben hat die Neufassung des Datenschutzgesetzes eine redaktionelle Anpassung der Vorläufigen Verwaltungsvorschrift sowie der zugehörigen Anlagen erforderlich gemacht. Zudem müssen sämtliche Passagen, die im Zusammenhang mit der Regelung zum Dateienregister nach § 24 BbgDSG alter Fassung standen, gestrichen werden.

2.2 Dateibeschreibung gem. § 8 Abs. 3 BbgDSG

Aufgrund der Novellierung des Brandenburgischen Datenschutzgesetzes[20] sind die datenverarbeitenden Stellen nicht mehr verpflichtet, mir eine Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, vorzulegen. Nach § 8 BbgDSG besteht jedoch weiterhin für jede datenverarbeitende Stelle die Pflicht, die Dateibeschreibung aktuell vor Ort zu führen. Dazu wurde von der Landesregierung die Verordnung zur Dateibeschreibung (DBeschrV)[21] erlassen, in der als Anlage die verbindlichen Musterformulare beigefügt sind. Es ist vorgesehen, Hinweise zum Ausfüllen dieser Musterformulare in die derzeitig in Überarbeitung stehenden Vorläufigen Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz aufzunehmen (s. unter 2.1).

Bei der Nutzung von Fremd-Software sollten die Vertragsbedingungen so gestaltet werden, daß die Dokumentationsunterlagen alle zur Dateienbeschreibung erforderlichen Informationen enthalten.

2.3 Akteneinsicht und -auskunft

---

19 s. 4. Tätigkeitsbericht unter 2.1

20 i. d. Fass. vom 23. Mai 1996, GVBl. I S. 185

21 vom 7. Oktober 1996, GVBl. II S. 695

2.3.1 Stand des Gesetzgebungsverfahrens für ein "allgemeines Akteneinsichtsrecht"

Die Verfassungen der neuen Bundesländer weisen neben den unverzichtbaren Regelungen insbesondere zur Ausgestaltung des Staatsrechts auch solche aus, die das mehr in die Zukunft gerichtete Lebensgefühl der Bürger verdeutlichen, eine Ausrichtung, die zugleich einen Ausdruck der Erfahrungen aus den zurückliegenden Jahren beinhaltet. Die Verfassung des Landes Brandenburg[22] enthält innerhalb des Abschnitts mit der Überschrift "Politische Gestaltungsrechte" in Artikel 21 Abs. 4 eine Regelung, wonach "jeder nach Maßgabe des Gesetzes das Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungsreinrichtungen des Landes und der Kommunen" hat, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen.

Nachdem mehrere Beschlüsse des Landtages gefaßt worden sind, einen Gesetzentwurf vorzulegen, hat die Landesregierung inzwischen einen Referentenentwurf erarbeitet, der sich jedoch noch im interministeriellen Abstimmungsverfahren befindet. Sowohl zu dem zunächst vom MI vorgelegten sog. "Eckpunkten" für ein solches Gesetz als auch dem o. g. Referentenentwurf habe ich Stellung genommen. Über den Fortgang der Angelegenheit werde ich weiterhin berichten.

2.3.2 Akteneinsichtsrecht der Abgeordneten

Im Berichtszeitraum hatte ein Abgeordneter die kompletten Unterlagen einsehen wollen, die im Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF) zu Beratungs- und Geschäftsbesorgungsverträgen im Zusammenhang mit der Errichtung von Altenpflegeheimen aufbewahrt wurden. Der Abgeordnete wollte sich nicht damit zufrieden geben, daß ihm das MASGF nur solche Unterlagen in Kopie zur Einsichtnahme überlassen hatte, die beteiligte Firmen betrafen und bei denen die Namen geschwärzt worden waren. Ihn interessierte u. a. auch der Schriftverkehr, der zur Vorbereitung der Verträge geführt worden war.

Das Ministerium verweigerte ihm dies und berief sich dabei auf den Datenschutz, der den Vertragspartnern zugute kommen müsse. Aus meiner Sicht hat in einem derartigen Fall das uneingeschränkte Informationsrecht eines Mitglieds des Landesparlaments aber Vorrang vor dem Datenschutz.

Da das Ministerium sich nicht zu einer wesentlichen Meinungsänderung durchringen konnte, wandte sich der Abgeordnete schließlich in dieser Frage mit einer Organklage an das Verfassungsgericht des Landes Brandenburg. Das Verfassungsgericht[23] entschied, daß das Verhalten der Landesregierung in dem zu entscheidenden Fall gegen Art. 56 Abs. 3 Satz 2 und 4, Abs. 4 Verfassung des Landes Brandenburg verstoße; der Abgeordnete habe ein Recht darauf, die dem Gericht genannten Unterlagen "vollständig und unter Offenlegung der Namen der an den Vorgängen Beteiligten" vorgelegt zu bekommen.

Das Verfassungsgericht bestätigte, daß der Landtag eine direkt von der Verfassung her abgeleitete Kompetenz zur Kontrolle bereits abgeschlossener Vorgänge der Exekutive hat. Der Datenschutz steht - bei einer Zusammenschau der Verfassungsbestimmungen zu dem in der Landesverfassung ausdrücklich genannten Persönlichkeitsrecht einerseits und den Rechten andererseits, die sich aus der Kontrollkompetenz des Landtages ergeben - dem Anspruch des Abgeordneten auf vollständige Information nicht von vornherein entgegen. Allerdings sind in der Verfassung Fälle genannt, in denen die

---

22 vom 20. August 1992, GVBl. I S. 298, geänd. d. Art. 2 d. NVG vom 27. Juni 1995, GVBl. I S. 150

23 VerfGBbg 3/96 vom 20. Juni 1996

Erteilung von Auskünften und die Einsichtnahme in Akten abgelehnt werden dürfen, nämlich dann, wenn überwiegende öffentliche oder private Interessen an der Geheimhaltung die Ablehnung zwingend erfordern.

Bei der Abwägung zwischen dem Informationsinteresse des Abgeordneten aus Art. 56 Abs. 4 Satz 1 und dem gleichfalls in der Verfassung (Art. 11) verbürgten "Grundrecht auf Datenschutz" zeigt es sich, daß das private Interesse der beteiligten Firmen nicht als "überwiegend" betrachtet werden kann. Der Anspruch des Abgeordneten auf Akteneinsicht im Zuge seiner Kontrollkompetenz hat in dem zu entscheidenden Fall ein besonderes Gewicht. Die Offenlegung der Namen ist zumutbar, weil es bei den beteiligten Dritten nicht um Informationen aus deren sozialem Bereich - etwa aus der unantastbaren Sphäre privater Lebensgestaltung - geht; die Betroffenen hatten vielmehr "mit einem im Lichte der Öffentlichkeit stehenden Ministerium" vertragliche Beziehungen.

3 Inneres

3.1 Melde- und Personenstandswesen

3.1.1 Novellierung melderechtlicher Vorschriften

3.1.1.1 Brandenburgisches Meldegesetzes

Schon in früheren Tätigkeitsberichten hatte ich auf mehrere Punkte hingewiesen, die einer unbedingten Regelung bzw. Neuregelung im Brandenburgischen Meldegesetz (BbgMeldeG)[24] bedürfen, so z. B.

- Behandlung der Kreismeldekarteien[25],

- Meldedaten (auch auf CD-ROM) an Adreßbuchverlage[26].

Darüber hinaus hat sich innerhalb von gut fünf Jahren nach Inkrafttreten des Gesetzes neben einer Reihe von Angleichungsmängeln an das Melderechtsrahmengesetz (MRRG)[27] noch weiterer Regelungs- bzw. Änderungsbedarf herausgestellt, so z. B. hinsichtlich der

- bestehenden Übermittlungsregelung, daß an öffentlich-rechtliche Religionsgesellschaften auch Daten jener Familienangehörigen ihrer Mitglieder übermittelt werden dürfen, die nicht derselben oder keiner Religionsgesellschaft angehören (s. unter 6.3),

- derzeitigen Regelungen zur automatisierten Datenverarbeitung im Meldebereich.

Bei meiner kürzlichen Prüfung von Meldebehörden (s. unter 12.4.1) bin ich noch auf zusätzliche, bisher nicht diskutierte oder für mich bislang nicht erkennbare Regelungslücken im Meldegesetz gestoßen.

---

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

25 s. 3. Tätigkeitsbericht unter 3.2.1.2

26 s. 4. Tätigkeitsbericht unter 3.1.1.6

27 vom 16. August 1980, BGBl. I S. 1429 i. d. Fass. vom 24. Juni 1994, BGBl. I S. 1430

Ein Entwurf der Landesregierung lag mir zum Redaktionsschluß noch nicht vor. Nach Information des Ministeriums des Innern (MI) ist ins Auge gefaßt, die Novellierungsvorlage noch zum Ende 1997 in den Landtag einbringen zu können. Nach kürzlich hierüber mit dem MI geführten Gesprächen hoffe ich, auch noch meine weiteren Anregungen und konkreten Regelungsvorschläge einbringen zu können. Erst danach wird es sinnvoll sein, hierüber Näheres zu berichten.

3.1.1.2 Datenübermittlungsverordnung

Die Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (MeldDÜV)[28] war in meinem vorigen Tätigkeitsbericht Gegenstand recht eingehender Ausführungen[29]. Die beabsichtigte Neufassung steht noch immer aus. Die Stellungnahme der Landesregierung zum Vorjahresbericht sowie Schriftwechsel und weitere Gespräche mit dem MI über die bisher kontrovers beurteilten Punkte brachten folgendes Ergebnis:

1. Die Landesregierung folgt meiner Auffassung, daß "Datenübermittlungen" nach Maßgabe der Verordnung auch das "Bereithalten zum Abruf" (Vorhalten zum Abruf) umfassen.

2. Zwar betont das MI zu Recht, daß im Verordnungstext nicht auf die nachrangigen Datenübermittlungsgrundsätze Brandenburgs[30] verwiesen werden könne. Gerade deshalb - und weil diese datenschutzgerechten Grundsätze weiterhin uneingeschränkt gelten sollen - muß ich entgegen der Auffassung der Landesregierung darauf bestehen, daß sie unmittelbarer Bestandteil der Rechtsverordnung werden.

3. Einer geforderten regelmäßigen Übermittlung von Meldedaten (Um- und Abmeldungen) an den ORB bzw. an die Gebühreneinzugszentrale (GEZ) zum Zweck des Rundfunkgebühreneinzugs bahnt sich nach mehreren Gesprächen mit Vertretern des ORB, der Staatskanzlei, dem MI und meiner Behörde ein gewisser Kompromiß an. Entscheidend dafür war, daß die Staatskanzlei ihre ablehnende Haltung zu diesem Verfahren - mit dem Schwarzhörer bzw. -seher aufgespürt werden sollen - im wesentlichen angesichts knapper öffentlicher Kassen aufgegeben hatte, obwohl damit eine Durchbrechung des Verwendungszwecks von Meldedaten verbunden ist.

Meinen datenschutzrechtlichen Bedenken soll dabei wenigstens insofern Rechnung getragen werden, daß hierbei zum einen auf die Mitteilung von Rufnamen verzichtet und zum anderen jeweils nur die letzte Adresse mitgeteilt wird. Des weiteren sollen diese sog. Bewegungsdaten aus den Melderegistern nicht sofort am jeweiligen Monatsende, sondern zeitverzögert erst nach zwei Monaten der GEZ übermittelt werden (Moratorium). Damit erhalten die meldepflichtigen Personen eine Chance, sich von sich aus anzumelden, bevor sie aufgrund des Datenabgleichs als potentielle Schwarzhörer und -seher eingestuft werden. Es erscheint mir darüber hinaus erfolgversprechend, die Bereitschaft zur rechtzeitigen Anmeldung bei der GEZ dadurch zu stärken, daß GEZ-Meldeformulare nicht nur in Banken, sondern auch bei den Meldestellen ausgelegt werden.

---

28 vom 26. Oktober 1992, GVBl. II S. 688

29 s. 4. Tätigkeitsbericht unter 3.1.1

30 Runderlaß des MI vom 17. September 1991 - II/7-2.100, ABl. S. 728

4. Hinsichtlich der Datenübermittlungen an Bürgermeister amtsangehöriger Gemeinden[31] will die Landesregierung meine Rechtsauffassung, daß der Regelungsgehalt von § 59 Abs. 3 und 4 Gemeindeordnung (GO)[32] unzureichend ist, nicht folgen. Soweit politische Gründe dafür sprechen sollten, hier keinen der Normenklarheit entsprechenden Aufgabenkatalog festzulegen, sollte sich die Landesregierung hierzu eindeutig erklären.

Bei kürzlich durchgeführten Kontrollbesuchen in 14 Meldestellen aus allen Landkreisen unseres Landes (s. unter 12.4.1) konnten meine Mitarbeiter feststellen, daß nur in drei Fällen (Meldestellen amtsangehöriger Gemeinden) - offensichtlich in Erwartung der neuen MeldDÜV oder aufgrund des kommunalpolitischen Drucks vor Ort - bereits jetzt den ehrenamtlichen Bürgermeistern zumindest die Daten von Alters- oder Ehejubilaren übermittelt werden. Die Verantwortlichen dieser Ämter gaben auf ausdrückliches Befragen hinsichtlich der beabsichtigten Regelung zu, daß die Erforderlichkeit für eine darüber hinausgehende Übermittlung - trotz immer wieder geäußerten Wunsches der ehrenamtlichen Bürgermeister - nicht erkennbar sei. In einigen Fällen wurde sogar die Befürchtung geäußert, daß die datenschutzrechtlich korrekte Weiterbehandlung insoweit übermittelter Daten sowohl mangels eindeutiger Zweckbindung als auch aufgrund kaum zu realisierender technisch-organisatorischer Datensicherungsmaßnahmen nicht garantiert werden könne.

5. Über die von mir geforderte Verschlüsselung aller regelmäßig zu übermittelnden, elektronisch gespeicherten Daten konnte bislang noch keine Übereinstimmung erzielt werden. Das MI hat darauf hingewiesen, daß einerseits allein aus Kostengründen nicht überall sofort die notwendigen Voraussetzungen hierfür (Anschaffung von Software) getroffen werden könnten, es andererseits für die Adressaten regelmäßig verschiedener Meldebehörden nur langfristig möglich wäre, sich auf die u. U. verschiedenen Verschlüsselungsmethoden einzustellen; daher wurde ich darum gebeten, diese Forderung bis zur nächsten Novellierung zurückzustellen. Dies ist aber aus Rechtsgründen nicht möglich.

Meine Forderung beruht auf § 29 Abs. 3 Satz 2 BbgMeldeG, wonach ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, nur eingerichtet werden darf, "soweit dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen ... angemessen ist". Dieses vom MI im Grundsatz ebenfalls nicht in Frage gestellte Erfordernis soll dem Recht auf informationelle Selbstbestimmung Betroffener Rechnung tragen.

Da auf dieses Recht jederzeit ein Anspruch besteht, kann selbst eine zeitlich gestaffelte Einführung der Verschlüsselung je nach Umsetzbarkeit zwischen den Meldebehörden und den einzelnen Adressaten nicht in Betracht kommen. Die Konsequenz kann nur sein, daß in der Rechtsverordnung auf automatisierte regelmäßige Datenübermittlungen in den Fällen verzichtet wird, in denen eine Verschlüsselung der Daten vom Tage ihres Inkrafttretens an nicht gewährleistet werden kann. Dies muß nicht zwangsweise dazu führen, daß auf Teile der Verordnung verzichtet werden muß; es ist auch denkbar, daß zusätzlich zum grundsätzlichen Gebot der Verschlüsselung eine ausdrückliche Regelung gefunden wird, die, solange eine Verschlüsselung noch nicht realisiert ist, die Datenübermittlung auf andere Art und Weise, die dem Schutzbedarf auch ausreichend Rechnung trägt, zuläßt (z. B. Listen- und Diskettentransport per Kurier statt Netzübertragung).

Ein genereller Verzicht auf eine Verschlüsselungsregelung unter Hinweis auf die allgemeinen

---

31 vgl. 4. Tätigkeitsbericht unter 3.1.1.2

32 vom 15. Oktober 1993, GVBl. I S. 398, geänd. d. Art. 3 d 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

Datensicherungsmaßnahmen nach § 10 BbgDSG (sog. zehn Gebote) kann nicht hingenommen werden. Formale Gründe sprechen dagegen, weil aufgrund der Verordnungsermächtigung des spezialgesetzlichen § 29 Abs. 2 BbgMeldeG in der Rechtsverordnung nicht nur Anlaß und Zweck der Übermittlung, die Datenempfänger sowie die zu übermittelnden Daten, sondern auch ihre Form sowie das Nähere über das Verfahren der Übermittlung festzulegen sind. Materielle Gründe sprechen insbesondere dagegen, weil zu befürchten wäre, daß es bei Zweifeln an der Ordnungsgemäßheit einzelner Übermittlungsvorgänge ständig zu Kontroversen darüber käme, ob die allgemeinen geforderten Schutzmaßnahmen dem Umfang und dem Schutzzweck angemessen sind.

Zu der Tatsache, daß gerade im Meldebereich auch für alle anderen Verfahren der automatisierten Datenübermittlung in weiten Netzen die Notwendigkeit der Verschlüsselung wegen des nach dem derzeitigen Stand der Technik generellen Gefährdungsgrades gegeben ist und deshalb zusätzliche Festlegungen im Brandenburgischen Meldegesetz selbst erforderlich sind, führe ich unter 12.4.1 Näheres aus. In weiteren Gesprächen hoffe ich, die Landesregierung im Sinne meiner Ausführungen überzeugen zu können.

3.1.2 Änderung des Personenstandsgesetzes

Nachdem ich im Juni 1996 vom Bundesbeauftragten für den Datenschutz darauf aufmerksam gemacht worden war, daß das Bundesministerium des Innern den Vorentwurf eines Fünften Gesetzes zur Änderung des Personenstandsgesetzes (5. PStÄndG, Stand: 25. März 1996) den Innenressorts der Länder zugeleitet hat, erhielt ich erst auf Anfrage diesen Entwurf vom MI zugesandt.

In meiner Stellungnahme hierzu konnte ich darauf hinweisen, daß der Entwurf weitgehend die seit Jahren vorgetragenen Forderungen der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt, die in die Personenstandsbücher einzutragenden Eingaben auf die Daten zu beschränken, die für den Beurkundungszweck selbst von Bedeutung sind. Dies begrüße ich ebenso wie im Detail die vorgesehene, an das Bundesarchivgesetz angelegte Regelung, nach der es für die Benutzung der Personenstandsbücher ausreicht, ein berechtigtes Interesse darzulegen, wenn seit dem Tod der Betroffenen mindestens 30 Jahre oder, falls deren Todestag nicht bekannt ist, seit der Geburt mindestens 120 Jahre vergangen sind. Hierdurch wird in Zukunft insbesondere die Ahnenforschung in angemessener Weise erleichtert werden. Damit dürfte eine datenschutzgerechte Regelung gefunden sein, die die immer wieder vorgebrachten unsachlichen Vorwürfe beenden dürfte, "der Datenschutz" und somit die Datenschutzbeauftragten seien Verhinderer der Ahnenforschung.

Auch begrüße ich die datenschutzgerecht konditionierte Öffnungsklausel zur Durchführung wissenschaftlicher Forschungsarbeiten. Hierzu hatte ich schon in meinem vierten Tätigkeitsbericht[33] ausgeführt. Allerdings sollte dem Transparenzgebot folgend ebenso konkret definiert werden, bei welchen wissenschaftlichen Forschungsarbeiten die Ausnahmeregelung gelten soll, wie welche Kriterien den besonderen Anlaß zur Prüfung der Zulässigkeit der Übermittlung durch den Standesbeamten bestimmen sollen. Diese Anregung hat das MI aufgenommen und in seiner Stellungnahme für das Land Brandenburg berücksichtigt. Dies trifft auch für meine Anregung zu, die in den zuletzt genannten Zusammenhängen benutzten Begriffe "personenbezogene Informationen" und "Informationen" durch den einschlägigen, klar definierten Begriff "personenbezogene Daten" zu ersetzen, weil jene Begriffe durch ihre Unterschiedlichkeit nicht dem Erfordernis der Normenklarheit genügen. Darüber hinaus fordere ich im Zusammenhang mit den Regelungen zu

[33] s. unter 6.1.2

wissenschaftlichen Forschungsarbeiten aber auch, daß in Anlehnung an § 28 Abs. 1 Satz 5 BbgDSG mit der jeweiligen Zustimmung durch die "zuständige Verwaltungsbehörde" sowohl der Empfänger als auch die Art der zu übermittelnden (bzw. anders zu verwendenden oder weiter zu übermittelnden) personenbezogenen Daten, der Kreis der Betroffenen und der konkrete Forschungszweck zu bezeichnen sind und diese Zustimmung dem Landesbeauftragten für den Datenschutz mitzuteilen ist.

Dem begrüßenswerten Regelungsvorhaben, in der Sterbeurkunde den Ort, an dem die Person tot aufgefunden wurden, als Sterbeort auszuweisen, auch wenn der tatsächliche Sterbeort nicht bekannt ist, fehlt in dem Vorentwurf leider eine Entsprechung hinsichtlich des Fehlens eines genauen Todeszeitpunkts. Auch hier sollte zur Vermeidung diskriminierender Spekulationen über die näheren Todesumstände eine fiktive Regelung etwa dahingehend gefunden werden, daß als Zeitpunkt des Todes der Sterbetag eingetragen wird, ohne daß erkennbar wird, ob innerhalb dieses Tages der genaue oder nur der ungefähre Zeitpunkt oder gar nur ein Zeitraum des Todeseintritts feststellbar war. Für im Sterbebuch angegebene längere Zeiträume sollte der für den ungefähren Zeitpunkt im Rahmen dieses Zeitraums angenommene Tag als Todestag in die Sterbeurkunde eingesetzt werden. Meinem diesbezüglichen Vorschlag, der im übrigen auch von Kollegen in anderen Bundesländern gleichermaßen vorgetragen wird, wollte das hiesige MI jedoch unter Hinweis darauf nicht folgen, daß die genaue Angabe des Todeszeitpunkts u. U. erbrechtliche Auswirkungen habe und deshalb nicht grundsätzlich auf die Zeitangabe verzichtet werden könne. Gleichwohl halte ich daran fest, daß eine gesetzliche Festlegung zu treffen ist, die es den überlebenden Angehörigen ermöglicht, von der Sterbeurkunde eines Angehörigen Gebrauch machen zu können, ohne gezwungen zu sein, in diesem Zusammenhang zusätzliche diskriminierende Sachverhalte mit offenbaren zu müssen. Es sollte erreicht werden, daß unter Aufrechterhaltung der Beweiskraft der jeweiligen Urkunden Daten nur in der Detaillierung übermittelt werden, wie sie zur Erledigung der jeweiligen konkreten privaten Angelegenheit erforderlich sind.

Zum technisch-organisatorischen Teil der beabsichtigten Neuregelungen konnte ich begrüßen, daß Behörden und sonstigen öffentliche Stellen, denen Angaben über Beurkundungen in ein Personenstandsbuch übermittelt werden dürfen, der unmittelbare Zugriff auf die Daten (Online-Zugriff) nicht gewährt wird. Es soll der vorgesehene Einsatz elektronischer Datenverarbeitung auf Hilfsfunktionen zum Ausdruck von Personenstandsurkunden und zur Führung von Zweitbüchern begrenzt bleiben.

Gleichwohl bedarf es auch für diesen "eingeschränkten ADV-Einsatz" eindeutiger materiell-rechtlicher Regelungen über technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes im Gesetz selbst.
Insbesondere im Hinblick auf die vorgesehene Regelung, nach der das Zweitbuch auch auf elektronischen Datenträgern geführt werden darf, ist es unabdingbar, die erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes (und zur dauerhaften Bestandswahrung der Personenstandsbücher) entweder im Personenstandsgesetz ausdrücklich selbst zu regeln oder zumindest zwingend auf die Anwendbarkeit der § 9 BDSG entsprechenden Bestimmungen in den Landesdatenschutzgesetzen (in Brandenburg: § 10 BbgDSG) zu verweisen. Regelungsansätze im Vorentwurf, wonach das Zweitbuch in einem anderen Gebäude als die Erstbücher aufzubewahren sind, können hier nicht ausreichen.

In technischer Hinsicht problematisch sind auf jeden Fall die vorgesehenen Aufbewahrungsfristen für Zweitbücher, wenn diese elektronisch gespeichert sind (30 bzw. 100 bzw. 120 Jahre). Magnetische Datenträger sollten erfahrungsgemäß nach 3 Jahren umkopiert werden, um die Daten selbst zu sichern. Selbst für eingebrannte CD-ROM oder WORM-Platten sind sehr lange Aufbewahrungsfristen aufgrund von Langzeiterfahrungen bisher tatsächlich nicht garantierbar, auch wenn deren Hersteller Garantien für 30 oder 50 Jahre übernehmen sollten[34].

[34] s. 4. Tätigkeitsbericht unter 1.5.5

Zu meinen technisch-organisatorischen Anmerkungen hat sich das MI nicht näher geäußert. Zum aktuellen Stand der Angelegenheit liegen zum Ende des Berichtszeitraums keine weiteren Informationen vor.

3.2 Grundstückswesen

3.2.1 Änderung des Vermessungs- und Liegenschaftsgesetzes/Verordnung zur Übermittlung von Liegenschaftskatasterdaten

Für den Berichtszeitraum hatte sich die Landesregierung ein umfangreiches Änderungsvorhaben für das Vermessungs- und Liegenschaftsgesetz (VermLiegG) für das Land Brandenburg vorgenommen, ergänzt durch eine "Verordnung über die Einrichtung automatisierter Abrufverfahren und regelmäßiger Datenübermittlungen im Liegenschaftskataster" (LiKaDÜV). Ein erster Entwurf lag im Frühjahr 1996 vor.

Eines der wichtigsten Anliegen der Landesregierung für die Änderung dieses Gesetzes war - neben der Anpassung an veränderte Gegebenheiten innerhalb und außerhalb der Verwaltung - die Berücksichtigung des Bedürfnisses, Daten aus dem Liegenschaftskataster regelmäßig und automatisiert abzugeben. Hierzu war nach § 9 BbgDSG eine gesetzliche Ermächtigung erforderlich. Für die Anpassung der Rechtslage und die den modernen Anforderungen entsprechende Ausstattung der öffentlichen Stellen, vor allem der Gemeinden, ist im Entwurf eine Verordnungsermächtigung enthalten; hiervon hat die Landesregierung zeitgleich mit der Novellierung Gebrauch gemacht.

Auch weitere Änderungsvorschläge, die bei dieser Novellierung berücksichtigt worden sind, betreffen zumeist den Datenschutz. So ist in einem neu eingefügten § 1 a der "Schutz personenbezogener Daten" in dem Vermessungs- und Liegenschaftsgesetz nun ausdrücklich geregelt. Ergänzend ist festgelegt worden, daß das Brandenburgische Datenschutzgesetz gilt. Allerdings wurde eine ausdrückliche Löschungsvorschrift mit § 12 Abs. 5 eingeführt.

Die Landesregierung hatte zunächst geplant, die Geburtsdaten aller in dem Kataster geführten Personen auszuweisen. Hiervon hat sie inzwischen Abstand genommen; neu eingefügt wurde aber mit § 9 VermLiegG die Möglichkeit, Namen und Anschriften von Verfügungsberechtigten und Bevollmächtigten der Eigentümer u. a. nachzuweisen. Dies entspricht den Anforderungen, die sich aus dem Wohnungseigentumsgesetz[35] ergeben. Mit dieser Erweiterung der Möglichkeit, Daten zu verarbeiten, wurde vor allem den Anforderungen entsprochen, die sich aus dem Wohnungseigentumsgesetz ergeben. Außerdem wurde festgelegt, daß das Grundbuchamt und das Finanzamt Auszüge aus dem Liegenschaftskataster erhalten können, soweit dies für die Erfüllung ihrer Aufgaben erforderlich ist.

Neu ist, daß künftig die Gemeinden (und Ämter) Einsicht in das Liegenschaftsbuch gewähren und Auszüge daraus erteilen können. Diese Möglichkeit wird allerdings nur an jeweils einer Stelle der Gemeinde (oder des Amtes) gegeben sein, damit der Datenschutz wirkungsvoller eingehalten werden kann.

Schließlich ist vor allem auf einige Klarstellungen hinzuweisen: Die Benutzung des Liegenschaftskatasters erfolgt nun ausdrücklich nur auf Antrag; dies wurde zwar bereits bisher so gehandhabt, die Festlegung im Gesetz trägt jedoch der Situation Rechnung, daß der Zugang zu Katasterdaten bei automatisierter Nutzung unter Einschaltung von Stellen

[35] Gesetz über das Wohnungseigentum und das Dauerwohnrecht vom 15. März 1951, BGBl. I S. 175, ber. S. 209

außerhalb des Katasteramtes besser kontrolliert werden muß. Die automatisierte Nutzung kann in dem Umfang, in dem Dritte - bei Darlegung eines berechtigten Interesses - Auskünfte und Auszüge erhalten können, auch wirtschaftlichen Unternehmen der Gemeinden und Ämter gewährt werden. Die Bußgeldvorschriften wurden insgesamt an die neue gesetzliche Situation angepaßt.

3.2.2 Unschädlichkeitszeugnisse im Grundstücksverkehr

Vom MI erhielt ich die Gelegenheit zur Stellungnahme zu einem Runderlaß betreffend das "Verfahren zur Erteilung von Unschädlichkeitszeugnissen im Grundstücksverkehr". Der Runderlaß wird ergänzt durch Formblätter, die als Anlagen 1 bis 11 an den knappen Textteil angefügt sind.

Hinter dem langen Namen des Runderlasses steht ein Verfahren, mit dem durch ein behördliches Zeugnis festgestellt wird, daß eine beabsichtigte Rechtsänderung für die Beteiligten nach einem vereinfachten und daher zeitlich stark verkürzten Verfahren abgewickelt werden kann. In jedem Fall kann nur ein Teil, der "im Verhältnis zum verbleibenden Teil des Grundstücks" einen geringen Wert hat, auf diese vereinfachte Weise von einem auf einen anderen Eigentümer übertragen werden.

Die vereinfachte Eigentumsübertragung bedingt eine starke Formalisierung. Diese wiederum hat zur Folge, daß Daten möglicher Beteiligter weitergegeben werden müssen, und zwar vorab bei der Anhörung sowie nach Prüfung des Antrags bei der Erteilung des beantragten Unschädlichkeitszeugnisses.

Die wesentlichen Vorgaben zu dem Verfahren sind in einem Landesgesetz festgelegt. Durch meine Beteiligung konnten daher nur geringfügige Änderungen im Sinne des Datenschutzes bewirkt werden. Allerdings habe ich erreicht, daß die öffentliche Bekanntgabe des Überprüfungsergebnisses, die nach § 9 Abs. 2 des Gesetzes über Unschädlichkeitszeugnisse im Grundstücksverkehr (GUZ)[36] ohne Bindung an ein Erfordernis zugelassen ist, infolge der Ausführungen in dem Runderlaß nur dann erfolgen darf, wenn eine Einzelbekanntmachung nicht oder nur schwer möglich ist. Der Erlaßgeber ist damit meinen Vorstellungen gefolgt, wonach eine öffentliche Bekanntmachung an einem strengen Erforderlichkeitsmaßstab gemessen werden muß, weil davon auszugehen ist, daß in aller Regel die Beteiligten (Eigentümer sowie Inhaber von im Grundbuch eingetragenen oder durch Eintragung gesicherten Rechten an dem Grundstück oder an einem das Grundstück belastenden Recht) der Behörde durch das vorangegangene Verfahren bekannt sein dürften.

[36] vom 8. Januar 1996, GVBl. I S. 2

3.3 Polizei

3.3.1 EUROPOL

Mitte 1995 ist die Konvention zur Errichtung eines Europäischen Polizeiamtes (EUROPOL) von den ständigen Vertretern der Mitgliedsstaaten der Europäischen Union in Brüssel unterzeichnet worden. Wegen der bis dahin noch offenen Frage, ob ein durch EUROPOL in seinen Rechten verletzter Bürger vor dem Europäischen Gerichtshof (EuGH) klagen kann, ist die Konvention zunächst nicht in Kraft getreten. Darüber haben sich die Mitgliedstaaten erst Mitte 1996 in Form einer sog. "Vorabentscheidungskompetenz" des EuGH geeinigt. Die nationalen Gerichte können im konkreten Einzelfall dem EuGH Fragen zur Auslegung der Konvention zur Vorabentscheidung vorlegen. Eine direkte Klage des Betroffenen ist dagegen nicht vorgesehen. Das zur Ratifizierung des Abkommens erforderliche Gesetz ist von der Bundesregierung im Oktober 1996 vorgelegt worden. Zu dem Entwurf habe ich Stellung genommen.

Vorab ist anzumerken, daß dieser Entwurf[37], ebenso wie schon der Entwurf eines Bundeskriminalamtgesetzes (BKA-Gesetz)[38], auf den ersterer sich an mehreren Stellen bezieht, die Tendenz verstärkt, polizeirechtliche Kompetenzen aus der Zuständigkeit der Länder in den Bund zu verschieben.

3.3.1.1 Verantwortliche Stellen

Zuständige Behörde für EUROPOL soll das BKA sein, das damit die Aufgaben der nationalen Stelle wahrnimmt. Unabhängig davon, ob es BKA-eigene Daten oder Daten der Länderpolizeien an EUROPOL übermittelt, ist ausschließlich das BKA zuständig für Änderungen, Berichtigungen und Löschungen der Daten einschließlich der Länderdaten sowie für die Weiterleitung der Auskunftsbegehren von Bürgern. Hier sollte eine Änderung des Entwurfs dahingehend erfolgen, daß die Änderung, Berichtigung und Löschung von Landesdaten nur aufgrund einer Mitteilung der für die Daten verantwortlichen Länderpolizei erfolgen kann. Im Zusammenhang mit den Auskunftsrechten der Bürger sollte die Norm dahingehend erweitert werden, daß auch die Länderpolizeien zuständige Stellen zur Entgegennahme von Auskunftsanträgen sind, wenn das jeweilige Landeskriminalamt selbst Datenspeicherungen in EUROPOL veranlaßt hat. Es ist damit verantwortlich für die Erteilung bzw. Verweigerung der Auskunft. Das BKA selbst sollte lediglich die Vorgaben der datenschutzrechtlich verantwortlichen Landespolizeien umsetzen.

3.3.1.2 Analyse-Dateien

Der Entwurf nennt als Übermittlungszweck u. a. die Analyse von Straftaten. Eingriffsbefugnisse hat die Polizei jedoch nur zur Erfüllung der ihr zugewiesenen Aufgaben der Gefahrenabwehr oder Strafverfolgung. Der Gesetzgeber sollte klarstellen, daß es unzulässig ist, personenbezogene Daten nur zum Zweck der Analyse zu übermitteln und zu verarbeiten.

3.3.1.3 Datenschutzkontrolle und -haftung

Im Entwurf wird dem Bundesbeauftragten für den Datenschutz die Aufgabe der nationalen Kontrollinstanz zugewiesen. Dies kann jedoch nur zutreffen, soweit es um die Kontrolle des BKA als Zentralstelle geht. Andernfalls bliebe

---

37 vom 20. Dezember 1996, BR-Drs. 957/96

38 vom 31. Mai 1995, BT-Drs. 13/1550

unberücksichtigt, daß die Landesbeauftragten für die Datenschutzkontrolle bei den Ländern zuständig sind, denen der Entwurf jedoch ausdrücklich die Verantwortung für die von Ihnen veranlaßte Datenverarbeitung in EUROPOL zuweist. Der Gesetzentwurf muß klarstellen, daß die Stellungnahme des Ländervertreters in der Gemeinsamen Kontrollinstanz immer dann "maßgebliche Berücksichtigung" findet, wenn Länderinteressen berührt werden.

Unterdessen hat der Bundesrat zu dem Gesetzentwurf Stellung genommen und die Vorschläge der Datenschutzbeauftragten der Länder zu ihrer Stellung in der Gemeinsamen Kontrollinstanz aufgegriffen. Das Gesetzgebungsverfahren ist noch nicht abgeschlossen.

3.3.2 Prüfung von Telefonüberwachungsmaßnahmen im Landeskriminalamt

Im Zusammenhang mit den datenschutzrechtlichen Prüfungen der Telefonüberwachungsmaßnahmen (TÜ-Maßnahmen) gem. § 100 a Strafprozeßordnung (StPO)[39] in den Staatsanwaltschaften (vgl. unter 4.4) sind auch das für die praktische Durchführung der TÜ-Maßnahmen zuständige Sachgebiet und das Dezernat Organisierte Kriminalität im Landeskriminalamt (LKA) geprüft worden.

3.3.2.1 Prüfung im Sachgebiet TÜ

Dem Sachgebiet ist die Aufgabe zugewiesen, die technisch-organisatorische Umsetzung von TÜ-Maßnahmen zu realisieren. Es betreibt keine eigenständigen Ermittlungen, sondern dient als technische Unterstützung für die von anderen Polizeidienststellen bzw. der Staatsanwaltschaft im Zuge ihrer Ermittlungen veranlaßten TÜ-Maßnahmen. Dabei wird das Sachgebiet nicht nur für eigene - vom LKA betriebene - Ermittlungsverfahren tätig, sondern auch für die Polizeipräsidien, die im übrigen selbst TÜ-Maßnahmen durchführen. Die dazu erforderlichen Aufzeichnungsgeräte stellt das LKA zur Verfügung.

Bei dem Kontrollbesuch wurden Ablauf und Dokumentation der TÜ-Maßnahmen geprüft.

- Auskunftsersuchen

Der ermittlungsführende Staatsanwalt ist zuständig für die Beantragung eines richterlichen Beschlusses zu einer TÜ-Maßnahme. Das Sachgebiet stellt die dazu erforderlichen Angaben zur Verfügung.

---

[39] BGBl. III 312-2

Dazu ersucht das Sachgebiet die Netz- und/oder Diensteanbieter um Auskunft über Name bzw. Telefonnummer des zu überwachenden Anschlusses sowie - falls erforderlich - über die dem Anschluß zuzuordnenden Verbindungsdaten. Rechtsgrundlagen sind das Gesetz über die Regulierung der Telekommunikation und des Postwesens (PTRegG)[40] für Auskünfte der Deutschen Telekom AG bzw. § 161 a StPO für Auskünfte anderer Netzbetreiber. § 100 b Abs. 3 StPO verpflichtet die Netzbetreiber, das Abhören zu ermöglichen.

- Arbeits- und Beweisbänder

Aufgezeichnet werden die überwachten Telefongespräche auf einem Arbeits- und einem Beweisband. Die Laufzeit (Summe der aufgenommenen Gespräche) wird zweimal täglich in einer dem Abhörvorgang zugeordneten Dokumentation zusammen mit dem Zeitpunkt der Kontrolle und dem Namen des Kontrollierenden registriert. Ebenso wird bei der Entnahme bespielter Bänder verfahren. Der zuständige Ermittlungsbeamte erhält entweder täglich das Arbeitsband mit den aufgenommenen Telefongesprächen oder er wird zumindest über den Stand des Abhörvorgangs informiert. Nach Abschluß der Überwachungsmaßnahme übergibt das Sachgebiet dem Staatsanwalt die versiegelten Beweisbänder. Bis dahin sind sie in einem extra gesicherten Safe im Sachgebiet gelagert.

- Dokumentation

Jede durchgeführte TÜ-Maßnahme wird mit fortlaufender Nummer im sog. Tagebuch registriert. Mit Beginn der Überwachungsmaßnahme legt das Sachgebiet eine TÜ-Akte an, die dem ermittelnden Sachbearbeiter nach Abschluß gegen Quittung zusammen mit den Beweisbändern ausgehändigt wird. In einer weiteren Akte, der sog. Arbeitsakte, werden die durch die Anfrage bei den Netzbetreibern entstandenen schriftlichen Unterlagen, die einer TÜ-Maßnahme zugeordnet werden können, und die o. g. Quittung abgelegt. Die Arbeitsakte bleibt im Sachgebiet.

- Aufbewahrung

Zur Aufbewahrung der Unterlagen führt das LKA ein Sonderarchiv, in dem die als Sonderakten eingestuften Tagebücher und Arbeitsakten aufbewahrt werden. Die maximale Aufbewahrungsfrist für Tagebücher beträgt 5, für Arbeitsakten 10 Jahre.

- Vernichtung

Die schriftlichen Unterlagen, die sich keiner TÜ-Maßnahme zuordnen lassen, werden zweimal jährlich vernichtet. Über die Vernichtung wird ein Protokoll angefertigt. Schriftliche Unterlagen, die eine zeugenschaftliche Vernehmung i. S. v. § 161 a StPO sind, gehen an den zuständigen Sachbearbeiter zur weiteren Verwendung. Die Arbeitsakten werden zusammen mit den Tonträgern im Beisein des zuständigen Staatsanwaltes vernichtet.

[40] vom 14. September 1994, BGBl. I S. 2325, 2371, ber. BGBl. I 1995 S. 103 verkündet als Art. 7 des Postneuordnungsgesetzes vom 14. September 1994, BGBl. I S. 2325, in Kraft am 1. Januar 1995

- Ergebnis der Prüfung

Die Prüfung der technisch-organisatorischen Realisierung von TÜ-Maßnahmen einschließlich der Dokumentation einzelner Verfahrensschritte, der Unterlagen sowie der Dokumentation ihres Verbleibs bzw. ihrer Vernichtung im Sachgebiet ergab keinerlei datenschutzrechtliche Mängel.

3.3.2.2 Datenschutzrechtliche Prüfung von Telefonüberwachungsmaßnahmen im Dezernat Organisierte Kriminalität

Ziel der Prüfung waren die im Zusammenhang mit abgeschlossenen Ermittlungsverfahren aus den Jahren 1992 bis 1994 durchgeführten TÜ-Maßnahmen. Prüfungsgegenstand sollten nicht nur die Ermittlungsakten sein, soweit sie nicht an die Staatsanwaltschaft abgegeben worden waren, sondern auch das Verfahren der praktischen Durchführung.

Eine Prüfung der Akten abgeschlossener Ermittlungsverfahren konnte nicht durchgeführt werden, da das Dezernat alle Ermittlungsverfahren an die Staatsanwaltschaft abgegeben hatte und grundsätzlich keine Duplikate von Ermittlungsvorgängen behält. Diese Praxis ist als Ausdruck informationeller Sparsamkeit nur zu begrüßen. Die Darstellung des Verfahrensablaufs einer TÜ-Maßnahme durch das LKA ergab keine Anhaltspunkte für datenschutzrechtliche Mängel.

3.3.3 Zentrale Bußgeldstelle der Polizei

Mitte Januar 1997 hat die Zentrale Bußgeldstelle der brandenburgischen Polizei in Gransee ihre Arbeit aufgenommen. Sie ist landesweit zuständig für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten durch die Polizei. Dem ging ein ca. einjähriges Pilotprojekt beim Polizeipräsidium Oranienburg voraus, in dessen Verlauf nach und nach die zur vollautomatisierten Bearbeitung der Verwarn- und Bußgeldverfahren benötigte Hard- und Software angeschafft und in das Datenverarbeitungssystem eingepaßt wurde. Derzeit verfügen die Polizeipräsidien Oranienburg, Eberswalde und Frankfurt (Oder) über Online-Anschlüsse an die Zentrale in Gransee, die Polizeipräsidien Potsdam und Cottbus sowie die Wasserschutzpolizei sollen im Verlauf des Jahres folgen.

Zur Abwicklung der Verwarn- und Bußgeldverfahren betreibt die Zentrale Bußgeldstelle die personenbezogene Datei "SC OWi", die auch schon dem Pilotprojekt zu Verfügung stand. Im Hinblick auf die geplante brandenburgweite Datenverarbeitung der in Verwarn- und Bußgeldverfahren anfallenden Daten habe ich angeregt, die Errichtungsanordnung für diese Datei einer kritischen Überprüfung und Überarbeitung zu unterziehen und dabei auf folgende Punkte hingewiesen:

- Automatisierte Protokollierung

Dazu hat das MI mitgeteilt, daß alle Datenverarbeitungsvorgänge im Verfahren protokolliert werden.

- Grundsätzliche Speicherung aller Führerscheindaten eines Betroffenen

Die umfassende Speicherung aller Führerscheindaten eines Betroffenen ist nur dann erforderlich, wenn ein Fahrverbot erteilt wird. Soweit eine Ordnungswidrigkeit durch einen Bußgeldbescheid geahndet wird, sind vollständige Angaben zu der Fahrerlaubnis nicht erforderlich. Gem. § 111 OWiG[41] muß der Betroffene nur Vornamen, Familien- bzw.

[41] Gesetz über Ordnungswidrigkeiten , BGBl. III 454-1

Geburtsnamen, Familienstand, Beruf, Wohnort, Wohnung und Staatsangehörigkeit angeben. Eine Verpflichtung, die Führerscheindaten mitzuteilen, besteht nicht.

Das im Verfahren vorgesehene Datenfeld "Führerscheindaten" ist kein Pflichtfeld. Eine Speicherung der Führerscheindaten erfolgt nur, wenn die Daten beim Betroffenen im Rahmen einer Verkehrskontrolle erhoben wurden oder wenn ein Fahrverbot erteilt wurde.

- Zeugenangaben in den Schreiben an den Betroffenen

Im Verwarnungsverfahren ist die Angabe des Zeugen mit Name und Anschrift nicht erforderlich. Für die Wahrung des Rechtsstaatsprinzips ist es ausreichend, wenn der Betroffene darauf hingewiesen wird, daß es einen Zeugen für die Verkehrsordnungswidrigkeit gibt.

Dazu hat das MI mitgeteilt, daß nur Polizeibeamte mit Namen und Dienstgrad als Zeugen aufgeführt werden. Bei allen anderen Fällen wird das Feld "Zeugenaussage" angekreuzt, es sei denn, der Zeuge hat der Angabe seines Namens zugestimmt.

Gegen die endgültige Errichtungsanordnung "SC OWi" bestanden keine datenschutzrechtlichen Bedenken.

Nachdem die Zentrale Bußgeldstelle in den Gebäuden des Polizeipräsidiums Oranienburg als vorläufigen Standort ihre Arbeit aufgenommen hatte, habe ich mir die automatisierten Verfahrensabläufe vorführen lassen. Dabei fanden sich im Datenverarbeitungssystem keine datenschutzrechtlichen Mängel hinsichtlich der technischen oder organisatorischen Verfahrensabläufe.

3.3.4 Errichtungsanordnung/Dateibeschreibung: neue Bezeichnung/neuer Inhalt

Mit der 1996 erfolgten Novellierung des Brandenburgischen Polizeigesetzes (BbgPolG)[42] ist die Verpflichtung der Polizei weggefallen, für jede Datei eine Errichtungsanordnung aufzustellen. Statt dessen legt § 48 Abs. 2 BbgPolG fest, daß eine Dateibeschreibung gem. § 8 BbgDSG vorzulegen ist, die neben anderen Angaben auch die in §§ 37, 39 Abs. 2, 57 BbgPolG festgelegten Löschungs- und Prüfungstermine sowie Aufbewahrungsfristen enthalten muß. Was auf den ersten Blick wie eine schlichte Umbenennung aussieht, durch die der Inhalt im wesentlichen unverändert bleibt, erweist sich in der praktischen Umsetzung durch das Zusammenwirken mehrerer Umstände als ziemlich problematisch.

§ 8 Abs. 3 BbgDSG ermächtigt die Landesregierung, den näheren Inhalt der Dateibeschreibung nach Abs. 1 durch Rechtsverordnung zu bestimmen. Das mit der Verordnung zur Dateibeschreibung (DBeschrV)[43] in Kraft gesetzte - für alle Landesverwaltungen verbindliche - Formular zur Dateibeschreibung wird den Anforderungen im Polizeibereich jedoch nicht gerecht. Insbesondere die zur eigenen und zur datenschutzrechtlichen Kontrolle erforderliche Zweckbestimmung der Datei sowie die Rechtsgrundlagen sind mit dem zur Verfügung stehenden Formular nur so unzulänglich anzugeben, daß sich dies zum Nachteil für die Betroffenen auswirken kann. Das Formular muß daher für den Polizeibereich geändert werden.

---

42 Gesetz über die Aufgaben und Befugnisse der Polizei im Land Brandenburg vom 19. März 1996, GVBl. I S. 74

43 vom 7. Oktober 1996, GVBl. II S. 695

Ob Errichtungsanordnung oder Dateibeschreibung: Beide haben gravierende Auswirkungen auf das Persönlichkeitsrecht der Betroffenen, über die die Polizei gem. §§ 37 bis 39 BbgPolG Daten speichern und verändern darf. Anhand der Errichtungsanordnung/Dateibeschreibung entscheidet der Sachbearbeiter, ob und in welche Datei der Datensatz eines Betroffenen einzustellen ist, ob wegen bestimmter Tatsachen, wie z. B. wegen des Delikts, der Motivation oder der Tatbegehung, zusätzlich auch eine Speicherung in einer bundesweiten Datei in Frage kommt und wie lange der Datensatz vorgehalten wird.

Sie sollen sowohl der Eigenkontrolle der datenverarbeitenden Stelle, die die Datei errichtet, als auch der externen Kontrolle durch den Datenschutzbeauftragten dienen, der anhand der Festlegungen einer Errichtungsanordnung/Dateibeschreibung die Rechtmäßigkeit der Speicherungen prüft.

Um den Anforderungen gerecht zu werden, müssen Dateibeschreibungen folgende gesetzlich festgelegte Angaben enthalten: Dateibezeichnung, Zweck, Rechtsgrundlage, Personenkreis sowie die von jedem Betroffenen zu erfassenden personenbezogenen Daten, Übermittlungen einschließlich der Datenart und des Empfängers bzw. des Absenders sowie die Löschungsfristen (§ 8 BbgDSG). Dies entspricht im wesentlichen den Angaben einer Errichtungsanordnung gemäß dem alten Polizeigesetz.

Besondere Bedeutung hat die Rechtsgrundlage. Damit können jedoch nicht nur die allgemeinen Befugnisnormen zur Datenspeicherung des Polizeigesetzes (§§ 37 bis 39 i. V. m. der Aufgabenzuweisung gem. § 1 BbgPolG) und ggf. der Strafprozeßordnung (§ 163 StPO) gemeint sein. Vielmehr müssen hier die Rechtsgrundlagen für die konkrete Aufgabenerfüllung, wie z. B. die Aufklärung und Verhütung bestimmter Straftaten oder von Straftaten eines bestimmten Deliktbereiches, hinzukommen, denen die Datei dient. Die Einstellung personenbezogener Daten eines Betroffenen in eine bestimmte Datei ist ein Grundrechtseingriff, der im konkreten Einzelfall nur unter den rechtlich festgelegten Voraussetzungen zulässig ist. Die Voraussetzungen bestimmen sich u. a. auch anhand der Straftat, mit der der Betroffene in Verbindung gebracht wird. Entgegen der Auffassung des Innenministeriums halte ich es daher für unerläßlich, daß bei den Rechtsvorschriften auch die Delikte gemäß Strafgesetzbuch aufgeführt werden, zu deren Verhütung und Aufklärung die entsprechende Datei betrieben wird. Wo sich bei Dateien, die im Zusammenhang mit umfangreichen Ermittlungsverfahren gegen bestimmte Tätergruppen eingerichtet werden, noch keine abschließende Aufzählung der in Frage kommenden Straftatbestände vornehmen läßt, muß zumindest der Deliktbereich benannt werden, auf den sich der Anfangsverdacht stützt.

Eine Errichtungsanordnung bzw. Dateibeschreibung ist eine unerläßliche Voraussetzung für den geordneten Betrieb einer Datei. Die ständige Beachtung der dort getroffenen Festlegungen sollte selbstverständlich sein. Wenn der Zweck sowie andere Voraussetzungen wie z. B. der Deliktbereich schon bei der Einstellung der Datensätze in die Datei nicht strikt eingehalten werden, ist eine effektive Nutzung auch durch eine später erfolgende Dateipflege nicht mehr herzustellen.

Eine solche Datei, die losgelöst von der Errichtungsanordnung betrieben wurde, habe ich in der Vergangenheit mehrfach geprüft[44]. Bei erneuter Kontrolle im Berichtszeitraum habe ich aufgrund der Mängel, die trotz erkennbarer Bemühungen augenscheinlich nicht mehr zu beheben waren, und insbesondere aber auch wegen der fehlenden Erforderlichkeit darauf gedrängt, die Datei aufzulösen und alle Datensätze zu löschen. Dem ist das Polizeipräsidium nachgekommen.

3.3.4.1 Datei "Index Libi-Vorzeigekartei"

[44] s. 2. Tätigkeitsbericht unter 3.6.2.4, S. 71

Die Datei wird in einem Polizeipräsidium als Vorgangsverwaltungsdatei geführt. Sie hat den Zweck der Verwaltung und der Registrierung personenbezogener Daten von denjenigen Personen, zu denen die Lichtbildvorzeigekartei (LVK) Täterfotos enthält. Die LVK wird durch die Richtlinie für die Führung der Lichtbildvorzeigekartei[45] noch geregelt.

- Richtlinien für die Führung der Lichtbildvorzeigekartei

In dem Runderlaß des MI aus dem Jahre 1993 sind Verfahrensregelungen zur eigentlichen LVK festgelegt. Rechtgrundlage für die in allen Polizeipräsidien des Landes geführten Karteien ist das Brandenburgische Polizeigesetz (§§ 1, 13 und 39 BbgPolG), demgemäß die Polizei die bei der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zweck der Gefahrenabwehr speichern, verändern und nutzen darf. Eine suchfähige Speicherung in Dateien und Akten ist jedoch nur über Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Den mit der Aufnahme seines Fotos in eine LVK verbundenen Eingriff in sein Persönlichkeitsrecht muß der Betroffene aber auch auf der Grundlage der Strafprozeßordnung (StPO) hinnehmen. Die §§ 163 und 163 b StPO legen fest, daß die Behörden und Beamten des Polizeidienstes Straftaten zu erforschen haben und dazu die Identität verdächtiger Personen feststellen dürfen. § 81 b StPO gestattet die Erstellung von Lichtbildern und Fingerabdrücken, soweit es für die Zwecke der Durchführung des Strafverfahrens oder des Erkennungsdienstes notwendig ist.

Voraussetzung für die Aufnahme in die LVK ist, daß die Betroffenen einer Straftat verdächtigt werden oder bereits überführt worden sind und Wiederholungsgefahr besteht. Auch Kinder und Jugendliche können in die LVK eingestellt werden, wenn dies wegen der Schwere der Tat und des bisherigen kriminellen Verhaltens angemessen erscheint. In jedem Fall ist jedoch der Grundsatz der Verhältnismäßigkeit bei der Entscheidung über die Aufnahme bzw. den Verbleib von Lichtbildern in der LVK zu beachten. Die Betroffenen müssen den nicht unerheblichen Eingriff in ihre Persönlichkeitsrechte nur hinnehmen, wenn das öffentliche Interesse an der Aufklärung von Straftaten überwiegt.

Bei der Einsichtnahme von Zeugen in die LVK sind Verfahrensvorkehrungen zum Schutz der Persönlichkeitsrechte der Betroffenen zu beachten. Zunächst darf eine Einsichtnahme nur erfolgen, wenn es vom Stand der Ermittlungen geboten ist. Den Zeugen einer Straftat werden zwar die Lichtbilder von evtl. in Frage kommenden tatverdächtigen Personen vorgelegt, dabei erfahren sie jedoch nicht die Personalien der Betroffenen.

Der o. g. Erlaß verpflichtet die Polizeipräsidien, die LVK mindestens einmal jährlich auf ihre Erforderlichkeit hin zu überprüfen. Lichtbilder müssen zumindest immer dann entfernt werden, wenn die abgebildete Person nach Aktenlage mindestens 5 Jahre in Freiheit war und in dieser Zeit keine Erkenntnisse über neue Straftaten angefallen sind.

- Dateibeschreibung

Die Dateibeschreibung zur Datei "Index Libi-Vorzeigekartei" entsprach nicht in allen Einzelheiten dem Erlaß. Darauf habe ich bei meiner Stellungnahme hingewiesen. Sie ist daraufhin dem Erlaß angepaßt worden.

Da ich aus datenschutzrechtlichen Gründen eine Verkürzung der maximalen Prüf- und Löschungsfristen (10 Jahre für Erwachsene, 5 Jahre für Jugendliche und 2 Jahre für Kinder) für erforderlich halte, habe ich zusätzlich vorgeschlagen, daß ein Jahr nach Einstellung in die Datei die Erforderlichkeit geprüft wird. Damit soll der Tatsache Rechnung getragen werden,

[45] vom 27. Oktober 1993, ABl. S. 1605

daß bei der Durchführung der erkennungsdienstlichen Maßnahme, dem Anlegen der Kriminalakte und der Aufnahme des Lichtbilds in die LVK noch nicht absehbar ist, ob sich der Tatverdacht gegen den Betroffenen bestätigt. Diese Erkenntnis liegt im allgemeinen erst nach Ablauf einer Jahresfrist und den zwischenzeitlich durchgeführten Ermittlungen vor. Ein Verbleib des Lichtbilds eines Betroffenen in der Vorzeigekartei und der Speicherung seiner personenbezogenen Daten in der o. g. Datei, gegen den sich der Anfangsverdacht nicht bestätigt hat, ist aus datenschutzrechtlichen Gründen unakzeptabel.

Das Ministerium hat zugesagt, diesen Vorschlag zu prüfen.

3.4 Verfassungsschutz

3.4.1 Dienstvorschriften

Im Laufe des vergangenen Jahres hat die Verfassungsschutzbehörde eine Reihe von Dienstvorschriften zur Informationsbeschaffung und -auswertung vorgelegt, zu denen meine Behörde wiederholt Stellung nehmen konnte:

- Dienstvorschrift über die Verarbeitung personenbezogener Daten in der Personenzentraldatei (PZD) des Nachrichtendienstlichen Informationssystems des Bundes und der Länder (NADIS) durch die Verfassungsschutzbehörde des Landes Brandenburg (DV NADIS-PZD)

Zwar läßt die Dienstvorschrift insgesamt erkennen, daß es der Verfassungsschutzbehörde ein Anliegen ist, dem Gebot der informationellen Sparsamkeit Rechnung zu tragen und die Persönlichkeitsrechte der Betroffenen durch Verfahrensvorkehrungen, wie z. B. die Zeitspeicherung, zu sichern, dennoch enthält sie zu weitgehende Erfassungsregelungen. So habe ich Bedenken gegen den Kreis der zu erfassenden Personen sowie den Datenumfang insgesamt.

Die Verfassungsschutzbehörden des Bundes und der Länder führen NADIS-PZD als Aktennachweissystem, in dem nur solche personenbezogenen Daten gespeichert werden, die zum Auffinden der Akten erforderlich sind. Dies gilt auch für die Speicherung von Identifizierungsdaten. Auch hier muß der Speicherungsumfang auf das zum Auffinden der Akten erforderliche Maß beschränkt werden. Operative Interessen, wie die Personenidentifizierung bzw. die Zuordnung einzelner Personen zu bestimmten Zusammenhängen, sind von der Zweckbestimmung der NADIS-PZD nicht mehr erfaßt. Ich habe Zweifel, ob eine Reihe von Angaben im Regelfall für das Auffinden von Akten benötigt werden. Ich verkenne nicht, daß bestimmte über die Identdaten hinausgehenden Angaben in einer - wenn auch verhältnismäßig geringen - Anzahl von Einzelfällen erforderlich sein können und ihrer Natur nach für diesen Zweck prinzipiell auch geeignet sind. Eine grundsätzliche und in jedem Fall erfolgende Erfassung ist jedoch unverhältnismäßig.

Des weiteren habe ich darauf hingewiesen, daß die Grenzen des § 6 Satz 2 Bundesverfassungsschutzgesetz (BVerfSchG)[46] dann überschritten sein dürften, wenn in NADIS-PZD eine Verbindung zu namentlich bezeichneten Dritten hergestellt wird, ohne daß diese in NADIS oder amtseigenen Dateien selbständig als verfassungsschutzrelevant erfaßt sind. Zwar können Dritte gem. § 7 Abs. 1 Ziff. 3 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[47] vom Einsatz

[46] vom 20. Dezember 1990, BGBl. I S. 2954, geänd. d. § 38 Abs. 2 SicherheitsüberprüfungsG vom 20. April 1994, BGBl. I S. 867

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

nachrichtendienstlicher Mittel betroffen sein, für die Speicherung dieser Personen in der Verbunddatei NADIS fehlt es jedoch an einer entsprechenden gesetzlichen Grundlage. Hierauf sollte insbesondere bei der Erfassung von Kontakt- und sonstigen Personen geachtet werden. Auch wenn in der Dienstvorschrift ausdrücklich festgelegt worden ist, daß die Speicherung personenbezogener Daten in NADIS-PZD erst zulässig ist, wenn die Verfassungsschutzrelevanz der entsprechenden Bestrebung festgestellt ist, wird damit nicht ausgeschlossen, daß die nicht verfassungsschutzrelevanten Kontaktpersonen bzw. Dritte im Zusammenhang mit der entsprechenden Bestrebung gespeichert werden könnten. Hier wäre eine Klarstellung nötig.

Des weiteren habe ich gefordert, daß die Dienstanweisung die Zeitdauer der Speicherung verbindlich vorgeben sollte und die Daten daraufhin zu löschen sind, wenn der Sachverhalt bis zum Fristablauf nicht abschließend geklärt wurde. Ohne eine solche Festlegung läuft die mit der Zeitspeicherung verbundene Absicht, NADIS-PZD nicht mit ungeklärten Sachverhalten zu belasten, ins Leere.

Um eine regelmäßige Dateienpflege zu gewährleisten, bedarf es in der Dienstvorschrift verbindlicher Fristen zur Erforderlichkeitsprüfung, nach deren Ablauf der Vorgang dem zuständigen Referatsleiter zur Entscheidung über die Weiterspeicherung oder die Löschung automatisch vorgelegt wird.

Die Verfassungsschutzbehörde hat diese Punkte nicht aufgegriffen.

- Dienstvorschrift für die Auswertung von Informationen auf dem Gebiet des politischen Extremismus für die Verfassungsschutzbehörde des Landes Brandenburg (DV Auswertung)

Nach eigenem Selbstverständnis versteht die Verfassungsschutzbehörde sich als politisches Frühwarnsystem vor extremistischen Tendenzen, die demokratische Schutzgüter gefährden könnten. Ihre Aufgabe ist die Feldbeobachtung und Analyse politisch relevanter gesellschaftlicher Strömungen und Sachverhalte, nicht die Täterermittlung. Letzteres gehört zum Aufgabenbereich der Strafverfolgungsbehörden.

In der Dienstvorschrift wird das nicht deutlich. Sie richtet die Aufgabenwahrnehmung stärker auf Personen als auf inhaltliche Ziele, Meinungen und Ideologien aus. Bei einer zu starken Konzentration auf Personen sehe ich jedoch gerade bei Organisationen, die extremistisch beeinflußt zu sein scheinen, die Gefahr einer Fehleinschätzung zu einzelnen Personen und damit einer länger dauernden rechtswidrigen Beobachtung durch die Verfassungschutzbehörde mit der Folge nicht erforderlicher Datenspeicherung. Dem Vorschlag, die Dienstvorschrift dahingehend zu überarbeiten, ist die Verfassungsschutzbehörde jedoch nicht gefolgt.

Sie hat jedoch die Anregung aufgegriffen, der Parlamentarischen Kontrollkommission zur Unterstützung ihrer Funktion als Kontrollorgan in Angelegenheiten des Verfassungsschutzes gem. § 23 BbgVerfSchG jährlich eine aktualisierte Liste der Beobachtungsobjekte zur Kenntnis zu geben.

Auch in dieser Dienstvorschrift scheint mir der zulässige Umfang von Informationen über relevante Kontaktpersonen zu groß. Er sollte sich auf das zur eindeutigen Identifizierung notwendige Mindestmaß beschränken, soweit es zur Aufgabenerfüllung der Verfassungsschutzbehörde überhaupt erforderlich ist, Personen zu erfassen, die selbst keiner Bestrebung gem. § 23 Abs. 1 Ziff. 1 oder 3 BbgVerfSchG zuzurechnen sind.

- Dienstvorschrift für die Beschaffung von Informationen auf dem Gebiet des politischen Extremismus der

Verfassungsschutzbehörde des Landes Brandenburg (DV Beschaffung)

Die Dienstvorschrift trifft u. a. Vorkehrungen, die bei der Durchführung von Befragungen zu beachten sind, darunter auch solche für die Durchführung von Befragungen von Kindern und Jugendlichen. Ich habe davon abgeraten, daß Minderjährige im Zusammenhang mit verfassungs- schutzrelevanten Sachverhalten überhaupt befragt werden sollen, da sie aufgrund ihrer Entwicklung noch nicht in der Lage sind, die Konsequenzen einer solchen Befragung abzuschätzen.

In § 6 Abs. 3 Satz 3 BbgVerfSchG ist festgelegt, daß Personen, die aus beruflichen Gründen ein Zeugnisverweigerungsrecht haben, von der Verfassungsschutzbehörde nicht in Anspruch genommen und Informationen von Ihnen nicht entgegengenommen werden dürfen. Daraus folgt, daß solche Personen von der Verfassungsschutzbehörde auch nicht zu befragen sind.

Die Verfassungsschutzbehörde ist meinen Anregungen dahingehend gefolgt, daß die Befragung von Kindern unzulässig ist; bei Jugendlichen soll besondere Zurückhaltung geübt werden. Personen, denen aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, dürfen nicht um Auskünfte gebeten werden, die in unmittelbarem Zusammenhang mit der Berufsausübung stehen. Auskünfte über andere Sachverhalte sind jedoch zulässig. Weder Kinder noch Personen, die der Amtsverschwiegenheit unterliegen, können als Vertrauensleute angeworben werden.

3.4.2 Prüfungen bei der Verfassungsschutzbehörde

Im Berichtszeitraum habe ich aus unterschiedlichen Anlässen Verwaltungsakten bzw. Vorgänge zu verschiedenen Gruppen

- Scientology-Church
- Kampagne gegen die Wehrpflicht

geprüft.

In beiden Fällen ergab die Prüfung, daß die Verfassungsschutzbehörde keine personenbezogenen Unterlagen führt. Zu beiden Gruppen gibt es Sachakten, in denen aus öffentlichen Quellen oder Publikationen der Gruppen stammende Vorgänge mit Personennennungen abgelegt sind. Eine Auswertung nach einzelnen Personen ist jedoch nicht erfolgt.

- Jugendprojekt "Neues Leben Dreieck Rathenow e. V."

Durch einen Journalisten bin ich auf die Zusammenarbeit der Verfassungsschutzbehörde mit dem Jugendprojekt aufmerksam gemacht worden. Der Reporter wollte u. a. wissen, ob es zulässig sei, daß die Verfassungsschutzbehörde Kinder bzw. Jugendliche beobachte. Gemäß § 9 BbgVerfSchG dürfen personenbezogene Daten Minderjähriger erfaßt werden. Um mich zu vergewissern, daß die besonderen Vorkehrungen zum Schutz von Kindern und Jugendlichen gemäß der Rechtsvorschrift beachtet worden sind, habe ich den Vorgang geprüft.

Die Verfassungsschutzbehörde hat erläutert, daß die Teilnahme an "Runden Tischen" sowie ähnlichen Gesprächskreisen nur auf Einladung der Initiatoren solcher Treffen erfolgt und daß die Verfassungsschutzmitarbeiter dort jeweils offen als solche auftreten. Unterlagen, die sich aus der Teilnahme ergeben, werden im Referat Verfassungsschutz durch Aufklärung/Öffentlichkeitsarbeit aufbewahrt und dort auch nur zu dessen Zwecken genutzt. Grundsätzlich ist jedoch festzustellen, daß auch solche Unterlagen zur Aufgabenerfüllung der Verfassungsschutzbehörde gemäß § 3 BbgVerfSchG

erforderlich sein müssen. Soweit sie benötigt werden, um die Arbeit eines Gremiums oder eines Projektes nachzuvollziehen, bedarf es im Regelfall keiner personenbezogenen Angaben. Vielmehr dürfte ein Sachverhaltsvermerk genügen. Personenbezogene Angaben sind daher zu vernichten bzw. in den Unterlagen zu schwärzen.

Die Prüfung der zum o. g. Projekt geführten Akten ergab, daß sie Anwesenheitslisten und Protokolle, darunter Wortprotokolle von Sitzungen des Vereins, sowie einen umfänglichen Schriftwechsel zwischen dem Vereinsvorstand und dem Projektleiter mit zahlreichen personenbezogenen Daten enthalten. Vor allem der Schriftwechsel gab Anlaß zu datenschutzrechtlichen Bedenken, da in ihm Ausführungen über die beruflichen Qualitäten Dritter zu finden sind.

Die Erhebung und Speicherung personenbezogener Daten im o. g. Rahmen hat keine Rechtsgrundlage, da der Verein einschließlich der Mitarbeiter sowie der Teilnehmerkreis an den Vereinssitzungen keinen verfassungsschutzrelevanten Bestrebungen gem. § 3 BbgVerfSchG zuzurechnen sind. Als Rechtsgrundlage können auch nicht die allgemeinen Bestimmungen des Brandenburgischen Datenschutzgesetzes herangezogen werden, weil die Datenverarbeitung der Verfassungsschutzbehörde bereichsspezifisch und damit abschließend im Verfassungsschutzgesetz geregelt ist. Die personenbezogenen Daten müssen daher gelöscht werden.

Schon während der Prüfung hat die Verfassungsschutzbehörde zugesagt, die Anwesenheits- und Verteilerlisten aus der Akte zu entfernen. Dies ist zwischenzeitlich geschehen. Bezüglich der anderen Prüfungsfeststellungen konnte sich die Verfassungsschutzbehörde noch nicht äußern, da die Prüfung erst in jüngster Zeit erfolgt ist.

Die Unterstützung des Vereins "Neues Leben Dreieck Rathenow e. V." durch den Verfassungsschutz erfolgte mit dem Ziel, das Projekt wissenschaftlich zu begleiten und durch den vom Verfassungsschutz ausgewählten Projektleiter eine Studie erstellen zu lassen. Da zwischen dem Verein und dem Projektleiter unterschiedliche Auffassungen zu Fragen des Datenschutzes bestehen, habe ich der Verfassungsschutzbehörde zugesagt, die Studie unter datenschutzrechtlichen Gesichtspunkten zu prüfen, um so sicherzustellen, daß gesetzliche Bestimmungen eingehalten werden.

3.4.3 Datenübermittlung anderer Behörden an den Verfassungsschutz

Schon in früheren Tätigkeitsberichten[48] hatte ich mich mit den problematischen Datenübermittlungen anderer Behörden an die Verfassungsschutzbehörde befaßt. Hauptlieferant personenbezogener Daten ist die Polizei. Die Frage, inwieweit die Verfassungsschutzbehörde Personen erfassen darf, die ihr als Demonstrationsteilnehmer von der Polizei übermittelt worden sind, war auch im Berichtszeitraum wieder Gegenstand von Erörterungen mit der Verfassungsschutzbehörde sowie im Landtag.

Eingriffsbefugnisse hat die Polizei gegenüber Personen, von denen entweder eine Gefahr ausgeht (§ 5 BbgPolG[49]) oder die sich an sog. gefährdeten oder gefährlichen Orten (gem. § 12 Abs. 1 Ziff. 2 und 3 BbgPolG) aufhalten. Die Eingriffsbefugnis ist in beiden Fällen jedoch daran geknüpft, daß Tatsachen oder Anhaltspunkte zu den betroffenen Personen vorliegen, die auf eine konkrete Gefahr oder das Begehen einer Straftat hinweisen. Bloße Einschätzungen oder Erfahrungen der Polizei reichen nicht aus. Gerade bei Identitätskontrollen an gefährlichen oder gefährdeten Orten sind höhere Anforderungen an die Eingriffsvoraussetzungen zu stellen. Sie sind nur im Hinblick auf Straftaten von erheblicher Bedeutung gegeben. Insbesondere aber müssen die Eingriffsvoraussetzungen im Polizeibereich liegen. Die nachträgliche Feststellung der

[48] s. 3. Tätigkeitsbericht unter 3.6.2.3 und 4. Tätigkeitsbericht unter 3.2.6

[49] vom 21. März 1996, GVBl. I S. 74

Verfassungsschutzbehörde, daß über die Betroffenen bereits Erkenntnisse bei ihr vorliegen, rechtfertigt weder die Erhebung noch die Übermittlung der Daten durch die Polizei.

Die bloße Teilnahme an einer nicht angemeldeten Demonstration ist mit Ausnahme von Demonstrationen innerhalb der Bannmeile eines Gesetzgebungsorgans des Bundes oder eines Landes bzw. des Bundesverfassungsgerichts nicht strafbewehrt (§ 16 VersammlG[50] i. V. m. § 106 StGB). Sie ist weder eine Straftat von erheblicher Bedeutung, noch eine Ordnungswidrigkeit, es sei denn, die Demonstration ist durch ein nachvollziehbares Verbot - also vorher - untersagt worden (§ 29 Abs. 1 VersammG).

Bei den Übermittlungen von Festnahmelisten ist weiterhin zu beachten, daß die Mehrzahl der Daten im Rahmen von Personalienfeststellungen und Ingewahrsamnahmen zur Durchsetzung von Platzverweisen bei Demonstrationen erhoben und die Listen bei der Polizei selbst nur zu kurzfristigen Dokumentationen polizeilichen Handelns gem. § 39 Abs. 1 BbgPolG gespeichert werden. Die Betroffenen dürften nur in wenigen Ausnahmefällen einer verfassungsschutzrelevanten Bestrebung zuzurechnen sein, so daß eine Übermittlung vollständiger Listen unverhältnismäßig ist.

Zu einer solchen Überprüfung vor der Übermittlung ist die Polizei gem. § 14 BbgVerfSchG verpflichtet. Während nämlich § 14 Abs. 1 BbgVerfSchG alle Landesbehörden verpflichtet, der Verfassungsschutzbehörde - ohne Ersuchen - Informationen zu übermitteln, die sich auf den gewaltgeneigten Extremismus und die Spionage beziehen, also die Übermittlungsverpflichtungen für die gesamte öffentliche Verwaltung auf die besonders gefährlichen verfassungsrelevanten Tatbestände beschränkt werden, normiert § 14 Abs. 2 BbgVerfSchG für die Polizei (und die Staatsanwaltschaft) eine Übermittlungsverpflichtung auch für den nicht gewaltgeneigten politischen Extremismus. In den Fällen des Abs. 1 obliegt die Erforderlichkeitsprüfung der Verfassungsschutzbehörde, in Fällen des Abs. 2 sind Polizei und Staatsanwaltschaft vor der Übermittlung verpflichtet, anhand "tatsächlicher Anhaltspunkte" zu prüfen, ob "die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist" (§ 14 Abs. 2 BbgVerfSchG). Daraus ergibt sich, daß die Polizei in jedem Einzelfall prüfen muß, ob die Voraussetzungen gem. Abs. 1 oder 2 gegeben sind, ob also die zu übermittelnden Informationen für die Aufgabenerfüllung der Verfassungsschutzbehörde erforderlich sind.

Die Erforderlichkeitsprüfung der zur Übermittlung verpflichteten Behörden enthebt die brandenburgische Verfassungsschutzbehörde jedoch nicht, ihrerseits selbst zu prüfen, ob die übermittelten Erkenntnisse im Einzelfall zur Aufgabenerfüllung erforderlich sind, und sie andernfalls zu vernichten.

Wie schon im 4. Tätigkeitsbericht dargelegt, habe ich angeregt, den beteiligten Behörden einen Erlaß an die Hand zu geben, der Kriterien und Verfahren für die Prüfungspflichten festlegt. Bei der Beratung jenes Berichtes und der Stellungnahme der Landesregierung hierzu im Landtag hat sich auch die zuständige parlamentarische Kontrollkommission mit dem Thema befaßt. Ein Entwurf eines Erlasses über die "Richtlinien über die Zusammenarbeit der Polizei des Landes Brandenburg mit den Nachrichtendiensten" ist immer noch im internen Abstimmungsverfahren.

3.5 Ausländer

3.5.1 Die Rückführung jugoslawischer Bürgerkriegsflüchtlinge

[50] Gesetz über Versammlungen und Aufzüge, i. d. Fass. vom 15. November 1978, BGBl. III 2180-4

Die seit geraumer Zeit in der Öffentlichkeit diskutierte Rückführung von Bürgerkriegsflüchtlingen in die Teilstaaten der auseinandergebrochenen Republik Jugoslawien beschäftigt auch die Datenschutzbeauftragten. Zur Durchführung der Rückkehr sieht die Bundesregierung vor, daß die Länder personenbezogene Daten der Betroffenen an eine beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFI) eingerichtete Projektgruppe zur Datenerfassung übermitteln. Sie begründet die Datenverarbeitung damit, daß sie benötigt werde, um Flüchtlinge gezielt in Gebiete zurückbringen zu können, für deren Wiederaufbau die Europäische Union (EU) Mittel bereitgestellt habe.

Für die Datenerhebung und Übermittlung gibt es im Ausländergesetz keine Rechtsgrundlage. Auch das Brandenburgische Datenschutzgesetz kann nicht herangezogen werden, so daß die Erhebung und Übermittlung der Daten (Name, Geburtsdatum, Geburtsort, Familienstand, Beruf, Volkszugehörigkeit, letzter Wohnsitz in Bosnien-Herzegowina einschl. Anschrift, Kanton, in den die freiwillige Ausreise erfolgen soll, sowie Einreisedatum in Deutschland und zuständige Ausländerbehörde) allenfalls auf freiwilliger Basis erfolgen kann.

Das Ministerium des Innern, das ebenfalls keine Rechtsgrundlage für eine Erhebung ohne Zustimmung der Betroffenen sieht, hat die Ausländerbehörden des Landes Brandenburg angewiesen, die oben aufgeführten Angaben nur von denjenigen Personen zu erfassen, die freiwillig zurückkehren möchten. Die Daten werden an das MI übermittelt und von dort an das Bundesinnenministerium weitergeleitet.

Da das gesamte Verfahren auf die freiwillige Rückkehr abstellt, habe ich gegen die damit verbundene Datenerhebung und -übermittlung keine datenschutzrechtlichen Bedenken.

Den oben dargestellten Sachstand hat mir das Ministerium Ende Januar 1997 erneut bestätigt. Anfang März hatte das Innenministerium jedoch im Ausschuß für Europaangelegenheiten und Entwicklungspolitik über den Stand der Rückführung berichtet und dabei mitgeteilt, daß nunmehr auf "der Basis der Erlaßlage"[51] auch Zwangsrückführungen möglich seien. Diese Aussage bedarf der Klärung. Für einen Erlaß, der die unfreiwillige Rückkehr regelt, bedürfte es immer noch eines Gesetzes, das die Betroffenen verpflichtet, personenbezogene Angaben zu ihrer Person zu machen. An der Rechtslage hat sich jedoch bis dato nichts geändert, so daß eine gesetzliche Vorschrift für die Erhebung und Übermittlung von Daten zur Rückführung nicht vorhanden ist.

3.5.2 Einen ausländischen Gast muß man sich leisten können

Wer heutzutage einen ausländischen Gast einladen möchte, muß zunächst zur Ausländerbehörde, um dort eine Verpflichtungserklärung gem. § 84 Ausländergesetz (AuslG)[52] abzugeben. Die Verpflichtungserklärung soll die Visumerteilung durch die Auslandsvertretung beschleunigen.
Ein Petent hat sich an mich gewandt, weil die Ausländerbehörde bei der Abgabe der Verpflichtungserklärung nicht nur den Nachweis verlangt habe, daß er als Gastgeber auch tatsächlich in der Lage sei, für die Kosten aufzukommen, sondern auch den dazu vorzulegenden Gehaltsnachweis als Kopie zur Akte genommen habe.

Dies halte ich für unzulässig, da es für die Erhebung und Verarbeitung von Daten über die wirtschaftliche Situation des Gastgebers eines ausländischen Gastes an einer ausreichenden Rechtsgrundlage fehlt. § 84 AuslG regelt die Haftungsverpflichtung, die der Gastgeber gegenüber der Ausländerbehörde abgibt. Er verpflichtet sich damit, für alle

---

51 LT-Drs. 2/672, Ausschußprotokoll vom 6. März 1997, TOP 3

52 vom 9. Juli 1990, BGBl. III 26-6

Kosten einschließlich Versorgung im Krankheits- oder Pflegefall aufzukommen, die durch seinen Gast verursacht werden. Eine Befugnis der zuständigen Behörde zur Erhebung der auf der Verdienstbescheinigung aufgeführten Daten ist in der Vorschrift nicht enthalten. Die Rechtslage läßt zwar die Erhebung und Verarbeitung der Identdaten (Name, Vorname, Geburtsdatum und -ort, Anschrift und Paßdaten) des Gastgebers sowie des Gastes zu, weil ohne sie die Verpflichtungserklärung ins Leere laufen würde, für die weiteren darüber hinausgehenden Daten der Verdienstbescheinigung sehe ich jedoch keine Anhaltspunkte.

Soweit die Behörde nach der Vorschrift überhaupt befugt sein sollte, nachzuprüfen, ob ein Gastgeber in der Lage ist, seine freiwillig eingegangene Haftungsverpflichtung zu erfüllen, muß ihm zumindest freigestellt werden, in welcher Weise er dies der Behörde darlegt. Hier kämen also auch die Vorlage neutraler Einkommensnachweise (aus denen nur das Monatsnettoeinkommen ersichtlich ist), Bürgschaften o. ä. in Frage, die aber auch nicht in Kopie zu den Akten genommen werden dürfen. In der Praxis bedeutet dies, daß die Ausländerbehörde lediglich die Vorlage und Prüfung aktenkundig macht.

Dieser Auffassung hat sich das MI angeschlossen. Darüber hinaus hat es mitgeteilt, daß die Verpflichtungserklärung zu der Akte des ausländischen Gastes genommen wird und dort auch über den Zeitpunkt der Abreise hinaus verbleibt, selbst wenn während des Besuches kein Ereignis eingetreten ist, für das der Gastgeber gemäß seiner Verpflichtungserklärung aufkommen muß. Begründet wird diese Praxis damit, daß die Ausländerbehörde einen Anhaltspunkt für künftige Besuche des Betroffenen habe. Ich vertrete den Standpunkt, daß die Verpflichtungserklärung aus der Akte zu entnehmen ist, wenn der Anlaß entfallen ist. Eine weitere Aufbewahrung ist für die Aufgabenerfüllung der Ausländerbehörde nicht erforderlich. Das Ministerium des Innern hat sich dazu noch nicht äußern können.

3.5.3 Ehe oder Scheinehe?

Bei Ehen zwischen Ausländern und deutschen Staatsbürgern besteht häufig der Verdacht, sie würden nur zu dem Zweck geschlossen, dem ausländischen Ehepartner eine Aufenthaltsgenehmigung zu verschaffen.

Gem. § 92 Abs. 2 Nr. 2 AuslG ist es strafbar, sich - oder einem anderen - mittels unvollständiger oder unrichtiger Angaben eine Aufenthaltsgenehmigung oder Duldung zu beschaffen. Zur Feststellung, ob im Zusammenhang mit der Ehe unrichtige oder unvollständige Angaben gemacht wurden und dem Ausländer somit kein Aufenthaltsanspruch zusteht, dürfen die Ausländerbehörden personenbezogene Daten gem. § 75 Abs. 1 AuslG erheben. Die Datenerhebung ist zum Zweck der Ausführung ausländerrechtlicher Bestimmungen erforderlich, da die Erteilung von Aufenthaltstiteln u. a. an das Bestehen einer "ehelichen Lebensgemeinschaft" (§ 1353 BGB) geknüpft ist. Datenschutzrechtlich problematisch sind die Fälle, in denen bei der Ausländerbehörde Zweifel bestehen, ob die Angabe eines Ausländers, in einer ehelichen Lebensgemeinschaft zu leben, den Tatsachen entspricht.

Dazu hat das Ministerium des Innern mitgeteilt, daß die Ausländerbehörden nur tätig werden, wenn konkrete Anhaltspunkte, wie z. B. die Mitteilung des Einwohnermeldeamts, daß die Ehepartner in getrennten Wohnungen leben, vorliegen. In diesen Fällen lädt die Ausländerbehörde die beiden Ehepartner zu getrennten Anhörungen vor. Fragen, die unzulässig tief in den höchst persönlichen Bereich der Ehepartner eindringen, werden bei diesen Anhörungen nicht gestellt. Wenn die Zweifel durch die Anhörung nicht ausgeräumt werden können, erteilen die Ausländerbehörden eine befristete Aufenthaltserlaubnis.

Bei begründetem Verdacht auf Bestehen einer Scheinehe erstatten die Ausländerbehörden Strafanzeige bei der Polizei. Im

vergangenen Jahr wurden insgesamt 18 Ermittlungsverfahren durchgeführt. Auch dabei werden keine Fragen nach dem Vollzug der Ehe o. ä. unzulässig tief in die Privatsphäre der Betroffenen eindringende Fragen gestellt. Die Anzeigen durch die jeweils örtlich zuständigen Ausländerbehörden werden im automatisierten Anzeigetagebuch nachgewiesen. Eine Speicherung in anderen Dateien erfolgt nicht.

In datenschutzrechtlicher Hinsicht ist gegen das in Brandenburg praktizierte Verfahren bei der Ermittlung von sog. Scheinehen nichts einzuwenden.

3.6 Statistik

3.6.1 Musterdienstanweisung für kommunale Statistikstellen

Im Berichtszeitraum ist unter meiner Beteiligung vom MI eine Muster-Dienstanweisung für kommunale Statistikstellen erarbeitet worden[53]. Damit sind sowohl die rechtlichen als auch verwaltungsmäßigen Voraussetzungen für die Einrichtung von kommunalen Statistikstellen klar geregelt. Dies war auch erforderlich, weil Statistikstellen wegen der strengen Verpflichtung zur Einhaltung des Statistikgeheimnisses als eigene Verwaltungsstellen eingerichtet werden müssen, die räumlich, organisatorisch und personell von der übrigen Verwaltung abzuschotten sind.

Diese Muster-Dienstanweisung zur Aufgabenbeschreibung und Abschottung der kommunalen Statistikstelle ist als Empfehlung zu verstehen, die für die Umsetzung der vom Gesetzgeber geforderten Maßnahmen Hilfestellung geben will. Innerhalb dieses Rahmens werden Kommunen und/oder Landkreise ihre eigenen und speziellen Anweisungen entwickeln. Allerdings kann der geforderte Sicherheitsstandard dabei nicht unterschritten werden.

3.6.2 Errichtung kommunaler Statistikstellen, Nutzung von Einzelangaben aus der Gebäude- und Wohnungszählung 1995 und amtliche Veröffentlichungen

[53] vom 5. August 1996, Rundschreiben an die Landräte der Landkreise und Oberbürgermeister der kreisfreien Städte

Die Einrichtung kommunaler Statistikstellen hatte insbesondere für die Städte aktuelle Bedeutung, da sie die Einzelangaben aus der Gebäude- und Wohnungszählung 1995 (GWZ 95) für eigene kommunalstatistische Zwecke vom Landesamt für Datenverarbeitung und Statistik (LDS) erhalten wollten[54]. Gem. § 11 Abs. 5 BbgStatG ist dazu u. a. eine schriftliche Dienstanweisung erforderlich[55]. Nach Absprache zwischen dem LDS und meiner Behörde haben mir die Kommunen diese Dienstanweisungen zunächst vorgelegt. Nach den erforderlichen Verbesserungen entsprechen sie nunmehr bei fünf Städten den gesetzlichen Anforderungen, so daß gegen die Übermittlung von Einzelangaben aus der GWZ 95 datenschutzrechtlich keine Bedenken mehr bestehen. Zwei weitere Städte sind derzeit noch mit Überarbeitungen ihrer Dienstanweisungen beschäftigt.

Die Regeln für die statistische Geheimhaltung gelten nicht nur für Veröffentlichungen der Statistischen Ämter des Bundes und der Länder, sondern selbstverständlich auch für Kommunalstatistiken. Hinsichtlich der amtlichen Veröffentlichung der Gemeindetabellen durch das LDS war ich mit diesem übereingekommen, daß Angaben, die eine bestimmte statistische Größe (bei der GWZ 95 3 Gebäude) unterschreiten, nicht ausgewiesen werden. Entsprechend ist diese Größe auch immer bei der Erstellung von Kommunalstatistiken zu berücksichtigen, die kommunale Statistikstellen übermitteln oder veröffentlichen. Denn bei kommunalstatistischen Darstellungen spielen zusätzlich und in besonderem Maße die Kleinräumigkeit, die Tiefe der regionalen Gliederung und die Differenzierung der statistischen Merkmale eine Rolle. Deshalb sind in der Muster-Dienstanweisung für kommunale Statistikstellen ausdrücklich besondere Regeln für die Anonymisierung fixiert worden, die auch in die konkreten Dienstanweisungen der Kommunen so zu übernehmen waren.

3.6.3 Volkszählung 2001

Die EU will in allen Mitgliedsländern im Jahre 2001 eine allgemeine Volks- und Wohnungszählung durchführen. Aus Kostengründen möchte die Bundesregierung auf eine direkte Datenerhebung bei den Bürgern verzichten und statt dessen lieber die Melderegister der Einwohnermeldeämter sekundärstatistisch nutzen.

Anfängliche Überlegungen, dazu die Melderegister um sensible personenbezogene Daten für statistische Zwecke zu erweitern, sind offensichtlich vom Tisch. Die Datenschutzbeauftragten des Bundes und der Länder einerseits und Landesbehörden andererseits hatten auf die datenschutzrechtliche Unzulässigkeit eines solchen Vorgehens hingewiesen, weil dabei das Prinzip der strikten Trennung von Statistik und Verwaltungsvollzug, das wegen der statistischen Geheimhaltung sowohl verfassungsrechtlich als auch gesetzlich vorgeschrieben ist, erheblich verletzt worden wäre.

Die Statistiker streiten jetzt darum, in welchem Umfang die Melderegister in der Bundesrepublik wegen nicht aktueller Daten fehlerbehaftet sind und ob sie überhaupt eine korrekte statistische Grundlage für eine Volkszählung abgeben können. Denn gegen eine sekundärstatistische Erhebung auf der Basis der vorliegenden Meldedaten bei einem unveränderten Aufbau des Meldedatensatzes ist datenschutzrechtlich grundsätzlich nichts einzuwenden.

---

54 s. auch 4. Tätigkeitsbericht unter 3.4.2.2

55 s. unter 3.6.1

Die sauberste und datenschutzrechtlich klarste Lösung wäre allerdings eine Primärerhebung bei den Bürgern, vergleichbar etwa der Volkszählung 1987 und der Gebäude- und Wohnungszählung 1995[56]. Ein solches Verfahren ist auch für den Bürger am ehesten zu durchschauen. Welcher Weg letztlich tatsächlich gewählt wird, ist zur Stunde noch nicht abzusehen.

3.7 Sonstiges

3.7.1 Prüfung der Datenverarbeitung in der Landesfeuerwehrschule

Im Januar 1997 führten meine Mitarbeiter einen Kontrollbesuch in der Landesfeuerwehrschule durch. Das Ziel des Kontrollbesuches war, die Durchsetzung technisch-organisatorischer Maßnahmen gem. § 10 BbgDSG zu überprüfen. Im einzelnen wurden folgende Sachverhalte festgestellt:

Für die Nutzung der internen TK-Anlage und des Zeiterfassungssystems waren bis zum Zeitpunkt der Kontrolle noch keine Dienstvereinbarungen mit dem Personalrat abgeschlossen worden. In meinem Kontrollbericht wies ich darauf hin, daß bei der automatisierten Verarbeitung von Mitarbeiterdaten gem. § 65 PersVG[57] der Personalrat - durch Abschluß von entsprechenden Dienstvereinbarungen - zu beteiligen ist.

Der Systemverwalter der Feuerwehrschule ist gleichzeitig der behördliche Datenschutzbeauftragte. Der daraus zwangsläufig resultierende Interessenkonflikt kann nur durch konsequente Trennung der beiden Funktionen gelöst werden. Im Kontrollbericht forderte ich die strikte Trennung dieser beiden Funktionen.

In der Feuerwehrschule Brandenburg werden zwei unabhängig voneinander arbeitende lokale Netzwerke betrieben (Verwaltungs- sowie Schulungsbereich). Beide Netzwerke können bei Bedarf miteinander verbunden werden. Auf das lokale Netzwerk im Schulungsbereich wird an dieser Stelle nicht weiter eingegangen, da in diesem keine personenbezogenen Daten verarbeitet werden. Das lokale Netzwerk im Verwaltungsbereich besteht aus einem NetWare-Server und diversen Arbeitsstationen. Derzeit erfolgt eine Umrüstung der PC's dahingehend, daß Diskettenlaufwerke ausgebaut werden und der Systemstart über das Netzwerk ermöglicht wird (Einsatz von Boot-Proms auf der Netzwerkkarte). Die Realisierung dieser Maßnahme begrüße ich sehr, da dadurch das gesamte Sicherheitsniveau des Netzwerkes erhöht wird. Die Datensicherung wird regelmäßig durchgeführt.

An der Arbeitsstation des Schulleiters ist ein Modem zur Datenfernübertragung angeschlossen. Dieses Modem wird nur während der Wartungszeit aktiviert. Der Systemverwalter ist in der Lage, die Fernwartung am Bildschirm mit zu verfolgen und jederzeit zu unterbrechen. Die Verbindung wird - nach telefonischer Absprache mit der Wartungsfirma - grundsätzlich von der Feuerwehrschule aufgebaut. Die Wartung erfolgt ca. einmal monatlich für 1-2 Stunden. Als Remote-Control-Programm wird Carbon Copy eingesetzt. Fernwartungsaktivitäten werden nicht protokolliert. Ein Wartungsvertrag ist derzeit nicht vorhanden. Dies habe ich in meinem Prüfbericht an die Landesfeuerwehrschule angemahnt und zusätzliche Maßnahmen zur Sicherung des Serverraumes gefordert.

---

[56] s. 4. Tätigkeitbericht unter 3.4.2.1

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

4 Justiz/Staatsanwaltschaft

4.1 Gesetze

Ein Schwerpunkt der Gesetzgebungstätigkeit des Bundes - im Bereich Justiz - betrifft derzeit das Verfahrensrecht im weitesten Sinn. Dazu gehören die Bereiche Untersuchungs- und Strafvollzug sowie Strafprozeßordnung. Damit sollen erst jetzt - 13 Jahre nachdem das Bundesverfassungsgericht dem Recht auf informationelle Selbstbestimmung den Rang eines Grundrechts zuerkannt hat - die damit einhergehenden Anforderungen an die verfassungskonforme Grundrechtswahrung im Verfahrensrecht umgesetzt werden.

4.1.1 Untersuchungshaftvollzugsgesetz

Wenn man von der sehr knappen gesetzlichen Vorgabe in der Strafprozeßordnung (§ 119 StPO)[58] absieht, war der Untersuchungshaftvollzug bisher im wesentlichen durch zahlreiche untergesetzliche Vorschriften geregelt. Der jetzt vorgelegte Entwurf für ein Untersuchungshaftvollzugsgesetz (UVollzG) schafft nunmehr eine einheitliche gesetzliche Grundlage.

Gesetzestechnisch wird dabei so verfahren, daß die den Datenschutz ausdrücklich betreffenden Paragraphen des (geänderten) Strafvollzugsgesetzes (StVollzÄndG) auch für den Untersuchungshaftvollzug gelten sollen. Diese Regelungen werden durch bestimmte Vorgaben in § 36 UVollzG in geringem Umfang an die Tatsache angepaßt, daß Untersuchungshäftlinge ja gerade nicht eine Strafe verbüßen, sondern daß sie z. B. wegen Fluchtgefahr festgehalten werden. Der weitgehend unterschiedliche Zweck der beiden Haft-Verfahren muß dabei auch den Umfang und die Reichweite des Datenschutzes mit berücksichtigen. Ich habe deshalb in meiner Stellungnahme gegenüber dem Justizministerium (MdJBE) vor allem darauf hingewiesen, daß durch eine eigenständige Regelung des Bereichs "Umgang mit personenbezogenen Daten im UVollzG" dem Datenschutz besser gerecht würde als durch die vorgeschlagene Form der Verweisung auf die einschlägigen Vorschriften im Strafvollzugsgesetz.

Einen gewissen Schwerpunkt nimmt - neben Vorschlägen zur Ausgestaltung des allgemeinen Datenschutzes - die Frage des Telefonverkehrs der Untersuchungshäftlinge ein. Hier geht es darum, wie einerseits dem Bedürfnis des Inhaftierten nach ungestörten Außenkontakten und andererseits den Aufgaben der Bediensteten der Haftanstalt, Störungen im Vollzug und dem Vorschubleisten zu weiteren Straftaten entgegenzuwirken, entsprochen werden kann. Durch eine Eingabe war ich konkret mit dieser Problematik befaßt (s. hierzu unter 4.3).

Bislang nicht aufgegriffen wurde weder im Untersuchungshaftvollzugsgesetz noch im Strafvollzugsänderungsgesetz die Frage der (Gefangenen-)Personalakten.

Leider auch nicht bedacht wurden meine Hinweise auf die außerordentlich langen Aufbewahrungsfristen für Krankenakten, die während des Untersuchungshaftvollzugs angelegt werden; sie werden um ein mehrfaches länger als entsprechende Unterlagen der Krankenkassen aufbewahrt, ohne daß dafür ein gewichtiger Grund erkennbar wäre.

Schließlich habe ich auch in diesem Zusammenhang auf den Täter-Opfer-Ausgleich hingewiesen (vgl. hierzu unter 4.2).

---

[58] i. d. Fass. vom 7. April 1987, BGBl. I S. 1074, ber. S. 1319

Gleichwohl habe ich die Tatsache, daß der Untersuchungshaftvollzug nun erstmalig durch ein umfassendes Gesetz gestaltet werden soll, ausdrücklich begrüßt.

4.1.2 Neuer Entwurf zur Änderung der Strafprozeßordnung

Ende letzten Jahres hat die Bundesregierung einen Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts - Strafverfahrensänderungsgesetz 1996 (StVÄG 1996)[59] - vorgelegt, der einen StVÄG-Entwurf der Länder[60] ablöst. Der Entwurf setzt die sich aus dem Volkszählungsurteil ergebenden Anforderungen an normenklare Regelungen der Eingriffsbefugnisse für die Strafverfolgungsbehörden nur unzulänglich um. In meiner Stellungnahme an das MdJBE habe ich u. a. folgende Regelungen kritisiert und dazu Änderungen vorgeschlagen:

- Öffentlichkeitsfahndung

In den §§ 131 bis 131 c des StVÄG-Entwurfs wird der Unterschied zwischen Ausschreibung zur Festnahme bzw. Aufenthaltsermittlung und eigentlicher Öffentlichkeitsfahndung nicht ausreichend klargestellt, so daß sowohl Ausschreibungen in den Fahndungshilfsmitteln der Strafverfolgungsbehörde als auch Fahndungsausschreiben in den Medien - also die Öffentlichkeitsfahndung im engeren Sinn - nach demselben Verfahren angeordnet werden. Die Ausschreibung in den Medien ist jedoch ein wesentlich schwererer Eingriff in das Persönlichkeitsrecht des Betroffenen, der dadurch nicht ausreichend berücksichtigt wird. Ich habe vorgeschlagen, die Befugnis zur eigentlichen Öffentlichkeitsfahndung auf den Richter bzw. die Staatsanwaltschaft zu beschränken, und nicht - wie vorgesehen - auch auf die Polizei als Hilfsbeamten der Staatsanwaltschaft zu erstrecken.

In den Vorschriften wird nicht ausreichend zwischen Beschuldigten und Zeugen differenziert. Die Fahndung nach Zeugen mittels der Medien ist nicht an besondere Voraussetzungen geknüpft. Zwar ist in einem Aufruf an die Öffentlichkeit die Zeugeneigenschaft des Betroffenen deutlich zu machen, er darf jedoch im Zusammenhang mit jeder Straftat erfolgen. Ich halte es aus Gründen der Verhältnismäßigkeit für unerläßlich, daß der mit der Veröffentlichung seines Bildes verbundene schwere Eingriff in die Persönlichkeitsrechte eines Zeugen mindestens an die Voraussetzung einer Straftat von erheblicher Bedeutung geknüpft wird.

- Auskunfts- und Akteneinsichtsmöglichkeiten für Privatpersonen und sonstige Stellen

§ 475 des Entwurfs stellt die Aktenauskunft aus Justizakten auf die Darlegung eines berechtigten Interesses der auskunftsbegehrenden Privatpersonen bzw. der sonstigen Stellen ab. Ich halte dies für zu weitgehend und habe daher gefordert, daß für die Aktenauskunft bzw. -einsicht ein rechtliches Interesse vorliegen muß.

- Wissenschaftliche Forschung

In § 476 ist dem Recht auf informationelle Selbstbestimmung der Betroffenen bei wissenschaftlichen Forschungsvorhaben im Bereich der Strafverfolgung nicht ausreichend Rechnung getragen. Ich habe daher gefordert, zunächst auf die Einwilligung der Betroffenen für die Übermittlung und Nutzung der Daten abzustellen, wie es sowohl im Bundes- als auch

---

59 vom 20. Dezember 1996, BR-Drs. 961/96

60 vom 14. Oktober 1994, BR-Drs. 620/94

im Brandenburgischen Datenschutzgesetz (s. § 28 BbgDSG) vorgesehen ist.

- Nutzung personenbezogener Informationen aus Strafverfahren durch die Polizei

§ 481 des Entwurfs läßt eine Nutzung von Daten aus Strafverfahren zur Gefahrenabwehr zu, bei der nicht zwischen den verschiedenen Datenerhebungsmaßnahmen und den damit verbundenen Eingriffsschwellen unterschieden wird. Damit wird der Zweckbindungsgrundsatz völlig außer Kraft gesetzt, den jedoch das Bundesverfassungsgericht im Volkszählungsurteil besonders hervorgehoben hat[61], und so die Grenzen zwischen polizeilicher Prävention und Strafverfolgung verwischt. Ich habe vorgeschlagen, daß die Polizeibehörden Daten aus Strafverfahren nur zur Abwehr einer erheblichen Gefahr oder zur Verhütung einer Straftat von erheblicher Bedeutung nutzen dürfen.

- Rückmeldung des Verfahrensausgangs

Die in § 482 des Entwurfs vorgesehene Rückmeldung des Verfahrensausgangs an die Polizei ist grundsätzlich zu begrüßen. Sie ist jedoch zu weit gefaßt. Zur Verwaltungsvereinfachung soll es zulässig sein, den Polizeibehörden einen Durchschlag der Mitteilung zum Bundeszentralregister (BZRG) zu übersenden. Damit erhält die Polizei jedoch Daten, wie z. B. die Nebenfolgen (Verlust und Aberkennung der Amtsfähigkeit, der Wählbarkeit und des Stimmrechts), die für ihre Aufgabenerfüllung nicht erforderlich sind. Hier ist durch Verfahrensvorkehrungen sicherzustellen, daß den Polizeibehörden tatsächlich nur der Verfahrensausgang übermittelt wird.

- Dateien

Die Regelungen in den §§ 483 bis 490 des Entwurfs stoßen wegen ihrer mangelnden Normenklarheit auf erhebliche datenschutzrechtliche Bedenken. In der vorliegenden Fassung legen sie weder das Datenprofil (§ 484 StPO-Entwurf) fest, noch enthalten sie abschließende Speicherungs- und Zugriffsbefugnisse (§§ 483, 484 StPO-Entwurf). Es fehlt an klaren Bestimmungen über die speichernden Stellen, die die Errichtung einer Datei an die konkrete Aufgabenerfüllung der datenverarbeitenden Stelle knüpfen. Dies gilt auch für die Errichtung gemeinsamer Dateien. Durch die Verknüpfung der Regelungen zur Vorgangsverwaltung (§ 485 StPO-Entwurf) mit den Regelungen zur Löschung (§ 490 StPO-Entwurf) wird das zeitlich nicht befristete Vorrätighalten von hochsensiblen Datensammlungen ermöglicht, auf die alle Behörden zugreifen dürfen, die in irgendeiner Weise mit dem Strafverfahren zu tun haben. Dies erweckt Zweifel an der Verfassungsmäßigkeit des Entwurfs. Die Regelungen sollten deshalb grundlegend überarbeitet werden. Dabei sollten Inhalt und Umfang staatsanwaltschaftlicher personenbezogener Dateien auf Länderebene klar abgegrenzt werden gegenüber dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV), das zur Zeit beim Bundeszentralregister in Berlin eingerichtet wird. Des weiteren sind Zugriffsmöglichkeiten für die Strafverfolgungsbehörden und die Strafjustizbehörden festzulegen, die sich an der jeweiligen Aufgabenerfüllung orientieren. Dringend erforderlich sind auch Regelungen, die den im Datenschutzrecht unterdessen erreichten Standard, wie z. B. Protokollierung der Zugriffe, Verschlüsselung bei Datenübertragung, interne Zugriffsregelungen, festschreiben.

In einem vor den Beratungen im Bundesrat stattgefundenen Gespräch stimmte das MdJBE meinen datenschutzrechtlichen Bedenken gegen mehrere Regelungen zu. In einigen Einzelfragen wollte das Ministerium meine Vorschläge aufgreifen und in die Beratungssitzungen einbringen. Unterdessen hat der Entwurf jedoch den Bundesrat passiert, ohne daß die gravierenden datenschutzrechtlichen Mängel beseitigt worden wären. Im Gegenteil: Der Bundesrat hat in seiner

[61] BVerfGE 65,1, 46

Stellungnahme wesentliche datenschutzrechtliche Verschlechterungen beschlossen. Eine Reihe von Verfahrensvorkehrungen zum Schutz der Persönlichkeitsrechte, wie z. B. Richtervorbehalte und die Beschränkung von Nutzungsbefugnissen für Daten, die mit den besonderen Erhebungsmethoden nach dem Polizeirecht erlangt worden sind, fallen nunmehr weg. Letzteres ist in Brandenburg aufgrund des Polizeirechts, das in diesem Punkte enger als der Strafprozeßordnungsentwurf gefaßt ist, nicht so gravierend.

Wenn das Gesetz in der vorliegenden Fassung verabschiedet wird, befürchte ich - ebenso wie meine Kollegen in Bund und Ländern - unverhältnismäßige Eingriffe in die Persönlichkeitsrechte der Bürger und Bürgerinnen unabhängig davon, ob sie im Zusammenhang mit einem Strafverfahren als Verdächtige, Beschuldigte, Tatopfer, Tatzeugen oder gänzlich Unbeteiligte auftreten[62].

4.2 Beteiligung privater Stellen beim Täter-Opfer-Ausgleich

Mit dem Täter-Opfer-Ausgleich hat sich meine Behörde im Berichtsjahr mehrfach befaßt. Der Anstoß ist hierzu vom MdJBE ausgegangen.

Der Täter-Opfer-Ausgleich (TOA) wird in Brandenburg sehr viel häufiger durchgeführt als in anderen - vor allem als in den alten - Bundesländern. In Brandenburg hat sich wohl auch deshalb besonders deutlich gezeigt, daß diese Aufgabe der Bearbeitung und Bewältigung der Folgen von Straftaten nicht allein durch die sozialen Dienste der Justiz bewältigt werden kann. Private Einrichtungen konnten für die Übernahme dieser Aufgabe verpflichtet werden.
Die gesetzliche Ausgestaltung des Datenschutzes in der Strafprozeßordnung (StPO) umfaßt die Einbeziehung privater Stellen in den TOA jedoch nicht. Da der Datenschutz im öffentlichen Bereich einerseits und im nicht-öffentlichen Bereich andererseits in Deutschland unterschiedlich ausgestaltet ist, kann der Kontakt zwischen einem privaten Träger und den betroffenen Personen wegen des Fehlens einer gesetzlichen Regelung der Materie im privaten Bereich nur bei vorheriger Einwilligung der Betroffenen hergestellt werden.

Es hat sich aber leider gezeigt, daß die bürokratisch wirkende Kontaktaufnahme vor allem zu den jugendlichen Tätern, zunächst mit dem alleinigen Ziel, die Zustimmung zu einem später durchzuführenden TOA zu erreichen, oft nicht erfolgreich ist. Vielen Betroffenen ist in der Lebenssituation, in der sich sowohl Täter wie Opfer befinden, das - nur - aus Gründen des Datenschutzes erforderliche Verfahren der Vorweg-Befragung nicht leicht verständlich zu machen.

Eine gesetzliche Regelung böte sich als Alternative an. Die Tatsache, daß die Strafprozeßordnung zur Zeit durch das Strafverfahrensänderungsgesetz (StVÄG) besonders auch im Bereich des Datenschutzes ausgestaltet wird, hat mich veranlaßt, auf das Erfordernis einer diesbezüglichen gesetzlichen Regelung aufmerksam zu machen. Ich kann nur hoffen, daß die Landesregierung, die sich intensiv und erfolgreich mit der Ausweitung des TOA befaßt, diese Anregung aufgreift und sie gegenüber der Bundesregierung und im Bundesrat aktiv vertritt. Die sonst verbleibende Möglichkeit, den Datenschutz im Bereich des TOA bei Beteiligung privater Träger durch Landesgesetz zu regeln, ist wesentlich weniger wünschenswert, schon deshalb, weil die Kompetenz zur Gesetzgebung in diesem Bereich beim Bund liegt und die Gesetzgebungskompetenz des Landes als Ergänzung bei Nichttätigwerden des Bundes insoweit erst nachgewiesen werden müßte.

---

62 s. Anlage 13

4.3 Eingaben/Anfragen aus Justizvollzugsanstalten

Auch der Straf- bzw. Untersuchungshäftling ist Grundrechteinhaber, die zu schützen sind, gerade weil sie durch die Haftbedingungen eingeschränkt sind.

Im Berichtszeitraum haben mich aus diesem Bereich auffällig viele Eingaben erreicht, von denen ich nachstehend anhand von zwei Beispielen mit Schwerpunkt Post- und Telefonkontrolle berichte:

- Postkontrolle von Schreiben, die dem Amtsgeheimnis unterliegen

Ein Häftling fragte nach, ob es zulässig sei, daß jeglicher Schriftverkehr, darunter auch an Gerichte, Rechtsanwälte, Polizei, Banken und Versicherungen gelesen werde. Der Häftling sah hier den Datenschutz verletzt. Mit dem Hinweis auf die Regelung im Strafvollzugsgesetz (in der Vollzugsgeschäftsordnung) konnte ich dem Petenten allerdings nur bestätigen, daß im Verlaufe einer angeordneten Überwachung der gesamte Schriftverkehr von den mit der Überwachung betrauten Bediensteten gelesen werden darf.

Das MdJBE schrieb mir auf meine Nachfrage hin außerdem, daß der Schriftwechsel neu aufgenommener junger Gefangener in den ersten drei Haftmonaten ohne Ausnahme überwacht werde. Die Gefängnisleitung nutzt diese Kontrollmöglichkeit, um z. B. zu verhindern, daß Kontakte zu dem Umfeld aufrechterhalten werden, aus dem heraus die Straftat entstanden war. In diese totale Überwachung ist ebenso der Schriftverkehr mit anderen Behörden, Rechtsanwälten, Banken, Versicherungen u. ä. einbezogen.

Nach Ablauf der Dreimonatsfrist wird geprüft, ob die Überwachung des weiteren Schriftwechsels aufzuheben oder weiterzuführen ist; in der Regel wird sie aufgehoben. Sobald die Überwachung entfällt, werden die Sendungen nicht mehr gelesen, sondern sie werden nur noch einer Sichtkontrolle unterzogen, durch die der Abteilungsbedienstete feststellt, daß außer dem Schreiben keine anderen Gegenstände auf den Postweg gegeben werden.

Im Zusammenhang mit vorgesehenen Prüfungen in Justizvollzugsanstalten bedarf das Verfahren der Postkontrolle einer weiteren Erörterung im Detail.

- "Nennung der Telefonnummer"

Eine der Eingaben betraf das Telefonieren aus der Haftanstalt heraus. In der Haftanstalt, aus der diese Eingabe kam, wird ein "Telefonbuch" geführt, in das alle herausgehenden Telefonate eingetragen werden. Außerdem muß das Telefonat angemeldet werden. Zu Abrechnungszwecken werden alle angegebenen Daten außerdem in eine extra dafür vorgesehene Datei gespeichert. Der Häftling, der in diesem Fall sein Persönlichkeitsrecht beeinträchtigt sah, wollte seine Angehörigen telefonisch erreichen. Er weigerte sich, Angaben über die angerufene Person einzutragen, weil diese Person zu ihrem Schutz eine Geheimnummer besitze.

Meine Nachfrage bei dem MdJBE stieß auf Verständnis. Gemeinsam mit meiner Behörde wurden Überlegungen angestellt, wie man dem Kontrollbedürfnis der Anstalt einerseits und dem Geheimhaltungswunsch des Gefangenen und seines Gesprächspartners andererseits einigermaßen entsprechen könnte. Die Voranmeldung muß zwar nach Meinung des MdJBE gefordert werden, aber es besteht offensichtlich kein Erfordernis, die Daten dann zusätzlich in ein Telefonbuch einzutragen. Ich erwarte, daß in Zukunft auch die Aufbewahrung dieser Unterlagen anders geregelt und die Möglichkeiten,

die eingetragenen Daten einzusehen, deutlich reduziert werden.

Daneben erhielt ich eine Eingabe mit der Forderung, mein Antwortschreiben "deutlich mit Parlamentspost zu bezeichnen", nur dann sei sichergestellt, daß das Antwortschreiben den Gefangenen erreiche und ihm die Unterlagen ausgehändigt würden.

Zwar ist der Landesbeauftragte für den Datenschutz beim Präsidenten des Brandenburgischen Landtages eingerichtet, dennoch kann mein Schriftwechsel nicht als "Parlamentspost" deklariert werden. Die Datenschutzbeauftragten unterfallen nicht den Vorschriften des § 29 Abs. 2 StVollzG. Die Post zwischen Häftlingen und meiner Dienststelle wird dennoch in Brandenburg genauso behandelt, als sei der Datenschutzbeauftragte in dieser Vorschrift mitgenannt, und die Post wird daher nicht kontrolliert.

Außerdem kam aus einer Haftanstalt die Bitte, einige Fragen für die Gefangenenzeitung zu beantworten. Dieser Bitte bin ich gern nachgekommen. Die Fragen konnten durch die Zusendung des 2. Tätigkeitsberichtes meiner Behörde beantwortet werden, der eine Zusammenfassung über die Prüfungen meiner Behörde in Justizvollzugsanstalten des Landes enthält.

4.4 Staatsanwaltschaften

4.4.1 Prüfung der Telefonüberwachungsmaßnahmen gem. § 100 a StPO

Im Berichtszeitraum wurden die in den Jahren 1992 bis 1994 durchgeführten Überwachungsmaßnahmen (TÜ-Maßnahmen) abgeschlossener Ermittlungsverfahren in den vier bei den Landgerichtsbezirken eingerichteten Staatsanwaltschaften (StA) geprüft (vgl. unter 3.3.2).

4.4.1.1 Feststellungen

Ziel der datenschutzrechtlichen Kontrolle war es, festzustellen, inwieweit die zur Wahrung des Grundrechts auf Brief-, Post- und Fernemeldegeheimnis (Art. 10 Grundgesetz) in den §§ 100 a und 100 b sowie 101 StPO getroffenen Vorkehrungen von Staatsanwaltschaft und Polizei eingehalten worden sind.

Die folgenden Verfahrensregelungen sollen gewährleisten, daß die Betroffenen keinen über das unbedingt erforderliche Maß hinausgehenden Grundrechtseingriff hinnehmen müssen:

- Richterliche Anordnung (§ 100 b StPO)

Die ermittelnde Staatsanwaltschaft beantragt schriftlich beim zuständigen Amtsgericht die Anordnung einer TÜ-Maßnahme. Der Antrag muß begründet sein und Name, Anschrift des Betroffenen, genaue Bezeichnung der zu überwachenden Fernmeldeanschlüsse sowie die zur Durchführung der TÜ-Maßnahme erforderlichen Angaben wie Art, Umfang und Dauer enthalten. Erst wenn ein Gericht die Überwachung schriftlich mit den o. g. Angaben angeordnet hat, darf abgehört werden. Die Höchstfrist für eine Abhörmaßnahme ist drei Monate, Verlängerungen durch jeweils weitere gerichtliche Anordnungen sind zulässig.

Die geprüften Unterlagen entsprachen in diesem Punkt im allgemeinen den gesetzlichen Vorschriften.

- Beendigung (§ 100 b Abs. 4 StPO)

TÜ-Maßnahmen sind unverzüglich zu beenden, wenn die der Anordnung zugrunde liegenden Voraussetzungen nicht mehr vorliegen. Diese Vorschrift war in allen geprüften Fällen befolgt worden.

- Nutzung und Vernichtung von TÜ-Unterlagen (§ 100 b Abs. 5 und 6 StPO)

Die durch die TÜ-Maßnahmen erlangten Unterlagen sind unverzüglich zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich sind. Als zu vernichtende Unterlagen kommen neben den Niederschriften in Form von wörtlichen Wiedergaben bzw. inhaltlichen Zusammenfassungen von Telefongesprächen auch die Berichte der Polizei in Betracht, soweit sie wörtliche Zitate aus abgehörten Telefongesprächen oder inhaltliche Wiedergabe von Sachverhalten enthalten, die bei der TÜ-Maßnahme bekannt wurden. Unter das Vernichtungsgebot fällt auch beweiserhebliches Material, wenn es durch andere Beweismittel bestätigt worden ist. Vor der Vernichtung muß geprüft werden, ob in den Unterlagen lediglich Erkenntnisse über Katalogstraftaten (Straftaten, bei denen gem. § 100 a StPO Telefonüberwachungsmaßnahmen angeordnet werden dürfen) vorliegen oder ob sie auch Erkenntnisse über andere - also Nicht-Katalogstraftaten - enthalten. Während Erkenntnisse über Katalogstraftaten auch in anderen Verfahren ohne Einschränkungen genutzt werden dürfen, unterliegen letztere einem Beweisverwertungsverbot. Sie dürfen lediglich als Grundlage für weitere Ermittlungen genutzt werden. Analoges gilt auch für die Nutzung in einem anderen Strafverfahren. Soweit die in einer TÜ-Maßnahme angefallenen Erkenntnisse Katalogstraftaten betreffen, unterliegen sie keinem Verwertungsverbot und dürfen in einem Ermittlungsverfahren gegen andere als die von der richterlichen Anordnung der TÜ-Maßnahme Betroffenen genutzt werden. Andere als Katalogstraftaten dürfen jedoch nur als Ermittlungsgrundlage herangezogen werden.

Die Prüfungen ergaben, daß - von wenigen Ausnahmen abgesehen - das gesetzliche Gebot der unverzüglichen Vernichtung von Unterlagen der oben beschriebenen Art nicht beachtet wurde.

In einem geprüften Ermittlungsverfahren waren die Erkenntnisse über eine Nicht-Katalogstraftat in Form einer wörtlichen Niederschrift, die auch die personenbezogenen Daten des von der TÜ-Maßnahme Betroffenen enthielt, zusammen mit einer Anzeige gegen Unbekannt an das Landeskriminalamt (LKA) eines anderen Bundeslandes gesandt worden. Hier wäre es lediglich zulässig gewesen, eine Sachverhaltsschilderung mit dem Aktenzeichen des ursprünglichen Ermittlungsverfahrens zu übermitteln.

- Auswertung und Vernichtung der Beweis- bzw. Arbeitsbänder (§ 100 b Abs. 5 und 6 StPO)

Abgehörte Telefongespräche werden auf zwei Bändern aufgezeichnet, dem sog. Beweis- und dem Arbeitsband. Während die Arbeitsbänder von den ermittelnden Polizeibeamten abgehört und ausgewertet werden, dienen die Beweisbänder als unmittelbares Beweismittel in der gerichtlichen Hauptverhandlung und werden bis dahin versiegelt und unberührt aufbewahrt. Grundsätzlich gilt für die Vernichtung der Bänder das bereits oben zur Vernichtung der anderen Unterlagen gesagte.

Im Gegensatz zu den schriftlichen Unterlagen sind jedoch die Beweis- bzw. Arbeitsbänder in allen geprüften Fällen nach Verfahrenseinstellung bzw. nach dem rechtskräftigen Abschluß des Gerichtsverfahrens vernichtet worden. Von wenigen Ausnahmen abgesehen war jedoch das Gebot der unverzüglichen Vernichtung nicht erfüllt. Teilweise lag zwischen Verfahrensabschluß und Vernichtung ein Zeitraum von mehreren Monaten.

- Protokollierung der Vernichtung (§ 100 b Abs. 6 StPO)

Die Vernichtung der Beweis- bzw. Arbeitsbänder und der übrigen Unterlagen muß in Gegenwart eines Staatsanwalts erfolgen. Über die Vernichtung ist ein Protokoll anzufertigen, das der Staatsanwalt und derjenige, der die Vernichtung durchführt, unterschreiben.

Die Protokolle waren häufig mangelhaft. So ließ sich in einigen Fällen nicht feststellen, wann die Vernichtung erfolgt war bzw. ob ein Staatsanwalt teilgenommen hatte.

Aus dem von der StA verwendeten Protokollformular ist nicht zu ersehen, welche Datenträger (Bänder bzw. Papierunterlagen) in welchem Umfang und auf welche Weise vernichtet worden sind.

- Mitteilung an die Betroffenen (§ 101 StPO)

Die Betroffenen sind von der Staatsanwaltschaft zu informieren, daß ihr Telefon abgehört worden ist. Eine Benachrichtigung über eine Abhörmaßnahme kann nur unterbleiben, solange durch ihr Bekanntwerden eine andere Person oder die öffentliche Sicherheit gefährdet würde. Im allgemeinen ist davon auszugehen, daß die Mitteilung über eine TÜ-Maßnahme während der Gerichtsverhandlung erfolgt. Anders verhält es sich jedoch, wenn das Verfahren durch die Staatsanwaltschaft eingestellt wird. In solchen Fällen bedarf es einer ausdrücklichen schriftlichen Benachrichtigung.

In einigen Fällen waren die Betroffenen bis zum Zeitpunkt der Prüfung noch nicht von der gegen sie durchgeführten Abhörmaßnahme unterrichtet worden, obwohl eine Gefährdung des Untersuchungszweckes oder anderer Personen nicht mehr bestand.

4.4.1.2 Konsequenzen aus den Prüfungen

Unterdessen haben die Staatsanwaltschaften die oben aufgelisteten Mängel in den geprüften Ermittlungsverfahren beseitigt.

Die Nichtbeachtung des unverzüglichen Vernichtungsverbots wird durch die Aktenführung begünstigt. Unsere Anregung, alle TÜ-Unterlagen in einer Sonderakte abzulegen, ist mit der Änderung der Brandenburgischen Aktenordnung[63] verfügt worden. Auch die geprüften Staatsanwaltschaften haben interne Verfügungen zu den Verfahrensabläufen bei der Durchführung von TÜ-Maßnahmen einschließlich der Vernichtung der dabei angefallenen Unterlagen erlassen, die - neben der oben erwähnten Ablage in Sonderbänden - eine stärkere Beachtung datenschutzrechtlicher Belange vorschreiben.

Daß es jedoch mit einer anderen Aktenführung allein noch nicht getan ist, zeigte sich bei einer Staatsanwaltschaft. Hier war das Gebot der unverzüglichen Vernichtung auch nicht befolgt worden, obwohl die TÜ-Unterlagen in Sonderbänden abgelegt waren.

Daher bedarf es meiner Meinung nach - ungeachtet der bereits getroffenen Vorkehrungen zum Schutz der Persönlichkeitsrechte der Betroffenen - einer verbindlichen landeseinheitlichen Regelung der Verfahrensschritte für die

63 vom 11. November 1996, JMBl. S. 164

Staatsanwaltschaften und die mit der Durchführung und Auswertung von TÜ-Maßnahmen betraute Polizei. Sie sollte u. a. folgende Einzelaspekte umfassen.

- Ermittlungsberichte der Polizei

Zahlreiche Erkenntnisse aus der TÜ-Maßnahme fließen in Form von Zusammenfassungen oder wörtlichen Zitaten in die Zwischen- bzw. Abschlußberichte der ermittelnden Polizeibeamten ein, die immer dann, wenn sie nicht mehr erforderlich sind, von den nicht zur Vernichtung vorgesehenen Berichtsteilen getrennt und - ebenso wie die Beweis- bzw. Arbeitsbänder - vernichtet werden müssen. Bei den geprüften Ermittlungsakten war dies in der Regel - wohl wegen des hohen Verwaltungsaufwandes - unterblieben. Um den Arbeitsaufwand zu reduzieren, sehen die oben erwähnten internen Verfügungen der Staatsanwaltschaften nicht nur vor, sämtliche TÜ-Unterlagen in Sonderbänden abzulegen, sondern auch die Polizei anzuhalten, die TÜ-Erkenntnisse in gesonderten Berichten zusammenzufassen und in den Zwischen- bzw. Abschlußberichten lediglich auf die dortigen Erkenntnisse zu verweisen. Dieses Verfahren sollte in die Regelung aufgenommen werden.

- Umgang mit Gesprächen mit erkennbar Unbeteiligten, Verteidigern u. ä.

Ich vertrete die Auffassung, daß darüber weder wörtliche noch inhaltliche Niederschriften angefertigt werden dürfen. Die Regelung sollte festlegen, daß lediglich die Fundstellenangaben solcher Gespräche vermerkt werden.

- Nutzung der TÜ-Erkenntnisse

Es bedarf zum einen einer Regelung, wie mit denjenigen Erkenntnissen aus TÜ-Maßnahmen zu verfahren ist, die sich zwar nicht auf Katalogstraftaten beziehen, sehr wohl aber Hinweise auf andere Straftatbestände enthalten. Solche Erkenntnisse dürfen in anderen Strafverfahren nur mittelbar verwertet und als Grundlage für weitere Ermittlungen genutzt werden. Um sicherzustellen, daß das Vernichtungsverbot nicht durch die Erstellung von Kopien umgangen wird, rege ich an, daß sie nur in Form von Vermerken mit Aktenzeichen, jedoch ohne Personenangaben des Betroffenen, zu den Ermittlungsakten des anderen Strafverfahrens genommen werden dürfen.

Im Zusammenhang mit der Verwertung von TÜ-Erkenntnissen ist es unbedingt erforderlich, ein Verfahren für ihre Nutzung zur Gefahrenabwehr verbindlich zu regeln. Da auch in solchen Fällen die Verantwortung bei der Staatsanwaltschaft liegt, kann jede weitere - über die Strafverfolgung hinausgehende - Verwertung von Erkenntnissen nur mit ihrer Zustimmung erfolgen.

- Vernichtung der Unterlagen und Protokollierung

Die gegenwärtige Praxis, daß TÜ-Unterlagen und -Bänder nur im LKA vernichtet werden können, sollte geändert werden. Ich gehe davon aus, daß das dem Grundrechtsschutz dienende unverzügliche Vernichtungsgebot stärker beachtet würde, wenn es nicht mit dem Zeitaufwand einer Dienstfahrt zum LKA in Basdorf verbunden wäre, sondern die Vernichtung im örtlich ansässigen Polizeipräsidium erfolgen könnte.

In die Regelung sollte ein neugestaltetes Protokollierungsformular aufgenommen werden, das neben den jetzt schon erforderlichen Angaben eine Beschreibung der zu vernichtenden Datenträger einschl. der schriftlichen Unterlagen (Überwachungszeitraum und Aktenfundstelle) sowie der Vernichtungstechnik enthält.

4.4.1.3 Abhören aufgrund eines technischen Fehlers

Der Vorgang wurde meiner Behörde durch die Eingabe eines Bürgers bekannt. Dem Betroffenen war von der Staatsanwaltschaft mitgeteilt worden, daß sein Telefon aufgrund eines technischen Fehlers versehentlich abgehört worden war. Bei einer der routinemäßig täglichen Überprüfungen der laufenden Telefonüberwachungen war der mit der Maßnahme betrauten Polizeidienststelle aufgefallen, daß der falsche Anschluß abgehört wurde. Die Abhörmaßnahme wurde sofort gestoppt, die Bänder ohne Abhören oder Auswertung versiegelt und die Telekom benachrichtigt. Bei der Überprüfung stellte die Telekom fest, daß der Anschluß des Petenten aufgrund eines durch die Umstellung auf digitale Vermittlung verursachten technischen Versehens geschaltet worden war. Vier Monate später wurden die Bänder, ohne daß sie zwischenzeitlich genutzt worden waren, vernichtet und darüber ein Protokoll erstellt.

Die Prüfung ergab keine Anhaltspunkte für einen anderen als den oben dargestellten Sachverhalt. Der Petent beschwerte sich zu Recht darüber, daß die während des Abhörvorgangs angefallenen Arbeits- bzw. Beweisbänder erst nach so langer Zeit vernichtet worden waren. Gründe für die lange Aufbewahrung konnte die StA nicht angeben.

4.4.2 Rückmeldeverfahren

Durchgängiges Thema der letzten Tätigkeitsberichte[64] war das von den Staatsanwaltschaften nur sporadisch betriebene Rückmeldeverfahren. Darunter sind die Meldungen der Staatsanwaltschaften an die Polizei über den Ausgang der staatsanwaltschaftlichen Ermittlungen zu verstehen.

Der bei Prüfungen von Kriminalakten immer wieder festzustellende unzureichende Rückfluß von Informationen über den Verfahrensausgang an die Polizei hat in datenschutzrechtlicher Hinsicht gravierende Auswirkungen. Die in § 37 i. V. m. § 39 BbgPolG vorgeschriebene Erforderlichkeitsprüfung führt wegen der Unkenntnis über den Verfahrensstand zu falschen Ergebnissen. Personenbezogene Daten werden nicht gelöscht, obwohl sie zur polizeilichen Aufgabenerfüllung nicht mehr erforderlich sind. Kriminalakten werden weiterhin aufbewahrt, weil die Abwägung, ob sie zur polizeilichen Aufgabenerfüllung erforderlich sind, aus Unkenntnis über den Ausgang des staatsanwaltschaftlichen Verfahrens nicht getroffen werden kann. Da die Polizei nicht über die Verfahrenseinstellung durch die Staatsanwaltschaft informiert worden ist, teilt sie den Betroffenen auch nicht die bereits eingestellten Ermittlungsverfahren als Datenspeicherung zu ihrer Person mit.

Im Verlauf des Berichtsjahres hat sich die Situation verändert. Wie das Justizministerium mitteilte, übersenden die Polizeidienststellen die Ermittlungsvorgänge zusammen mit einem Formular, das den Staatsanwaltschaften die formularmäßige Rückmeldung (Aktenzeichen und Mitteilung über den Verfahrensausgang) ermöglicht. Der Generalstaatsanwalt hat bei den Staatsanwaltschaften darauf gedrungen, daß das Rückmeldeverfahren von allen Staatsanwaltschaften regelmäßig und einheitlich praktiziert wird. Dies wird aus einzelnen Polizeidienststellen bestätigt. Wenn nun in den Polizeipräsidien durch ein geeignetes Postverteilungsverfahren sichergestellt wird, daß die Kriminalaktenhaltung Kenntnis vom Ausgang des staatsanwaltschaftlichen Ermittlungsverfahrens erhält, ist zu hoffen, daß die datenschutzrechtlichen Belange der Betroffenen nunmehr angemessen gewahrt werden können.

---

[64] s. 2. Tätigkeitsbericht unter 3.6.2.2, 3. Tätigkeitsbericht unter 4.1.4, 4. Tätigkeitsbericht unter 4.3

4.5 Forschung

Bitten des Justizministeriums um Stellungnahmen zu genehmigungspflichtigen Forschungsprojekten (§ 28 BbgDSG) gehören inzwischen zur routinemäßigen, vertrauensvollen Zusammenarbeit zwischen dem MdJBE und meiner Behörde. Im Berichtszeitraum handelte es sich dabei überwiegend um länderübergreifende Vorhaben, so daß diesbezügliche Verfahrensfragen auch immer möglichst einvernehmlich mit anderen Landesbeauftragten abzustimmen waren. Im folgenden soll beispielhaft auf zwei Forschungsprojekte eingegangen werden.

4.5.1 Strafjustiz und DDR-Vergangenheit

Bei dem Forschungsprojekt "Strafjustiz und DDR-Vergangenheit" handelt es sich um ein Editionsvorhaben im Rahmen der "Amsterdamer Sammlung", die bisher sämtliche (west-)deutschen Urteile wegen nationalsozialistischer Tötungsverbrechen im Wortlaut enthält. In vergleichbarer Weise soll die Sammlung um strafrechtliche Entscheidungen zum Systemunrecht der DDR ergänzt werden; auch die brandenburgische Justizverwaltung sollte hierfür die vorhandenen Unterlagen zur Verfügung stellen.

Nach Auffassung des MdJBE überwiegt bei der Durchführung des Forschungsvorhabens das öffentliche Interesse die schutzwürdigen Belange der Betroffenen erheblich. Der Zweck der Forschung läßt sich auch nicht auf andere Weise erreichen. Zudem war nicht mit der Einwilligung der Betroffenen zu rechnen, so daß unter diesen Voraussetzungen § 28 Abs. 2 Satz 1 Buchst. c BbgDSG die Rechtsgrundlage für die Datenverarbeitung darstellt. Aber auch unter diesen Bedingungen ist die Zumutbarkeit des Eingriffs in das Recht auf informationelle Selbstbestimmung der Betroffenen abzuwägen. Es sind Maßnahmen festzulegen, die den Eingriff auf das erforderliche Minimum reduzieren. Dazu habe ich folgende Verfahren empfohlen:

- Auswahlkriterien

Die Antragsteller waren von einer Auswertung sämtlich ergangener Urteile, Anklageschriften und wichtigen Verfügungen ausgegangen. Dies hätte dem datenschutzrechtlichen Grundsatz der Erforderlichkeit widersprochen. Insoweit habe ich dem Ministerium nahegelegt, durch die Justizverwaltung eine Auswahl des in Frage kommenden Materials anhand von vorgegebenen Kriterien vornehmen zu lassen. Davon ausgeschlossen werden sollten solche, die keinesfalls für eine Dokumentation in Betracht kommen und die auch keinen Erkenntnisgewinn im Hinblick auf die Forschungsfragen des Projekts versprechen. Bei den Verfügungen sollten auch nur solche in Betracht gezogen werden, die in rechtlicher Hinsicht für eine größere Zahl anderer Verfahren "Anleitungscharakter" gehabt haben bzw. einen zeithistorischen Sachstand festhalten.

- Anonymisierungsverfahren

Für das Anonymisieren der Unterlagen ist ein mehrstufiges Verfahren vorgesehen, dessen Einsatz auch für andere Forschungsprojekte empfehlenswert ist. Zusätzlich zu der gängigen Vorgehensweise (Kopieren, Schwärzen der Namen und anderer unmittelbar auf eine Person zeigende Angaben auf der Kopie, Kopieren der Zwischenkopie sowie deren Vernichtung) sollen die Unterlagen eingescannt und anschließend mittels eines Textverarbeitungssystems auf das noch Vorhandensein personenbezogener Daten überprüft werden. Es erscheint bedenkenswert, ob in vergleichbaren Fällen nicht generell die übliche und zeitaufwendige Anonymisierung von Unterlagen durch dieses Verfahren material- und zeitökonomisch ersetzt werden kann.

Meine Hinweise hat das MdJBE in seinem Genehmigungsbescheid aufgenommen.

4.5.2 Begleitforschung zum Täter-Opfer-Ausgleich

Anliegen des Forschungsvorhabens "Begleitforschung zum Täter-Opfer-Ausgleich" ist es, in einer sozialwissenschaftlich angelegten Analyse sowohl in Sachsen-Anhalt als auch in Brandenburg die unterschiedlichen und teilweise neuen Herangehensweisen der Anwendung des Täter-Opfer-Ausgleichs[65] einer systematischen Auswertung unter Einbeziehung der auf allen Ebenen am Verfahren Beteiligten (Polizei, Staatsanwälte, Konfliktschlichter und Rechtsanwälte sowie Täter und Opfer) zuzuführen. Methodisch sind hierfür Interviews und die Beantwortung von Fragebögen auf freiwilliger Basis vorgesehen. Es bestand zusätzlich der Wunsch an einer "teilnehmenden Beobachtung" am Schlichtungsgespräch und einer Auswertung der Handakten des Schlichters. Die Teilnahme am Schlichtungsgespräch ist datenschutzrechtlich nur unter der Voraussetzung denkbar, daß dazu alle Beteiligten (einschließlich der Eltern bei jugendlichen Tätern) ihre Einwilligung erteilt haben. Ich hatte daher vorgeschlagen, diese Vielschichtigkeit gesprächsweise unter Beteiligung von Vertretern der Ministerien, der Forschungseinrichtung und der Landesbeauftragten für den Datenschutz zu erörtern. Diesem Vorschlag wurde gefolgt und dabei einvernehmlich Verfahren gefunden, die als datenschutzgerecht anzusehen sind.

Für die "teilnehmende Beobachtung" wird vorab über den Schlichter eine Einverständniserklärung eingeholt und gem. § 4 Abs. 2 BbgDSG schriftlich dokumentiert. Sie wird von diesem zunächst zu den Unterlagen genommen und mit der Abgabe des Falls dem Justizministerium übergeben. Die Unterlagen unterliegen damit den Aufbewahrungsfristen der Justizverwaltung. Während der Schlichtung wird lediglich ein Beobachtungsprotokoll geführt; auf diesem wird anstelle des Namens des Schlichters die Einrichtung vermerkt.

Von der direkten Einsicht in die Handakten wird abgesehen. Dies hätte zur Folge gehabt, daß gemäß der Legaldefinition nach § 3 Abs. 2 Ziff. 4 BbgDSG personenbezogene Daten nicht nur von Tätern und Opfern, sondern darüber hinaus Aufzeichnungen subjektiver Eindrücke des Schlichters in Verbindung mit der behandelnden Sache und Daten Dritter übermittelt worden wären. Da hierfür selbst seitens der Forschungseinrichtung keine Erforderlichkeit dargelegt werden konnte, ist vorgesehen, daß der Schlichter selbst die vorgesehenen Fragen für die Handaktenanalyse aus seinen Akten beantwortet. Damit kann sichergestellt werden, daß die Datenerhebung anonym erfolgt.

5 Bildung, Jugend und Sport

5.1 Gesetze und Verordnungen

5.1.1 Anpassung gesetzlicher Vorschriften an das Brandenburgische Schulgesetz

[65] s. hierzu auch unter 4.2

Das Inkrafttreten des Brandenburgischen Schulgesetzes (BbgSchulG)[66] im vergangenen Jahr macht die zügige förmliche und inhaltliche Anpassung der auf der Grundlage des Ersten Schulreformgesetzes (1. SRG)[67] erlassenen Rechtsverordnungen und Verwaltungsvorschriften an die neue Rechtslage erforderlich. Nach Auskunft des Ministeriums für Bildung, Jugend und Sport (MBJS) soll die Überarbeitung dieser Vorschriften rechtzeitig bis zum Schulbeginn 1997/98 abgeschlossen werden. Bisher liegen mir bereits die Entwürfe der Datenschutzverordnung Schulwesen und der überarbeiteten Verwaltungsvorschriften über Akten an Schulen im Land Brandenburg (VV-Schulakten)[68] zur Stellungnahme vor. Die Erste Verordnung zur Änderung der Ausbildungs- und Prüfungsordnung der Fachschulen[69] ist bereits in Kraft getreten.

5.1.1.1 Datenschutzverordnung Schulwesen

Der Erlaß einer Datenschutzverordnung Schulwesen (DSVS) ist aufgrund der Bestimmung des § 65 Abs. 11 BbgSchulG notwendig geworden. Im Entwurf werden die bisherigen datenschutzrechtlichen Regelungen, die sich vorwiegend in den Verwaltungsvorschriften über den Schutz personenbezogener Daten und über statistische Erhebungen (VV-Datenschutz/Statistik)[70] und den VV-Schulakten (s. unter 5.1.1.2) befanden, im wesentlichen aufgegriffen.

Die automatisierte Datenverarbeitung außerhalb der Schule hatte die Schulleitung bisher - ähnlich wie in Hessen - lediglich "in begründeten Ausnahmefällen" zu genehmigen. Der Hessische Landesbeauftragte für den Datenschutz wies mich darauf hin, daß diese Klausel in Hessen von den Lehrern als "Angstklausel" gesehen werde. Da die Genehmigung erteilt werden soll, sofern der Antrag einen zulässigen Datenkatalog enthält und die Sicherstellung der Datenschutzmaßnahmen gewährleistet ist, wird das MBJS auf meine Empfehlung hin diese Klausel streichen.

Zusätzlich sind Bestimmungen zum Datenschutz in Schulbehörden und nachgeordneten Einrichtungen in den Entwurf der DSVS aufgenommen worden. Eine Auflistung aller Daten ist als Anlage 1 der Verordnung vorgesehen, wie ich dies bereits im 3. Tätigkeitsbericht[71] gefordert hatte.

Im übrigen will das MBJS alle meine Hinweise zum Entwurf berücksichtigen, von denen an dieser Stelle nur einige hervorgehoben werden sollen:

Vorgesehen war eine Regelung, wonach die Schule Daten über gesundheitliche Beeinträchtigungen oder Behinderungen ohne Einwilligung der Betroffenen verarbeiten darf, wenn eine Übermittlung durch das Gesundheitsamt erfolgt. Diese von mir als zu allgemein kritisierte Formulierung hat das MBJS auf meinen Vorschlag dahingehend konkretisiert, daß es sich lediglich um einen Ausnahmefall handele und die Übermittlung durch das Gesundheitsamt infolge schulärztlicher Untersuchungen nur aufgrund einer gesetzlichen Übermittlungsbefugnis zulässig sei. Hintergrund dieser Ausnahmeregelung ist, daß sich Eltern weigern könnten, die gesundheitliche Beeinträchtigung (z. B. Epilepsie) ihres Kindes anzugeben, diese Angabe jedoch zu schulorganisatorischen Zwecken (Teilnahme am Sportunterricht) erforderlich ist.

---

66 vom 12. April 1996, GVBl. I S. 102

67 i. d. Fass. vom 1. Juli 1992, GVBl. I S. 694, zul. geänd. d. Art. 1 d. Verord. vom 17. Juni 1993, GVBl. II S. 276

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

69 vom 17. Dezember 1996, GVBl. II S. 21

70 vom 26. November 1993, ABl. MBJS S. 50, geänd. am 3. Dezember 1995, ABl. MBJS S. 560

71 s. unter 5.1.1

Der Verordnungsentwurf legt erstmals fest, daß eine Verwendung von ausschließlich der Verwaltung dienenden Datenverarbeitungsgeräten im Unterricht oder eine Vernetzung mit im Unterricht verwendeten Datenverarbeitungsgeräten ausgeschlossen sein muß. Damit soll einerseits zum Ausdruck gebracht werden, daß der PC jeweils für die Schulverwaltungs- oder Unterrichtszwecke getrennt benutzt werden soll, andererseits beide nicht miteinander vernetzt werden dürfen. Jedoch kann ein Unterrichts-PC auch für Schulverwaltungszwecke und umgekehrt vorübergehend eingesetzt werden (z. B. zum Ausdruck von Zeugnissen), soweit die dafür erforderlichen Sicherheitsmaßnahmen getroffen worden sind (z. B. Löschung der Schülerdaten auf der Festplatte).

Die in § 65 Abs. 6 Satz 3 BbgSchulG vorgeschriebene Aktenkundigkeit von Übermittlungsvorgängen präzisiert die DSVS folgendermaßen: Der anzulegende Vermerk muß die Rechtsgrundlage der Übermittlung, den Umfang der zu übermittelnden Daten sowie die genaue Bezeichnung und Anschrift des Empfängers enthalten. Der Vermerk soll zu den Unterlagen der Schulverwaltung genommen werden.

Die in der DSVS enthaltenen datenschutzrechtlichen Regelungen für Schulpsychologinnen und Schulpsychologen sind im wesentlichen den Nummern 6 bis 8 der VV-Schulpsychologische Beratung[72] entnommen worden. Bei der vom MBJS vorgenommenen Übertragung sind jedoch zunächst zwei Aspekte unberücksichtigt geblieben. Es fehlte die Unterrichtung der Betroffenen über das Ergebnis im Rahmen der Begründung schulbehördlicher Entscheidungen sowie die dreijährige Aufbewahrungsfrist für schulpsychologische Aufzeichnungen, beginnend ab Beendigung der Schulpflicht der Schüler.

Im Rahmen der Planung und Statistik im Schulbereich war zunächst vorgesehen, daß das MBJS personenbezogene Daten verarbeiten darf, sofern diese Daten für die Unterrichtsplanung, für Personalmaßnahmen, für die Stellenbewirtschaftung oder für allgemeine schulaufsichtliche Maßnahmen erforderlich sind. Auf meine Hinweise hin, daß personenbezogene Daten, die bei den Schulen oder den Schulämtern rechtmäßig anfallen, auch nur von diesen selbst zu Geschäftsstatistiken gem. § 9 Abs. 1 BbgStatG[73] verarbeitet werden dürfen, hat das MBJS unter Verweis auf diese statistische Regelung die Vorschrift zufriedenstellend geändert.

5.1.1.2 Neuregelung der VV-Schulakten

Die künftige VV-Schulakten enthält nur noch 5 Ziffern. Sie regelt neben der Begriffsbestimmung die Aufbewahrung, Aussonderung und Vernichtung von Akten. Darüber hinaus enthält sie Übergangs- und Schlußbestimmungen. Die übrigen Vorschriften (Übermittlung, Klassen- und Notenbücher, Schülerakte und Schülerkarteien) sind in die unter 5.1.1.1 abgehandelte DSVS übernommen worden.

Neu in den Katalog der Akten wurden folgende Unterlagen aufgenommen: Schriftverkehr, Unterlagen der Mitwirkungsgremien der Schule und Unterlagen der Schulverwaltung (Verwaltungsakten) sowie Unterlagen über Lehrkräfte und Personen des sonstigen pädagogischen Personals. Mit Inkrafttreten der VV-Schulakten entfällt hingegen die Möglichkeit, Schülerkarteien zu führen.

Die Neuregelung sieht jetzt eine zweijährige Aufbewahrungsfrist für Unterlagen über erteilte Ordnungsmaßnahmen vor.

---

[72] vom 5. September 1994, ABl. MBJS S. 803

[73] vom 11. September 1996, GVBl. I S. 294

Auf meine Anregung hin werden die Schüler oder ihre Eltern über die Rückgabemöglichkeit von abgelaufenen Klassenarbeiten, Klausuren und Prüfungsunterlagen vor der Vernichtung informiert. Diese Information ist wichtig, damit die Betroffenen überhaupt ihre Rückgabewünsche äußern können.

In der VV-Schulakten ist als Übergangsbestimmung vorgesehen, daß Unterlagen, die vor dem 01.01.1991 entstanden sind, bis zum 31.12.1999 aufzubewahren sind. Danach sollen Durchschriften oder Kopien der Abgangs- und Abschlußzeugnisse oder die diese rekonstruierenden Unterlagen an das staatliche Schulamt übergeben werden.

5.1.2 Lehrerfortbildung

Das Brandenburgische Schulgesetz enthält keine lehrerbildungsrechtlichen Regelungen. Das MBJS beabsichtigt, diese in einem eigenen Lehrerbildungsgesetz für das Land Brandenburg zu treffen. Deshalb sind bis dahin die §§ 61, 64 bis 71 und § 72 Buchst. a und b 1. SRG als Übergangslösung weiter in Kraft geblieben und es mußten

- die Ergänzungsprüfungsverordnung[74] und
- die Prüfungsberufsverordnung[75]

noch auf der Grundlage des § 75 Abs. 2 Buchst. c 1. SRG bis zum 31. Juli 1996 in Kraft gesetzt werden. Hierzu habe ich jeweils Stellung genommen; das Ministerium hat die Vorschläge teilweise berücksichtigt.

Das Ministerium ist aufgefordert, einen Entwurf für ein Lehrerfortbildungsgesetz vorzulegen.

5.2 Datenschutz im Schulbereich

5.2.1 Kontrollbesuche in Schulen

Das Inkrafttreten des Brandenburgischen Schulgesetzes habe ich zum Anlaß genommen, in zehn Schulen Datenschutzkontrollen durchzuführen. Dabei handelte es sich um zwei Realschulen, zwei Gymnasien und sechs Gesamtschulen in verschiedenen Landkreisen. Schwerpunkte der Prüfung waren jeweils die Umsetzung der datenschutzrechtlichen Bestimmungen (VV-Schulakten, VV-Datenschutz/Statistik sowie die allgemeinen Bestimmungen wie z. B. § 8 Abs. 1 BbgDSG) und die Einhaltung technisch-organisatorischer Maßnahmen. Zusätzlich hat mit dem MBJS eine Gesamtauswertung der Kontrollbesuche stattgefunden.

Einen Großteil der festgestellten Mängel führe ich darauf zurück, daß sich einige Schulen wohl erst nach Ankündigung des Kontrollbesuchs intensiv mit datenschutzrechtlichen Bestimmungen im Schulbereich auseinandergesetzt haben. Die folgende Zusammenfassung der Prüfungs-feststellungen soll anderen Schulen eine Handlungshilfe geben:

- Schülerakte

---

[74] vom 25. Juli 1996, GVBl. II S. 605

[75] vom 25. Juli 1996, GVBl. II S. 613

In die Schülerakte gehört lediglich ein aktuell geführtes Schülerstammblatt, auf dem grundsätzlich nur die vorgeschriebenen Daten vermerkt sein dürfen. Soweit Schülerstammblätter von anderen Schulen übernommen worden sind und diesen Anforderungen nicht mehr entsprechen, weil z. B. das Datum der Religionszugehörigkeit enthalten ist, sind diese zu vernichten und neu anzulegen. Die automatisierte Führung der Schülerstammblätter ersetzt nicht die entsprechende Papierform. Nach Auffassung des MBJS soll auch in diesen Fällen das Schülerstammblatt in Papierform Bestandteil der Schülerakte sein, da es über alle wichtigen Informationen der Schüler auf einen Blick Auskunft gibt.

Kopien von Schwerbehindertenausweisen zum Nachweis des Grades der körperlichen Behinderung und den damit verbundenen schulorganisatorischen Einschränkungen sind nicht zu den Schülerakten zu nehmen; hierzu reicht ein entsprechender Hinweis auf die Tatsache der Schwerbehinderung aus.

Da die Krankenkasse lediglich für den Eintritt eines Schadensereignisses gegenüber dem Unfallversicherungsträger genannt werden muß, ist die vorsorgliche Erfassung dieser Daten in der Schülerakte oder im Notenbuch unverhältnismäßig und führt zu einer unzulässigen Datenvorratshaltung. Im Falle eines Unfalles können die Erziehungsberechtigten bei der Benachrichtigung nach der Krankenkasse gefragt werden.

In Schülerakten fanden sich Laufzettel vom Gesundheitsamt mit medizinischen Daten. Ich werde darauf hinwirken, daß Gesundheitsämter nur noch kodierte Befunde für diese Zwecke ausstellen. Bis dahin müssen solche Laufzettel vernichtet werden.

Freistellungsanträge von Schülern einschließlich der Bestätigungen durch die Schulleitung sollten gesondert (in einem Ordner) aufbewahrt werden.

- Klassen-, Kurs- und Notenbücher

Im Klassenbuch sind grundsätzlich nur die in Nr. 5 VV-Schulakten aufgeführten Daten einzutragen. Trotzdem waren häufig die dienstliche Telefonnummer der Eltern und das Geburtsdatum der Schüler festgehalten. Obwohl gute Gründe für solche Datenspeicherungen sprechen, können sie - mangels Rechtsgrundlage - doch nur auf freiwilliger Basis erhoben werden. Dabei sind die Betroffenen auf den Zweck der Datenerhebung, auf den Ort der Speicherung sowie auf die Folgen der Verweigerung (keine Rechtsnachteile) hinzuweisen.

Gem. Nr. 6 VV-Schulakten sind Notenspiegel Informationen über Noten und dürfen somit ausschließlich in den dafür vorgesehenen Notenbüchern eingetragen werden.

Entschuldigungsschreiben dürfen nicht in Kursbücher eingeklebt oder gar lose im Klassenbuch aufbewahrt werden. Der Klassenlehrer hat - auch im Vertretungsfall - für deren Aufbewahrung in einer gesonderten Mappe und deren Vernichtung zu sorgen.

Ärztliche Atteste gehören ebenfalls nicht in das Klassenbuch, sondern müssen in einem verschlossenen Umschlag in der Schülerakte abgeheftet werden.

In den Notenbüchern werden zum Teil Besonderheiten eingetragen (wie z. B. körperbehindert, Wespenallergie). Gem. Nr. 8 Buchst. a ff. VV-Schulakten müssen jedoch besondere gesundheitliche Beeinträchtigungen in das dafür vorgesehene Feld

des Schülerstammblattes eingetragen werden, sofern dazu die Einwilligung der Eltern vorliegt.

- Schülerkarteikarten

In einer Schule ist mir berichtet worden, daß sie der Polizei Einblick in die Schülerkarteikarten gewährt habe, um Schüleranschriften zu ermitteln. Hierzu ist zu bemerken, daß in konkreten Ermittlungsverfahren die Identdaten bei der Meldebehörde und nicht bei der Schule zu erheben sind. In Verfahren, in denen die Schule nicht selbst Anzeigeerstatter ist, teilt die Schule die zur Aufklärung des Ermittlungsverfahren erforderlichen und ihr vorliegenden Informationen unter Berücksichtigung der Schweigepflicht mit. Vor der Informationsweitergabe sollte sie jedoch selbst prüfen, ob Umstände vorliegen (wie z. B. Anwesenheit im Unterricht zum Tatzeitpunkt), die einen tatverdächtigen Schüler als Täter ausschließen. Sofern die Polizei die Zusammenarbeit mit der Schule zu Zwecken der Prävention sucht, dürfen hierbei grundsätzlich keine personenbezogenen Informationen übermittelt werden. Wenn die Schule über Anhaltspunkte für eine Straftat verfügt, sollte sie ihrerseits Anzeige erstatten.

Jugendärztliche Beurteilungen, die gelegentlich an Schülerkarteikarten geheftet worden waren, müssen in einem verschlossenen Umschlag in der Schülerakte abgelegt werden. Dies ist um so mehr zu beachten, als mit Inkrafttreten der VV-Schulakten Schülerkarteikarten nicht mehr geführt werden dürfen.

- "Mitteilungshefte"

Häufig bedienen sich Fachlehrer sog. "Mitteilungshefte", um den Klassenlehrer über das Fehlverhalten seiner Schüler/Schülerinnen zu informieren. Gegen ein solches Vorgehen ergeben sich nur dann aus datenschutzrechtlicher Sicht Einwände, wenn die Mitteilungshefte Dritten ohne weiteres einsehbar sind und nicht verschlossen entweder im Lehrerzimmer oder im Sekretariat aufbewahrt werden.

- Datenübermittlungen

Regelmäßig werden personenbezogene Schülerdaten an Busunternehmen übermittelt, um ermäßigte Fahrkarten auszustellen. Im Einzelfall hat dabei die Schule zu prüfen, ob die angeforderten Daten für die Aufgabenerfüllung überhaupt erforderlich sind. Das dürfte für den Namen, Vornamen und die Haltestelle/Einstiegsort des Fahrschülers zutreffen, nicht jedoch für darüber hinausgehende Daten wie z. B. das Geburtsdatum.

Zur "internen" Übermittlung werden offensichtlich gern Aushänge im Lehrerzimmer genutzt, in denen beispielsweise der Lehrkörper über Erkrankungen einzelner Schüler unterrichtet wird oder Fehlzeiten eines bestimmten Schülers notiert werden sollen. Ob dies unter schulorganisatorischen Gesichtspunkten eine sinnvolle Verfahrensweise darstellt, sei hier dahingestellt. Da aber neben den Lehrern auch schulfremde Personen Zugang zu dem Lehrerzimmer haben und somit unbefugt Kenntnis über diese sensiblen Daten erhalten, sind solche Aushänge unzulässig.

- Verwendung von Formularen

Für die Durchführung von Schülerbetriebspraktika wurden zum Teil noch alte Vereinbarungsformulare verwendet, obwohl hierfür ein in der Anlage zur VV-Betriebspraktika[76] überarbeitetes Formular verbindlich vorgesehen ist.

[76] vom 4. September 1995, ABl. MBJS S. 502

- Technisch-organisatorische Maßnahmen

Bei den geprüften Schulen war der Standard der technischen Ausstattung nicht gerade zeitgemäß. Von den zehn Schulen verfügen lediglich zwei über Computer für die Wahrnehmung von Verwaltungsaufgaben. Selbst bei diesen fehlten die Dateibeschreibungen und die Geräteverzeichnisse nach § 8 Abs. 1 und Abs. 4 BbgDSG oder sie waren unvollständig ausgefüllt. Hierbei mußte ich auf die Verordnung zur Dateibeschreibung[77] (s. unter 2.2) und auf die darin enthaltenen zu verwendenden Musterformblätter hinweisen.

Ob schuleigene oder private Datenverarbeitungsgeräte außerhalb der Schule zur Verarbeitung personenbezogener Daten eingesetzt werden, konnte nicht in jedem Fall beantwortet werden. Hierzu mußte ich auf Nr. 3 a Abs. 1 VV-Datenschutz/Statistik und die Anlage 3 hinweisen, wonach jede dienstliche Nutzung privater PC's einer Genehmigung des Schulleiters bedarf.

Erfreulicherweise verfügen 9 von 10 Schulen über einen Aktenvernichter als Grundausstattung des Sekretariats. Allerdings entsprachen diese nicht immer den jeweils erforderlichen Sicherheitsstufen nach DIN 32757[78].
In manchen Schulen sind Grund- und Gesamt- bzw. Realschule mit jeweils eigenen Schulleitungen unter einem Dach vereint. In diesen Fällen muß sichergestellt werden, daß neben der personellen Trennung auch eine getrennte Aufbewahrung von Schülerakten besteht. Selbst wenn nur ein Sekretariat für alle Schulformen zur Verfügung steht, dürfen die Schulleiter lediglich Zugriff auf Schülerakten ihrer jeweiligen Schule haben.

---

77 vom 7. Oktober 1996, GVBl. II S. 695

78 s. 4. Tätigkeitsbericht unter 1.4.3 sowie Broschüre "Technisch-organisatorische Aspekte des Datenschutzes" aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert" unter Pkt. 6

Zum Teil sind bereits Altunterlagen, die nicht zu den Schulakten im Sinne der VV-Schulakten zu zählen sind, vernichtet worden, anstatt diese gem. § 4 Abs. 1 BbgArchivG dem zuständigen Archiv anzubieten. Dies ist in Unkenntnis des Rundschreiben 29/96 vom MBJS[79] geschehen, wonach Schulakten in den Schulen bis auf weiteres aufzubewahren sind.

Klausuren sind nach Ablauf einer einjährigen Aufbewahrungsfrist zu vernichten oder an den Schüler auszuhändigen.

Ein besonderes Problem ist die Sicherung der Schulgebäude. Einbrüche fanden seit 1990 fast in allen der geprüften Schulen statt. In keinem Fall war von der naheliegenden Möglichkeit, polizeiliche Beratungsstellen um praktische Hinweise zur Gebäudeabsicherung zu bitten, Gebrauch gemacht worden.

Nur vereinzelt existierten Dienstanweisungen zum Datenschutz in der Schule. Sofern sie vorhanden waren, müssen diese noch an die Bestimmungen des Brandenburgischen Schulgesetzes und an die im Laufe des Jahres in Kraft tretenden untergesetzlichen Bestimmungen angepaßt werden.

Aufgrund der zugesandten Prüfberichte haben mir die Schulen unterdessen erfreuerlicherweise mitgeteilt, daß sie die festgestellten Mängel zwischenzeitlich abgestellt haben. Lediglich für die Dienstanweisungen trifft dies nicht zu; diesbezüglich hatte ich darauf orientiert, daß deren Überarbeitung unverzüglich nach Inkrafttreten der DSVS (s. unter 5.1.1.1) sowie der VV-Schulakten (s. unter 5.1.1.2) geschehen soll. Im übrigen habe ich regelmäßig Gelegenheit genommen, darauf hinzuweisen, welche Änderungen durch Überarbeitung der geltenden Bestimmungen zu erwarten sind.

5.2.2 Schulverwaltungssystem

Das MBJS hat sich im März 1996 entschlossen, einheitliche EDV-Programme zur schulinternen Verwaltung anzuschaffen. Diese Initiative wurde meinerseits begrüßt, da einheitliche und standardisierte Programme den Wildwuchs selbst erstellter Dateien eindämmen und so am effektivsten die Gewähr für eine aus datenschutzrechtlicher Sicht zufriedenstellende Durchführung technisch-organisatorischer Sicherheitsmaßnahmen bieten. Bei der Planung des Projektes hat das Ministerium unter Leitung des Pädagogischen Landesinstituts Brandenburg meine Behörde einbezogen. Inzwischen wurde ein Produkt ausgewählt und Landeslizenzen vom MBJS erworben. Die Software kann von jeder Schule kostenlos bezogen werden.

Nach der schrittweisen Einführung der Programme an den Schulen wird ein elektronischer Datenaustausch angestrebt, was z. B. die statistischen Erhebungen im Schulbereich wesentlich vereinfachen wird. In der Endphase soll dieses Vorhaben sogar über eine Datenfernübertragung realisiert werden. Die Übertragung personenbezogener Daten über öffentliche Netze muß unter besonderen sicherheitstechnischen Voraussetzungen stattfinden.

In das Programm dürfen nur die Schülerdaten aufgenommen werden, die abschließend in der DSVS (s. unter 5.1.1.1) aufgeführt sind. Eine Erweiterung des Datenkatalogs in der Anlage 1 des DSVS-Entwurfs hat u. a. durch die Aufnahme des Datums "Geburtsname" stattgefunden. Darüber hinausgehende Angaben wie z. B. " Religionsunterricht" sind, soweit deren Erforderlichkeit bejaht wird, lediglich mit Einwilligung der Eltern einzutragen.

Ich werde mich weiterhin über die Entwicklung des Schulinformationssystems informieren und gegebenenfalls kritische Hinweise geben.

---

[79] vom 19. April 1996, ABl. des MBJS, S. 299

5.2.3 Eingaben/Anfragen

5.2.3.1 Adreßweitergabe von Schulabgängern an Banken

Ein Schulverwaltungsamt fragte bei mir an, ob die Weitergabe der Adressen von Schulabgängern an Banken gegen den Datenschutz verstoßen würde. Die Filiale einer Bank beabsichtige, diesen Gutscheine zuzuschicken. Diese Verfahrensweise sei laut Auskunft der anfragenden Bank in den alten Bundesländern und auch bei anderen Schulträgern "gang und gäbe".

Eine solche Datenübermittlung an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung der Betroffenen zulässig. Allerdings würde aus datenschutzrechtlicher Sicht auch nichts gegen ein Adreßmittlungsverfahren[80] einzuwenden sein. Dabei würden der Schulverwaltung von der Bank vorfrankierte (nicht adressierte) Kuverts mit dem zu übersendenden Material übergeben. Von dieser würden die Kuverts dann aufgrund des dort vorliegenden Anschriftenmaterials adressiert und verschickt werden. Der Adressat entscheidet dabei durch seine Rückantwort selbst, ob er sich mit der Bank in Verbindung setzen möchte. Auf diese Weise wird vermieden, daß die Adressen von Schulabgängern Dritten unbefugterweise zur Kenntnis gelangen und daß die Einwilligung zur Nutzung von ursprünglich zu anderen Zwecken gespeicherten Daten eingeholt werden muß. Diese Rechtsauffassung teilte ich dem Schulverwaltungsamt mit. Darüber hinaus habe ich aufgrund der angeblich weit verbreiteten Vorgehensweise zur Werbung künftiger Kunden das MBJS über die Angelegenheit in Kenntnis gesetzt und gebeten, die Schulverwaltungsämter mittels eines Rundschreibens auf die Rechtslage hinzuweisen.

Meiner Rechtsauffassung hat sich das Ministerium nach einigem Zögern schließlich angeschlossen. Obwohl das Adreßmittlungsverfahren nach seiner Meinung einen unverhältnismäßig hohen Verwaltungsaufwand darstelle, hat es schließlich die staatlichen Schulämter sowie die Schulverwaltungsämter nochmals darauf hingewiesen, daß eine Weitergabe von Daten der Schülerinnen und Schüler, der Eltern und Lehrkräfte nur im Rahmen der Bestimmungen der VV-Datenschutz/Statistik bzw. des § 65 BbgSchulG erfolgen dürfe.

5.2.3.2 Erfassung der "Nichtteilnahme" am Religionsunterricht

Eltern machten mich auf folgenden Sachverhalt aufmerksam: In der Elternversammlung einer Grundschule habe ein Religionslehrer Anmeldeformulare für die Teilnahme am Religionsunterricht mit der Maßgabe verteilt, daß auch die Eltern den Bogen ausfüllen sollten, die eine Teilnahme ihrer Kinder nicht wünschten.

Gem. § 9 Abs. 2 Satz 4 BbgSchulG ist lediglich eine schriftliche Erklärung der am Unterricht teilnehmenden Schüler erforderlich. Die Nichtteilnahme soll danach nicht dokumentiert werden. Eine diesbezügliche Datenerhebung ist somit unzulässig. Diese Rechtslage habe ich sofort dem Schulleiter der betreffenden Grundschule mitgeteilt. Darüber hinaus habe ich das MBJS über diesen Vorgang unterrichtet und empfohlen, zur Rechtsklarheit ein Rundschreiben an alle Schulen zu erarbeiten.

Der Schulleiter stellte daraufhin das unzulässige Verfahren auf meinen Hinweis hin sofort ab. Das anfänglich etwas uneinsichtige MBJS zeigte sich doch noch kooperativ. Der Sachverhalt wurde zunächst in der Dienstberatung der Schulräte dargelegt, damit diese die Information an die Schulleitungen weitergeben. Unterdessen hat mir das MBJS den Entwurf

[80] s. auch unter 5.2.4.2

eines Rundschreibens zugeleitet, in dem alle Schulen des Landes über die unzulässige Handlungsweise im Rahmen der Teilnahme am evangelischen Religionsunterricht aufgeklärt werden.

5.2.4 Wissenschaftliche Untersuchungen

5.2.4.1 Studie: Politische Sozialisation von Gymnasiasten

Die behördliche Datenschutzbeauftragte einer kreisfreien Stadt sprach mich auf das Projekt "Politische Sozialisation von Gymnasiasten" an, zu dem ich laut Informationsmaterial hinsichtlich der Vorgehensweise meine Billigung gegeben hätte. Diese Unterstellung stellte sich alsbald als unzutreffend heraus. Vielmehr handelte es sich um ein vom MBJS genehmigungspflichtiges Forschungsvorhaben einer Universität sowie einer Fachhochschule des Landes, über das der Projektleiter mit dem behördlichen Datenschutzbeauftragten ein Telefonat geführt hatte. Zudem hatte das MBJS selbst die Genehmigung des Forschungsprojektes ohne hinreichende Prüfung erteilt.

Das Projekt hatte zum Ziel, die Ausbildung politischer Einstellungen, Verhaltensbereitschaften und Verhaltensweisen (u. a. auch Mitgliedschaften in Organisationen, ehrenamtliche Tätigkeiten, Engagement, Konfliktbereitschaft, Toleranz und Diskursfähigkeit, Gewaltbereitschaft und Gewalterfahrung) von Jugendlichen im Alter von 15 und 16 Jahren zu untersuchen. Deshalb bezog die Untersuchung auch neben der Befragung der Jugendlichen selbst sowohl deren Eltern (getrennte schriftliche Befragung) als auch gleichaltrige Freunde (soweit durch parallele klassenweise Befragung erfaßt) mit ein. Die Befragung sollte ungefähr im Abstand von einem Jahr wiederholt werden, sofern sich dies für die Nachzeichnung von Kausalhypothesen als erfolgversprechend herausstellen sollte. In die Untersuchung sollten bei der ersten Befragung etwa 1200 Gymnasiasten und 1400 Real- und Gesamtschüler (jeweils der Klasse 10) einbezogen werden. Letztere sollten in der zweiten Erhebung postalisch befragt werden, da sie zu diesem Zeitpunkt überwiegend bereits die Schule verlassen haben werden.

Das MBJS hatte zwar in seinem Genehmigungsschreiben einige datenschutzrechtliche Hinweise gegeben, die jedoch unzureichend waren. Dies traf insbesondere für die datenschutzrechtlichen Voraussetzungen der Einwilligungsgerklärung gem. § 4 Abs. 1 BbgDSG zu. Sie hätten lediglich in engster Verbindung mit dem Informationsschreiben an die Eltern hinsichtlich des Aufklärungsgebotes gegenüber dem Betroffenen als ausreichend angesehen werden können. Die Einverständniserklärung soll wegen des Bestimmtheitsgebotes zu folgenden Aspekten selbst Ausführungen enthalten:

- Zweck der Erhebung (z. B. durch Nennung des Forschungsprojektes),
- Angabe der datenverarbeitenden Stelle,
- Rechtsgrundlage der Erhebung und ggf. Verarbeitung personenbezogener Daten und
- Hinweis auf die Rechtsfolgen der Einverständniserklärung.

Darüber hinaus vermißte ich hinsichtlich der technisch-organisatorischen Maßnahmen Hinweise zur Art und Weise der Abgabe/Übersendung der Fragebögen sowohl von Schülern als auch deren Müttern, die Angabe von Löschungsfristen für die Adressen als Zusicherung an den Betroffenen sowie die Art und Weise der Verwendung von Code-Nummern im Fragebogen.

Da die Erstbefragung bereits abgeschlossen war, ließen sich daraus nur Konsequenzen für die zu diesem Zeitpunkt lediglich beabsichtigte Zweitbefragung ziehen und der Vorfall zum Anlaß nehmen, die Problematik der genehmigungspflichtigen Forschungsvorhaben gem. § 66 Abs. 1 BbgSchulG i. V. m. Nr. 1 Abs. 1

VV-WissU[81] mit dem MBJS zu klären. Hierzu waren Gespräche beim Staatssekretär sowie mit dem für die Genehmigung von Forschungsvorhaben befaßten Referat hilfreich, bei denen folgende Festlegungen für eine künftige Verfahrensweise, die hoffentlich künftig derartige Vorkommnisse vermeiden helfen, getroffen worden sind:

- Jedem Genehmigungsantrag ist eine Datenschutzkonzeption beizufügen.
- An die Einverständniserklärungen sind Mindestanforderungen (s. oben) zu stellen.
- Meine Behörde wird laufend über die vom MBJS genehmigten Projekte informiert.

Darüber hinaus habe ich über den Rektor der Universität Kontakt mit dem Projektleiter aufgenommen und für die zweite Erhebungswelle folgende Dinge abgeklärt:

Die Adressen der Haupt- und Realschüler werden weiterhin aufbewahrt, wenn sich auch deren Eltern an der Erstbefragung beteiligt haben. Sofern im Rahmen der zweiten Erhebungswelle nach spätestens drei Monaten keine Rückantworten der angeschriebenen bisherigen Teilnehmer beim Projektleiter erfolgen, müssen die Adressen dieser Nichtteilnehmer gelöscht werden. Im Zuge der Datenauswertung dürfen keine vernetzten Computer benutzt werden, um einen unbefugten und unbegrenzten Zugriff auf diese Daten zu vermeiden.

Der Projektleiter teilte mir daraufhin mit, daß er alle Adressen von Gymnasiasten vernichtet habe mit Ausnahme der Adressen derjenigen, die ein zusätzliches Tonbandinterview außerhalb der Schule gegeben hatten und in einem Jahr noch einmal um ein Tonbandinterview gebeten werden sollen. Die Einverständniserklärungen für die zweite Erhebung wurden meinen Vorgaben entsprechend überarbeitet.
Für weitere Forschungsprojekte der Universität habe ich darauf hingewiesen, daß Datenschutzkonzeptionen zu erstellen seien, die den verfahrensmäßigen Umgang mit den zu verarbeitenden personenbezogenen Daten (z. B. die Beschreibung der Rechnersysteme, Zugriffsrechte, Lagerung der Adreßlisten) detailliert regeln. Diese sind jeweils als Bestandteil der Genehmigungsunterlagen beim MBJS mit einzureichen.

Der Rektor der Universität teilte mir daraufhin mit, daß im Wintersemester 1996/97 im Rahmen der Schulung/Beratung von Wissenschaftlern verstärkt auf die in diesem Projekt aufgetretenen datenschutzrechtlichen Defizite hingewiesen werden solle.

5.2.4.2 Studie: Ausbildungs- und Berufswege von Schulabgängern

An das MBJS war das Anliegen herangetragen worden, die Übermittlung von ca. 1000 Adressen studienberechtigter Schulabgänger des Schulentlassungsjahres 1995/96 zu genehmigen, um darauf aufbauend eine Befragung über deren schulischen Werdegang durchzuführen. Gegen die Herausgabe der Adressen von Studienberechtigten bestand aus Sicht des MBJS einerseits erhebliche Bedenken, andererseits zeigte es an der Durchführung der Studie ein besonderes Interesse, da es sich von ihr eine gewichtige Unterstützung zu bildungspolitischen Entscheidungen erhoffte. Das Ministerium bat mich um eine Stellungnahme, da es die Möglichkeit, die Befragungsunterlagen durch die Schulen direkt an die Studienberechtigten zu senden (Adreßmittlungsverfahren), nicht in Betracht ziehen wollte. Es würde für die Schulen einen zu großen Verwaltungsaufwand nach sich ziehen.

Meiner Auffassung nach besteht für die Schulen der größte Aufwand in der Regel darin, daß sie die Adressen heraussuchen

[81] vom 1. August 1995, ABl. MBJS S. 408

müssen. Ob sie diese dann in einem zweiten Schritt listen- oder formmäßig erfassen oder ob sie diese auf Kuverts - notfalls auch handschriftlich - übertragen, stellt vom erforderlichen Arbeitsaufwand her keinen wesentlichen Unterschied dar. Es dürfte in Zukunft außerdem davon auszugehen sein, daß die Schulsekretariate in der Lage sind, serienmäßig Adreßetiketten auszudrucken, die dann lediglich auf Kuverts aufgeklebt werden müssen.

Das MBJS hat schließlich doch in seiner Genehmigung auf das Adreßmittlungsverfahren abgestellt. Da es sich bei der Angelegenheit um Wiederholungsuntersuchungen handelt, hat das Ministerium für das kommende Schuljahr bzw. für weitere geplante Untersuchungen angekündigt, die beantragende Stelle darauf hinzuweisen, daß Fragebögen vor Beendigung des Schuljahres durch die Schule an die Schüler verteilt werden können, so daß einerseits die Schulsekretariate nicht zusätzlich belastet werden und andererseits auch das Recht der Schülerinnen und Schüler auf informationelle Selbstbestimmung gewahrt bleibt.

5.2.4.3 Fragebogen zum Freizeitverhalten von Schülern

Ein Jugendamt hat mich über das Modellvorhaben "Netzwerk für potentielle junge Trebegänger" des Landesjugendamtes informiert. Mit diesem Modellvorhaben soll ein freier Träger beauftragt werden, eine Zuarbeit für die Jugendhilfe zu leisten, indem die Schüler der 9. und 10. Klasse über das in ihrem Wohnort vorhandene Freizeitangebot befragt werden sollen, um so herauszufinden, ob die "Schulbummelei" lediglich bei solchen Schülern verstärkt auftritt, die kaum oder gar keine Freizeitangebote wahrnehmen. Die Ergebnisse sollen als Entscheidungsgrundlage für die Jugendhilfeplanung dienen. Da auf dem Fragebogen zwar keine Namen, wohl aber der Wohnort angeben sind, kann aufgrund des u. U. sehr kleinräumigen Ortsbezugs der Fragebogen nicht als eine anonyme Datenerfassung i. S. d. § 3 Abs. 3 BbgDSG angesehen werden. Daher habe ich empfohlen, anstatt der Angabe "Ich wohne in der Ortschaft" den Ortsbezug großräumiger in "Gemeinde" abzuändern. Darüber hinaus habe ich beanstandet, daß die Schüler die Namen älterer Vereinsmitglieder angeben sollten und daß keine Einwilligungserklärung der Eltern vorgesehen ist.

In einem Gespräch sowohl mit dem freien Träger als auch mit der Jugendhilfeplanerin des Jugendamtes konnte erreicht werden, daß meinen Vorschlägen entsprechend verfahren wird.

5.2.4.4 Merkblatt/Checkliste für Forschungsvorhaben an Schulen

Die bei der Studie "Politische Sozialisation von Gymnasiasten" (s. unter 5.2.4.1) aufgetretenen erheblichen datenschutzrechtlichen Defizite haben mich dazu veranlaßt, in Abstimmung mit dem MBJS ein Merkblatt zur Datenerhebung und -verarbeitung bei Forschungsvorhaben an Schulen zu erarbeiten. Das Ministerium hatte ein solches Verfahren begrüßt. Die Gespräche sind jedoch noch nicht abgeschlossen.

Darüber hinaus habe ich dem Ministerium einen Fragenkatalog zur Prüfung von genehmigungspflichtigen Forschungsvorhaben zugeleitet, der als "Checkliste" hierfür dienen könnte. Ich hege die Hoffnung, daß sich dadurch künftig die Genehmigungsverfahren formalisieren und somit deren datenschutzrechtliche Überprüfung erleichtern lassen.

5.3 Jugend

5.3.1 Kitagebührenerhebung - neue Rechtslage

Alte Rechtslage:

Nach der alten Regelung in § 17 Abs. 4 Brandenburgisches Kindertagesstättengesetz (Kita-Gesetz)[82] konnte der örtliche Träger der öffentlichen Jugendhilfe in strittigen Fällen verlangen, daß die Angaben zur Einkommenshöhe ihm gegenüber glaubhaft gemacht werden. Wie in der Vergangenheit mehrfach berichtet[83], bereitete die Formulierung "in strittigen Fällen" dem Praxisanwender große Auslegungsschwierigkeiten. Mit dem Ersten Gesetz zur Änderung des Kindertagesstättengesetzes[84] (s. auch unter 7.3.1.6) ist nunmehr Rechtssicherheit eingetreten. Bedauerlicherweise habe ich den Entwurf erst zusammen mit der Einladung zur Beratungssitzung des Ausschusses für Bildung, Jugend und Sport erhalten.

Neue Rechtslage:

Zunächst ist mit Satz 4 in § 17 Abs. 3 Kita-Gesetz eine eigene Rechtsgrundlage für das Verarbeiten von personenbezogenen Daten durch den Träger der Einrichtung geschaffen worden. Dabei sind die Angaben über die Einkommensverhältnisse nur für die aktuelle Festlegung der Höhe des Elternbeitrages, d. h. für den zeitlichen Abschnitt, für den Kita-Elternbeiträge zu zahlen sind, als erforderlich anzusehen. Eine darüber hinausgehende Erhebung von Daten auf Vorrat ist unzulässig. Damit haben die Eltern eine Nachweispflicht gegenüber dem Träger der Einrichtung über ihr Einkommen, sofern sie nicht die Höchstbeiträge bezahlen wollen.

82 vom 10. Juni 1992, GVBl. I S. 178

83 s. 1. Tätigkeitsbericht unter 7.3; 2. Tätigkeitsbericht unter 7.3.1; 3. Tätigkeitsbericht unter 7.1.5

84 vom 7. Juni 1996, GVBl. I S. 17

Die bisher von mir empfohlene Selbsteinstufung ohne Kontrollmöglichkeit der Einkommensverhältnisse ist gem. § 17 Abs. 3 Satz 4 und 5 Kita-Gesetz nicht mehr zulässig. Die Erklärungen und Nachweise zur Einkommenshöhe müssen gegenüber dem Träger abgegeben werden, wobei eine eidesstattliche Versicherung nicht ausreichend ist. Zum Nachweis dieser Angaben sind geeignete Urkunden (z. B. Steuerbescheid, Einkommensbescheinigungen des Arbeitgebers, u. ä.) im Original vorzulegen. Eine Kopie der Nachweise kann zu den Akten genommen werden. Diese können selbst mit den Originalen vorgelegt werden, wobei etwaige Angaben, die zur Überprüfung der Einkommensverhältnisse nicht benötigt werden (z. B. über die Religionszugehörigkeit, den Arbeitgeber, u. ä.) unkenntlich gemacht werden können[85]. Gemäß § 17 Abs. 3 Satz 5 Kita-Gesetz sind die Daten zu löschen, sobald sie für die Festsetzung und Erhebung der Elternbeiträge nicht mehr erforderlich sind. Das ist u. a. immer dann der Fall, wenn eine neue, aktuellere Einkommensangabe gegenüber dem Träger der Kindertagesstätte gemacht wurde. Bei kommunalen Trägern, die Elternbeiträge öffentlich-rechtlich erheben, sind die Daten zu löschen, sobald der Gebührenbescheid Bestandskraft erlangt hat, d. h. wenn der Bescheid nicht mehr mit Rechtsmitteln (Widerspruch, Anfechtungsklage) angefochten werden kann.

5.3.2 Verwendungsnachweis über Betreuungsmittel

In meinem 4. Tätigkeitsbericht[86] hatte ich im Zusammenhang mit einer Petition eines freien Trägers über den o. g. Runderlaß an die örtlichen Träger der öffentlichen Jugendhilfe im Land Brandenburg berichtet. Danach sollten für die Gewährung und Verwendung von Landeshaushaltsmitteln für die Kindertagesbetreuung die betreuten Kinder namentlich aufgelistet nachgewiesen werden.

Da nähere Ausführungen hierzu bislang noch fehlen, habe ich dem freien Träger mitgeteilt, daß auch das damals zuständige Ministerium für Arbeit, Soziales, Gesundheit und Frauen bisher nicht die Auffassung vertrat, den Erlaß zum jetzigen Zeitpunkt umzusetzen. Von dem seit 1. August 1996 zuständigen Ministerium für Bildung, Jugend und Sport habe ich auf meine Anfrage hin noch keine Antwort erhalten.

In der Zwischenzeit ist eine neue Verordnung über die Angemessenheit der Betriebskosten in Kindertagesstätten und das Antrags- und Zahlungsverfahren (Kita-BKV)[87] ohne meine Beteiligung in Kraft getreten, die jedoch keine aus datenschutzrechtlicher Sicht für das Verfahren entscheidungsrelevanten Änderungen enthält.

6 Wissenschaft, Forschung und Kultur

6.1 Verwendung der Einweg-Hashfunktion als Lösungsweg für an sich zu löschende Daten

---

85 vgl. das Verfahren zum Einkommensprüfungserlaß unter 10.1.2

86 s. unter 7.4.3

87 vom 22. Januar 1997, GVBl. II S. 46

Bei Langzeituntersuchungen, für die über eine Reihe von Jahren weitere Probanden rekrutiert werden sollen, gewinnt im Verlauf der Studie das Problem immer mehr an Bedeutung, daß Bürger erneut angeschrieben werden, die bereits in den Vorjahren unmißverständlich ihre freiwillige Beteiligung an einer Studie (§ 4 Abs. 1 Alternative b BbgDSG) abgelehnt hatten. Durch die Bearbeitung einer Eingabe eines Bürgers bin ich auf die Praxis gestoßen, daß über solche "Verweigerer" eine Datei geführt wird, gegen die die Adressen der gem. § 32 Abs. 2 Brandenburgisches Meldegesetz (BbgMeldeG)[88] erhaltenen Gruppenauskünfte der nachfolgenden Jahre abgeglichen werden. Dies wurde mir damit erklärt, daß hierdurch sowohl Postgebühren gespart als auch die erfahrungsgemäß und nicht unberechtigte emotionale Reaktion dieses Personenkreises auf ein erneutes Anschreiben hin vermieden würden. Durch letzteres wurde zusätzlich befürchtet, daß insgesamt die Studie in Verruf kommen könnte. Für die Speicherung gibt es jedoch keine Rechtsgrundlage, sie ist für den Zweck des eigentlichen Forschungsvorhabens nicht erforderlich, und es fehlt hierfür die Einwilligung der Betroffenen.

Als Lösungsweg für diesen offensichtlichen Interessenkonflikt zwischen Datenschutz einerseits und den pragmatischen Vorstellungen der Wissenschaftler andererseits habe ich angeregt, anstelle der unzulässigen Datei von Verweigerern eine Blackbox zu verwenden. Aus der Literatur sind sog. Einweg-Hashfunktionen (z. B. MD 5, SHA) bekannt, die aus einer beliebig langen Zeichenkette einen eindeutigen Wert fester Länge erzeugen (z. B. 16 Byte). Dieser Wert wird auch als Hashwert bezeichnet. Ein Rückschluß vom erzeugten Hashwert auf die Eingangszeichenkette ist grundsätzlich nicht möglich. Damit werden personenbezogene Informationen vorgehalten, die nur im positiven Abgleichsfall als solche identifiziert werden.

In einer Datei (sog. Blackbox) werden die Hashwerte der Betroffenen gespeichert, die nicht an der Untersuchung teilnehmen wollen. Von den neuen Adressen wird von jedem Datensatz der Hashwert ermittelt und überprüft, ob dieser in der "Hashdatei" enthalten ist. Ist dies der Fall, wird automatisch der jeweilige Datensatz verworfen, wenn nicht, erfolgt eine weitere Verarbeitung des Datensatzes. Im übrigen wird permanent die Blackbox mit "Verweigerern" ergänzt.

Würde der Betroffene auch einer solchen Verfahrensweise widersprechen, wäre dem Willen nachzukommen; d. h. für den Preis eines möglichen erneuten Anschreibens - worauf der Betroffene hinzuweisen wäre - müßte von der Einstellung seiner Adresse in eine solche Blackbox abgesehen werden.

6.2 Einstellung von Telefon- und Vorlesungsverzeichnissen der Hoch- und Fachschulen im Internet

Den Universitäten des Landes zufolge gehört es heute zum "modernen Image" einer solchen Einrichtung, Telefon- und Vorlesungsverzeichnisse in das Internet einzustellen. Hierzu ist aus datenschutzrechtlicher Sicht folgendes anzumerken:

Die Verarbeitung personenbezogener Daten von Bediensteten der Universitäten und Fachschulen richtet sich nach § 29 Abs. 1 BbgDSG (Datenverarbeitung bei Dienst- und Arbeitsverhältnissen). Danach ist eine Datenübermittlung "an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat".

Daraus sind unterschiedliche Schlußfolgerungen in bezug auf die Erstellung und Nutzung eines Telefon- und/oder

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

Vorlesungsverzeichnisses einmal behördenintern und zum anderen außerhalb der Behörde zu ziehen. Von den vom Gesetzgeber eingeräumten Möglichkeiten (Darlegung eines rechtlichen Interesses, Erforderlichkeit bzw. Einwilligung) scheidet erstere aus.

Im Sinne der Erforderlichkeit bestehen selbstverständlich keine datenschutzrechtlichen Bedenken gegen die Erstellung eines Telefonverzeichnisses an einer öffentlichen Stelle in Papier- oder elektronischer Form zur internen Nutzung. Die Angehörigen einer Universität sind zum einen zur Wahrnehmung ihrer Tätigkeit darauf angewiesen, zum anderen hält sich die interne Verbreitung von Telefonnummern bzw. Telefonverzeichnissen im Rahmen der Zweckbestimmung des Dienst-/ Arbeitsverhältnisses. Ebenfalls vom Erforderlichkeitsgrundsatz ausgehend kommt für mich die Weitergabe dienstlicher Telefonverzeichnisse an andere öffentliche Stellen nur in Betracht, wenn mit diesen ein enger dienstlicher Kontakt besteht. Dabei spielt es nur eine untergeordnete Rolle, auf welchem Datenträger dies geschieht.

Auch im Rahmen eines veröffentlichten Vorlesungsverzeichnisses können Telefonnummern angegeben werden und zwar begrenzt auf Beschäftigte, die speziell bei ihrer Dienstausübung im Kontakt mit Bürgern stehen. Als unzulässig würde ich es jedoch erachten, wenn dies beispielsweise auch Mitarbeiter des Schreib- und anderer innerer Dienste, die in der Regel keine fernmündlichen Außenkontakte unterhalten, betreffen würde.

Da der Dienstverkehr - wie dargestellt - nur in einem eingeschränkten Umfang die Übermittlung von Beschäftigtendaten i. S. v. § 29 Abs. 1 BbgDSG erfordert, komme ich zu dem Schluß, daß die Eingabe entsprechender Daten (hier: Telefondaten) in ein öffentlich zugängliches Netz wie das Internet der Einwilligung des Betroffenen bedarf. Die Übermittlung kann im übrigen nicht mit dem Hinweis auf das Transparenzgebot der Verwaltung oder den Umstand, daß hier dienstliche Angelegenheiten der Betroffenen, nicht aber ihre Persönlichkeitssphäre berührt seien, gerechtfertigt werden. Zwar kann sich ein Bediensteter, dessen Daten im Rahmen seiner amtlichen Funktion verarbeitet werden müssen, als "Amtswalter" nicht auf sein Recht auf informationelle Selbstbestimmung berufen[89]. Aber er genießt selbstverständlich diesen Grundrechtsschutz, soweit die Datenverarbeitung dienstlich nicht erforderlich ist.
Eine derartige Differenzierung ist auch deshalb angezeigt, weil die Eingabe personenbezogener Daten in ein weltweit offenes Netz ein Zurverfügungstellen zum Abruf für jedermann i. S. v. § 3 Abs. 2 Nr. 4 BbgDSG darstellt, das Risiken (kommerzielle Nutzung z. B. bei Direktmarketing, Gefahr des unangeforderten Anschreibens und der Belästigung) verursacht, denen eine öffentliche Stelle ihre Angehörigen nicht ohne deren Einwilligung aussetzen darf. Die Einhaltung der Zweckbindung kann in solchen Verzeichnissen nicht sichergestellt werden. Es besteht zudem die Gefahr, daß die elektronisch verfügbaren Personendaten mit sonstigen elektronischen Daten, z. B. mit Adreßbuch- oder Telefonverzeichnissen oder Prominenten-, Presse- oder Wirtschaftsdatenbanken, kombiniert werden und so zur Erstellung von Persönlichkeitsprofilen genutzt werden können.

6.3 Staatsvertrag mit den evangelischen Landeskirchen Berlin-Brandenburg

[89] OVG Rheinland-Pfalz, DVBl. 1995, 629

Bereits in meinem 3. Tätigkeitsbericht[90] bin ich auf den Staatsvertrag mit den evangelischen Landeskirchen Berlin-Brandenburg (Staatskirchenvertrag) eingegangen und habe dort meiner Hoffnung Ausdruck verliehen, daß sich mit dem damals bevorstehenden Zuständigkeitswechsel von der Staatskanzlei zum Ministerium für Wissenschaft, Forschung und Kultur (MWFK) in dieser Angelegenheit auch eine konstruktive Zusammenarbeit zwischen Landesregierung und meiner Behörde ergeben könnte. Wie dem Staatskirchenvertrag bzw. dem Gesetz zum Inkrafttreten desselben[91] zu entnehmen, ist dies nicht in Erfüllung gegangen. Von dem zwischenzeitlich gesprächsweise erzielten Einvernehmen bei strittigen Punkten hat die Landesregierung bedauerlicherweise später wieder Abstand genommen. Eine Beteiligung meiner Behörde an den vorbereitenden Verhandlungen wegen der datenschutzrechtlichen Aspekte wurde im Gegensatz zur Praxis in anderen Bundesländern kategorisch abgelehnt.

90 s. unter 6.4

91 vom 10. März 1997, GVBl. I S. 4

Insbesondere Art. 22 Staatskirchenvertrag (Meldewesen) gibt Anlaß für unterschiedliche Auffassungen. Nach Abs. 1 dürfen aufgrund einer Generalklausel nach wie vor zwecks Ordnung und Pflege des kirchlichen Meldewesens den Kirchen die zur Erfüllung ihrer Aufgaben erforderlichen Daten aus dem Melderegister übermittelt werden. Dies läßt offen, was die Kirche für erforderlich hält. Auch die schließlich im Schlußprotokoll aufgenommene Klarstellung, daß die Übermittlung im Rahmen der melderechtlichen Bestimmungen des Landes erfolgt, ändert an dieser Situation nichts wesentliches. Im Gegenteil wird damit festgeschrieben, daß die in § 30 Abs. 2 BbgMeldeG aufgeführten Daten von Ehegatten, minderjährigen Kindern und Eltern minderjähriger Kinder der Mitglieder, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgemeinschaft angehören, übermittelt werden dürfen. Dies entspricht zwar dem traditionellen kirchlichen Verständnis der Registrierung ihrer Mitglieder im Familienverbund[92], hingegen wohl nicht dem Verständnis von Datenschutz der hiervon betroffenen Bürger. Erfreulicherweise war bei der Erörterung der Angelegenheit im Ausschuß für Wissenschaft, Forschung und Kultur die Rede davon, daß der Landesgesetzgeber frei sei, durch Änderung des Meldegesetzes den hierzu vorgetragenen Bedenken des Landesbeauftragten bei der bevorstehenden Novellierung des Meldegesetzes Rechnung zu tragen (s. unter 3.1.1).

Ebenfalls strittig geblieben ist die Regelung des Abs. 3 in Art. 22. Danach gewährleisten die Kirchen im kirchlichen Bereich den Datenschutz. Dies versteht sich aufgrund der Autonomie der Kirche von selbst. Festzuschreiben wäre gewesen, welche datenschutzrechtlichen Standards für Datenübermittlungen aus dem staatlichen Bereich einzuhalten sind. Hierfür maßgebend ist derzeit § 30 Abs. 3 BbgMeldeG. Danach trifft das Innenministerium - ohne Bezugnahme auf eine Rechtsgrundlage - die Feststellung, ob ausreichende Datenschutzmaßnahmen getroffen sind. Daher habe ich großen Wert darauf gelegt, Art. 22 Abs. 3 in Analogie zu Art. 23 des sachsenanhaltinischen Kirchenvertrages dahingehend abzuändern, daß im kirchlichen Bereich ein dem staatlichen Bereich gleichwertiger Datenschutz zu sichern ist. Zumindest diese Selbstverpflichtung der evangelischen Landeskirchen Berlin-Brandenburg wäre für alle Beteiligten akzeptabel gewesen.

6.4 Archive

6.4.1 Benutzungsordnung des Brandenburgischen Landeshauptarchivs

Das MWFK hat im Rahmen seiner Dienst- und Fachaufsicht gegenüber dem Brandenburgischen Landeshauptarchiv gem. § 17 Abs. 1 Ziff. 1 Brandenburgisches Archivgesetz (BbgArchivG)[93] dessen Benutzungsordnung (LHArchBO) zu genehmigen und bat mich hierzu um eine datenschutzrechtliche Stellungnahme. Der Entwurf glich inhaltlich weitgehend den Vorschriften in anderen Ländern.

Ich habe folgende ergänzende Vorschläge vorgebracht, die in die Benutzungsordnung des Landeshauptarchivs übernommen werden:

- Das Antragsformular ist um einen Hinweis auf Rechtsfolgen bei nicht vollständig ausgefüllten Anträgen (Nichtbearbeitung) sowie um die Angabe des Zwecks, weswegen der/die Antragstel-

92 Verordnung über die in das Gemeindeverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen i. d. Fass. vom 10. September 1993, Kirchl. ABl. Nr. 2/1994, S. 30

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

ler/in ggf. seinen/ihren Personalausweis bzw. Paß vorzulegen hat, zu ergänzen.

- Neben §§ 7 - 9 BbgArchivG sind auch die §§ 10 und 11 BbgArchivG als Entscheidungsgrundlage für Archivnutzung heranzuziehen.

- Ein Rechtsanspruch auf schriftliche Entscheidung im Falle der Ablehnung besteht nur, sofern dies beantragt wird.

- Die Antragsformulare sind nach Benutzung des gewünschten Archivgutes zu vernichten (Verhinderung von Benutzerprofilen).

- Der Antrag auf Nutzungsgenehmigung wird als Anhang Teil der Benutzerordnung.

6.4.2 Verwaltungsvorschriften zum Archivgesetz: Ein erster Entwurf

Bereits wiederholt[94] habe ich die Schaffung von Verwaltungsvorschriften gem. § 17 Abs. 2 BbgArchivG angemahnt, um so vor allem in den Kommunalarchiven eine möglichst einheitliche Nutzung von Archivgut zu gewährleisten.

Ein erster Entwurf erfüllt jedoch diese Erwartung nicht, da darin weitgehend lediglich Gesetzespassagen zitiert werden. Dies erscheint mir keineswegs eine ausreichende Hilfestellung für die Archivare zu sein, deren Problem ja gerade darin besteht, im konkreten Einzelfall eine pflichtgemäße ermessensfehlerfreie Entscheidung treffen zu müssen. Hierzu wäre es angezeigt, die Verfahrensweise allgemein mit Fallkonstellationen darzustellen sowie Begriffsdefinitionen zu geben.

Nachdem dieser Entwurf zunächst mit Archivfachleuten diskutiert werden soll, werde ich erneut Gelegenheit haben, zu einer überarbeiteten Fassung Stellung zu nehmen.

6.4.3 Genehmigungsverfahren zum Betreiben eines öffentlichen Archivs

An mich war die Bitte herangetragen worden, an der Erstellung eines Informationstechnik-Konzeptes (IT-Konzept) für die Stiftung Brandenburgische Gedenkstätten beratend mitzuwirken. Dieses sollte sowohl den administrativen Bereich als auch vorhandene Archivbestände abdecken.

Bei der Prüfung der rechtlichen Situation stellte sich folgendes Problem heraus: Der unmittelbare Geltungsbereich des Brandenburgischen Archivgesetzes läßt sich aus § 1 Abs. 1 i. V. m. § 2 Abs. 1 und 7 BbgArchivG herleiten. Als juristische Person des öffentlichen Rechts, die der Aufsicht des Landes Brandenburg untersteht, fällt die Stiftung Brandenburgische Gedenkstätten jedoch nicht hierunter. Für sie gelten die Bestimmungen in § 4 Abs. 4 BbgArchivG. Das bedeutet, daß sie nur dann ein eigenes öffentliches Archiv unterhalten kann, wenn sie den archivfachlichen Voraussetzungen i. S. v. § 2 Abs. 8 BbgArchivG genügt. Diese grundsätzliche Voraussetzung hat zunächst einmal die oberste Archivbehörde (MWFK) festzustellen. Bereits diesbezüglich tat sich das Ministerium sehr schwer.

Schließlich stimmte es meiner Auffassung jedoch zu. Verfahrensmäßig ist künftig vorgesehen, Archive juristischer Personen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen, auf Antrag - und nach Prüfung ob die archivfachlichen Voraussetzungen vorliegen - von der archivrechtlichen Anbietungspflicht gem. § 4 Abs. 1 BbgArchivG zu

---

[94] s. 3. Tätigkeitsbericht unter 6.6 und 4. Tätigkeitsbericht unter 6.1.3

befreien und sie in der Folge als Archiv gem. § 4 Abs. 4 BbgArchivG anzuerkennen. Den Bescheid erläßt die oberste Archivbehörde unter Einbeziehung des Brandenburgischen Landeshauptarchivs. Die nunmehr vorgesehene Verfahrensweise würde nicht nur für die Gedenkstätten, sondern auch für alle Archive staatlicher Stellen des Landes (u. a. Fontane-Archiv, Hoch- und Fachhochschulen, Forschungseinrichtungen) zutreffen.

7 Arbeit, Soziales, Gesundheit und Frauen

7.1 Arbeit

7.1.1 Anforderung von Arbeitnehmerverzeichnissen durch die Arbeitsämter

Eine Krankenkasse bat mich anläßlich von Übermittlungsersuchen verschiedener Arbeitsämter um Rat. Die Arbeitsämter forderten von der Krankenkasse Arbeitnehmerverzeichnisse einzelner Arbeitgeber, die sowohl frühere als auch derzeitig Beschäftigte enthalten sollten. Hintergrund dieser Maßnahme war, daß die Arbeitsämter bei Prüfungen zur Bekämpfung von illegaler Beschäftigung zeitnahe Informationen benötigen, weil ansonsten die Betroffenen häufig nicht mehr greifbar sind. Die Krankenkasse sah einerseits ihre gesetzliche und gesellschaftspolitische Verpflichtung, die für die Bekämpfung der illegalen Beschäftigung tätigen Verwaltungen bei dieser Aufgabe zu unterstützen. Andererseits hatte sie Bedenken, mit dem geforderten Arbeitnehmerverzeichnis überwiegend Daten über Versicherte zu offenbaren, die gerade nicht illegal beschäftigt sind.

Die Unterstützungspflicht der Krankenkassen zugunsten der Arbeitsämter bei der Bekämpfung von illegaler Beschäftigung ist in verschiedenen Vorschriften des Vierten (SGB IV)[95] und des Fünften (SGB V)[96] Buches des Sozialgesetzbuches geregelt. Im konkreten Fall dürfte es sich um ein durch die Bundesanstalt für Arbeit initiiertes Prüfungsverfahren nach § 107 SGB IV handeln, das sich auf die Einhaltung der §§ 99 und 102 bis 104 SGB IV bezieht, also wiederum verschiedenste Fälle erfaßt. Teilweise erscheint eine Beteiligung der Krankenkassen hierfür gar nicht notwendig, teilweise müßten sich Anfragen auf bestimmte Personen beschränken lassen, teilweise dürften Nachforschungen bei den Arbeitgebern vorrangig sein. Ich konnte der Krankenkasse daher nur raten, bei den Arbeitsämtern zu erfragen, aufgrund welcher Rechtsvorschrift diese welche Prüfung vornehmen wollten, welche Daten dabei jeweils von ihnen benötigt würden und wieso bzw. inwiefern ihre Erhebungsmöglichkeiten bei den Arbeitgebern zur Klärung der Angelegenheit nicht genügten.

Die Krankenkasse hat meine Stellungnahme erfreulicherweise zum Anlaß genommen, zwischenzeitlich so zu verfahren, daß sie den Arbeitsämtern keine Arbeitnehmerlisten überläßt, sondern Auskünfte nur in konkreten Einzelfällen, bei denen die Begründung des Arbeitsamtes für die jeweilige Übermittlungsbefugnis ausreichend erscheint, erteilt.

---

95 vom 23. Dezember 1976, BGBl. I S. 3845, zul. geänd. durch das WFG vom 25. September 1996, BGBl. I S. 1461

96 vom 20. Dezember 1988, BGBl. I S. 2477, zul. geänd. durch das UVEG vom 7. August 1996, BGBl. I S. 1254

7.2 Soziales

7.2.1 Gesetze und Verordnungen

7.2.1.1 Gesetzliche Unfallversicherung - SGB VII

Durch das Unfallversicherungseinordnungsgesetz (UVEG)[97] wurden Regelungen der Reichsversicherungsordnung (RVO)[98] abgelöst und das Recht der gesetzlichen Unfallversicherung als SGB VII in das Sozialgesetzbuch eingefügt. Datenschutzrechtlich relevante Bestimmungen finden sich vor allem im 7. und 8. Kapitel des SGB VII. Dort sind Regelungen zur Zusammenarbeit mit anderen Leistungsträgern, z. B. den Krankenkassen, sowie zu den Pflichten der Unternehmen in bezug auf die für ihre Unternehmen zuständigen Unfallversicherungsträger getroffen. Weitere spezielle datenschutzrechtliche Vorschriften sind insbesondere auf die starke Beteiligung von Ärzten an den Vorgängen im Unfallversicherungsrecht zurückzuführen. Auch für die Forschung zur Bekämpfung von Berufskrankheiten dürfen Patientendaten unter bestimmten Voraussetzungen übermittelt werden.

7.2.1.2 Reform des Sozialhilferechts

Das Bundessozialhilfegesetz (BSHG)[99] hat durch das Gesetz zur Reform des Sozialhilferechts[100] etliche Änderungen erfahren, die aus datenschutzrechtlicher Sicht nicht begrüßenswert erscheinen. Obwohl sich mit mir noch andere Datenschutzbeauftragte mit ihren Bedenken an die zuständigen Ministerien gewandt hatten, konnte lediglich erreicht werden, daß die gesetzliche Vermutung des Füreinandereinstehens von Verwandten oder Verschwägerten, die mit dem Hilfesuchenden in Haushaltsgemeinschaft leben, sowie von Personen, die in eheähnlicher Gesellschaft leben, nicht auf weitere Personen (z. B. Wohngemeinschaftsmitglieder) ausgedehnt wurde.

Die bisher lediglich verwaltungsintern bestehende Regelung, daß die Gerichte bei Räumungsklagen verpflichtet sind, dem örtlichen Sozialamt über diesen Umstand Mitteilung zu machen, hat nun immerhin eine gesetzliche Grundlage erhalten. Die datenschutzgerechteren Varianten, im Falle einer Räumungsklage dem Betroffenen von seiten des Gerichts ein übersichtliches Formular zur Beantragung von Sozialhilfe zu übersenden oder dem Beklagten zumindest die Möglichkeit eines Widerspruchsrechts einzuräumen, das eine Unterrichtung des Trägers der Sozialhilfe durch das Gericht unterbinden könnte, haben sich nicht durchsetzen können.

Nach § 117 Abs. 3 Satz 1 BSHG waren die Träger der Sozialhilfe bisher nur in Einzelfällen befugt, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Sozialhilfeempfängern z. B. bei anderen Stellen ihrer Verwaltung im Rahmen des Erforderlichen zu überprüfen. Durch die Reform wurde auch ein regelmäßiger automatisierter Datenabgleich ermöglicht, der nicht nur auf die Fälle abzielt, bei denen konkrete Anhaltspunkte für eine Überprüfung bestehen, sondern diesen eben generell zuläßt.

7.2.1.3 Brandenburgisches Sozialberufsgesetz

---

97 vom 7. August 1996, BGBl. I S. 1254

98 vom 15. Dezember 1924, RGBl. I S. 779

99 vom 23. März 1994, BGBl. I S. 646; zul. geänd. durch das Gesetz zur Reform des Sozialhilferechts vom 23. Juli 1996, BGBl. I S. 1088

100 vom 23. Juli 1996, BGBl. I S. 1088

Das Brandenburgische Sozialberufsgesetz (BbgSozBerG)[101] wurde durch das Erste Gesetz zur Änderung des Brandenburgischen Sozialberufsgesetzes[102] um bereichsspezifische Regelungen zum Datenschutz in § 8 a ergänzt. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF) hat in etlichen Punkten meine Anregungen berücksichtigt. Dabei hätte dem Erforderlichkeitsprinzip meiner Ansicht nach noch etwas besser Rechnung getragen werden können. Außerdem habe ich bedauert, daß nicht im Gesetz selbst, sondern lediglich in einer Rechtsverordnung bestimmt werden soll, welche Daten zu welchem Zweck erhoben und gespeichert und an welche Behörde übermittelt werden dürfen, in welchen Fällen Daten nach Zweckänderungen weiterverarbeitet werden dürfen und welche Auskünfte die Betroffenen zu erteilen haben.

7.2.2 Aktuelle Fälle

7.2.2.1 Anforderung von Krankenunterlagen durch Krankenkassen

In meinem 4. Tätigkeitsbericht[103] hatte ich darüber berichtet, daß eine Krankenkasse bei einem Krankenhaus Krankenunterlagen anfordere, um diese an den Medizinischen Dienst der Krankenkassen (MDK) weiterzusenden. Unter anderem hatte ich dort darauf hingewiesen, daß § 276 Abs. 2 SGB V[104] eine Datenübermittlung nur unmittelbar zwischen dem Leistungserbringer (Krankenhaus, Arzt, u. a.) und dem mit der Begutachtung beauftragten MDK vorschreibt. Das MASGF hat sich dieser Ansicht mit Erlaß vom 27. August 1996 angeschlossen. Der Erlaß wurde sowohl den Krankenkassen des Landes Brandenburg, dem MDK als auch den Krankenhäusern durch das Ministerium zur Kenntnis gegeben. Ich mußte jedoch feststellen, daß die Umsetzung den Krankenkassen immer wieder Schwierigkeiten bereitete (s. unter 7.2.2.4). Unterdessen hat mich das MASGF darüber informiert, daß der MDK seinen Spitzenverband (MDS) eingeschaltet und dieser sich gegen den Erlaß des Ministeriums gewendet habe.

Sowohl durch ein Krankenhaus als auch durch eine Petition einer Krankenversicherten bin ich darauf hingewiesen worden, daß die Krankenkassen zwischenzeitlich dazu übergehen, zur Umgehung des § 276 Abs. 2 SGB V die Anforderungen von Krankenunterlagen für den MDK auf Einwilligungserklärungen der Patienten zu stützen. Ich bin der Ansicht, daß der Gesetzgeber in § 276 Abs. 2 SGB V eine Entscheidung zur Übermittlung von Sozialdaten der Leistungserbringer an den mit einem Gutachten beauftragten MDK getroffen hat, die nicht zur Disposition der Beteiligten steht, mit Hilfe einer Einwilligungserklärung des Versicherten also nicht abgeändert werden kann. Dabei ist auch zu bedenken, daß der MDK im Gegensatz zur Krankenkasse bei den Leistungserbringern die fraglichen Daten erheben kann, ohne auf den umständlicheren Weg der Einholung einer Einverständniserklärung angewiesen zu sein. Angesichts seiner fachlichen Qualifikation kann er auch wesentlich exakter beurteilen, welche Daten für seine konkrete Aufgabe erforderlich sind. Die gesetzlich vorgeschriebene Verfahrensweise ist also einfacher, weniger zeitaufwendig und wird dem Prinzip der Erforderlichkeit besser gerecht als der von den Krankenkassen bevorzugte Weg. Hinzu kommt, daß eine Einwilligung in einen anderen als den gesetzlichen Übermittlungsweg schon deshalb kaum je wirksam sein könnte, weil der Betroffene in der Regel nicht darauf hingewiesen worden sein wird, daß das Gesetz in § 276 Abs. 2 SGB V einen anderen Weg für die Datenübermittlung vorsieht. Das hiesige Innenministerium - datenschutzrechtlich u. a. zuständig für den Datenschutz in

---

101 vom 10. Oktober 1996, GVBl. I S. 308

102 vom 26. Juni 1996, GVBl. I S. 202

103 s. unter 7.1.2.6

104 vom 20. Dezember 1988 , BGBl. I S. 2477, zul. geänd. d. das UVEG vom 7. August 1996, BGBl. I S. 1254

Krankenhäusern privater Träger - hat mir zwischenzeitlich mitgeteilt, daß es meine Ansicht teilt, daß die erforderlichen Unterlagen im Rahmen der Maßnahmen nach § 275 Abs. 1 - 3 SGB V gem. § 276 Abs. 2 SGB V unmittelbar an den MDK zu senden sind und dies auch nicht mit einer Einverständniserklärung des Betroffenen umgangen werden darf.

7.2.2.2 Einkommensnachweis selbständig Tätiger zur Bestimmung des Krankenkassenbeitrages

Ein Petent war von einer Krankenkasse aufgefordert worden, zur Ermittlung seines Einkommens als selbständig Tätiger beispielsweise eine Steuererklärung mit Steuerbescheid und Einkommenssteuerberechnung vorzulegen. Um festzustellen, welche Verfahrensweise sowohl datenschutzgerecht als auch praktikabel sein könnte, habe ich die Krankenkassen des Landes zu dieser Thematik befragt. Grundsätzlich erachteten diese eine Selbsterklärung für ausreichend. Sie haben darüber hinaus darauf hingewiesen, daß ein Nachweis mittels Steuerbescheid sich als unpraktikabel erwiesen habe, vor allem da dieser häufig erst sehr spät vorliege. In manchen Unterlagen sind auch personenbezogene Daten vorhanden, die für den Einkommensnachweis nicht relevant sind. Hier bleibt es dem Betroffenen überlassen, inwieweit er Schwärzungen vornimmt. Das MASGF besteht wegen § 4 Sozialversicherungs-Rechnungsverordnung[105] darauf, daß Belege selbst zu den Akten genommen werden und nicht nur eine entsprechende Notiz erfolgt.

Als datenschutzgerecht und praktikabel halte ich in Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz folgende Verfahren:

- die Abgabe einer vom Finanzamt bestätigten persönlichen Erklärung des Versicherten über das beitragsrelevante Einkommen oder

- die Abgabe einer vom Finanzamt bestätigten Erklärung/Bescheinigung eines Steuerberaters über dieses Einkommen.

Diesen Vorschlag habe ich auch dem MASGF unterbreitet, es hält diese Verfahrensweise ebenso für akzeptabel wie die Forderung nach der Vorlage einer Kopie z. B. des Einkommenssteuerbescheids, wenn der Betroffene darauf hingewiesen wurde, daß er nicht relevante Angaben unkenntlich machen kann. Das Ministerium hat allerdings darauf hingewiesen, daß steuerpflichtige Einkünfte und beitragspflichtige Einkommen i. S. d. Sozialgesetzbuch V erheblich voneinander abweichen können. Einheitliche, auch mit mir abgestimmte Festlegungen zur Ermittlung der Einkünfte von freiwillig versicherten Selbständigen würde auch das MASGF begrüßen. Da die Anforderungen an den Nachweis jedoch im pflichtgemäßen Ermessen der Krankenkassen stehen, müßten diese insoweit die Initiative ergreifen.
Dem Petenten konnte ich deshalb nur raten, sich mit seiner Krankenkasse darüber zu verständigen, welche Daten in den geforderten Unterlagen anonymisiert werden können und sich bei konkreten Streitpunkten ggf. nochmals an mich zu wenden.

7.2.2.3 Krankenkassenwechsel

Nach § 175 Abs. 1 Satz 1 SGB V haben die Versicherungspflichtigen nunmehr das Recht, sich eine Krankenkasse frei zu wählen. Diese Krankenkasse darf die Mitgliedschaft des Wahlberechtigten grundsätzlich nicht ablehnen. Will ein Versicherungspflichtiger seine Krankenkasse wechseln, so besteht unter den Voraussetzungen des § 175 Abs. 4 SGB V ein Kündigungsrecht. Nach Satz 3 dieser Vorschrift wird die Kündigung wirksam, wenn das Mitglied innerhalb der Kündigungsfrist eine Mitgliedschaft bei einer anderen Krankenkasse durch eine Mitgliedsbescheinigung nachweist.

---

[105] vom 3. August 1991, BGBl. I S. 809

Durch eine Petition wurde ich darauf aufmerksam gemacht, daß eine Krankenkasse in Kündigungsfällen die Arbeitgeber ihrer Versicherten aufforderte, ihr den Nachweis einer anderweitigen Mitgliedschaft in einer Krankenkasse vorzulegen, da andernfalls die Kündigung nicht wirksam würde. Ich habe diese Krankenkasse darauf hingewiesen, daß schon nach dem Wortlaut des § 175 Abs. 4 Satz 3 SGB V eine solche Anfrage beim Arbeitgeber nicht akzeptabel sei und sich auch aus einer anderen Vorschrift für den zugrundeliegenden Fall keine Befugnis für diesen ergebe, der Krankenkasse diese Unterlagen vorzulegen. Die betroffene Krankenkasse hat mitgeteilt, daß das Verfahren zwischenzeitlich abgeändert worden sei.

7.2.2.4 Formulare und Sozialdatenschutz

- Krankenkassen

Ein Krankenhaus hatte mir datenschutzrechtliche Bedenken gegen das Formular einer Krankenkasse für die Entscheidung über die Verlängerung einer stationären Behandlung vorgetragen. In dem Vordruck war beispielsweise nach dem bisherigen Krankheitsverlauf und bis in alle Einzelheiten nach dem Therapiekonzept gefragt worden. Nach längeren Recherchen stellte sich heraus, daß von der Krankenkasse ein Formular verwandt worden war, das seit Jahren keine Anwendung mehr finden sollte. Auch bei der Umsetzung des Erlasses des MASGF zur Datenerhebung durch Krankenkassen in Krankenhäusern (s. unter 7.2.2.1) waren teilweise noch monatelang veraltete Vordrucke im Umlauf. Die jeweils betroffenen Krankenkassen haben diese Vorfälle zum Anlaß genommen, ihr Personal darauf hinzuweisen, daß nur aktuelle Formulare zu verwenden und Altbestände zur Vernichtung abzugeben sind.

Ebenfalls als veraltet erwies sich ein Formblatt, mit dem eine Krankenkasse Angaben von Arbeitgebern erheben wollte, die eine Lohnfortzahlung ablehnten. Datenerhebungen zu dem Zweck zu klären, ob diese Weigerung unrechtmäßig ist und der krankengeldbezahlende Sozialversicherungsträger demgemäß einen Anspruch aus dem übergegangenen Entgeltfortzahlungsanspruch nach § 115 SGB X[106] geltend machen kann, sind nicht im an sich abschließenden Katalog der Datenerhebungen der Krankenkassen nach § 284 Abs. 1 SGB V[107] erwähnt und daher streng genommen nicht zulässig. Sofern eine Einwilligung des Betroffenen oder die Voraussetzungen des § 67 a Abs. 2 Nr. 2 SGB X vorliegen, habe ich mich angesichts der unbefriedigenden Situation in dem geschilderten Fall dazu entschieden, diese Datenerhebungen der Krankenkassen zu anderen als den unter § 284 Abs. 1 SGB V genannten Zwecken nicht zu beanstanden. Ich habe jedoch verlangt, daß auf die Freiwilligkeit der Auskunftserteilung zu personenbezogenen Daten hinzuweisen ist. Dem ist die Krankenkasse nachgekommen.

Derzeit aktuell ist die Diskussion insbesondere mit Krankenkassen um die Formulierung von Einwilligungserklärungen bzw. Erklärungen zur Entbindung von der ärztlichen Schweigepflicht. Dabei sind datenschutzrechtliche Hinweise häufig nur im Ansatz vorhanden. Auch der Zweck der Datenerhebungen oder Datenübermittlungen wird kaum hinreichend bestimmt angegeben. Der Personenkreis, der aufgrund der Erklärung berechtigt sein soll, der Stelle, die dem Betroffenen das Formular vorlegt, Auskünfte u. ä zu erteilen, wird häufig so pauschal beschrieben, daß sich niemand völlig sicher sein kann, ob auch er aufgrund der Erklärung berechtigt sein soll, Auskünfte zu erteilen. Eine Verweigerung/Beschränkung der Einwilligungserklärung ist nicht vorgesehen, ebenso fehlt der Hinweis auf die jederzeit bestehende Möglichkeit, die Erklärung zu widerrufen. Darüber hinaus habe ich jeweils darum gebeten zu prüfen, ob eine Einwilligungserklärung tatsächlich notwendig ist. In vielen Fällen besteht bereits eine gesetzliche Ermächtigungsgrundlage für eine

---

106 BGBl. III 86-7-3

107 vom 20. Dezember 1988, BGBl. I S. 2477, zul. geänd. d. das UVEG vom 7. August 1996, BGBl. I S. 1254

Datenerhebung bzw. -übermittlung, oder das Gesetz schreibt einen Weg vor, der auch nicht mittels einer Einwilligungserklärung umgangen werden darf (vgl. unter 7.2.2.1).

- Sozialhilfeträger

Aufgrund einer Petition habe ich mich damit beschäftigt, ob das Prinzip der Erforderlichkeit noch gewahrt ist, wenn personenbezogene Daten, die ein Sozialamt gerade erst wenige Wochen zuvor von dem Betroffenen erhoben hatte, nochmals abgefragt werden. Für den Sozialhilfeempfänger könnte es eine Vereinfachung darstellen, wenn ihm die Angabe: "Keine Änderungen seit dem letzten Antrag (vom .....)" gestattet würde.

Vielfach ist in Formularen eine Zustimmung zur Einholung von Bankauskünften vorgesehen. Nach dem Urteil des Hessischen VGH[108] stellt die Zustimmung zur Einholung von Bankauskünften ohne Vorliegen eines konkreten Anhaltspunktes eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers dar und ist i. S. v. § 60 Abs. 1 Nr. 1 SGB I[109] nicht erforderlich. Die Sozialleistungsträger haben mitgeteilt, nur in besonderen Einzelfällen von den Zustimmungen zu Bankauskünften Gebrauch zu machen. Sofern Anhaltspunkte dafür sprechen, daß die Angaben des Antragstellers bzw. die von ihm vorgelegten Nachweise nicht vollständig und/oder nicht wahrheitsgemäß sind, ist gegen das Verlangen, einer Bankauskunft zuzustimmen, grundsätzlich nichts einzuwenden. Dem Betroffenen ist aber zu erläutern, warum in seinem Fall ausnahmsweise eine Bankauskunft notwendig erscheint, ob Alternativen dazu denkbar sind und welche Voraussetzungen und Folgen diese haben. Ist die Einholung einer Bankauskunft formularmäßig vorgesehen, so muß sie als Alternative zum Ankreuzen ausgestaltet sein, um zu gewährleisten, daß nicht in jedem Fall vorsorglich eine solche Zustimmungserklärung vom Betroffenen gefordert wird.

Insgesamt war auch bei diesen Fragebögen darauf hinzuweisen, daß Ausführungen über datenschutzrechtlich relevante Bestimmungen an den Anfang des Fragebogens zu stellen und möglichst durch Fettdruck hervorzuheben sind.

Die Anforderungen des § 67 a Abs. 3 SGB X

- Angabe des Erhebungszwecks,
- Mitteilung, ob eine Auskunftspflicht oder -obliegenheit besteht oder die Auskunft freiwillig ist,
- Mitteilung der Rechtsvorschriften (nebst Fundstelle im Gesetzblatt),
- Mitteilung evtl. nachteiliger Folgen einer Auskunftsverweigerung

bei einer Datenerhebung beim/mit Hilfe des Betroffenen waren allenfalls ansatzweise erfüllt. Insbesondere waren nicht alle Daten, die lediglich freiwillig erhoben werden können, in den Formularen ausdrücklich gekennzeichnet.

Aufgrund eines Berichts, den ich dem MASGF nach einer Umfrage im Lande über die Gewährung von Sozialhilfe in Form von Sachleistungen auf dessen Bitte übermittelt hatte, hat das Ministerium gegenüber den Sozialamtsleitern in einer Besprechung zum Ausdruck gebracht, daß grundsätzlich die Gewährung von Geldleistungen Vorrang gegenüber der Sachleistungsgewährung habe und beispielsweise Gutscheine nur in Ausnahmefällen an Stelle von Geldleistungen treten sollten. Sofern Gutscheine Daten von Hilfeempfängern enthielten, wurde empfohlen, diese zu verschlüsseln.

---

[108] vom 2. Februar 1995, RDV 1995 S. 175

[109] vom 11. Dezember 1975, BGBl. I S. 3015, zul. geänd. d. das UVEG vom 7. August 1996, BGBl. I S. 1254

Bei allen Überlegungen hierzu ist davon auszugehen, daß bereits die Verwendung eines von einer Behörde ausgestellten Gutscheines jeden durchschnittlich informierten Bürger darauf schließen läßt, daß der Verwender Sozialhilfeempfänger sein muß. Deswegen ist im Interesse des Datenschutzes, aber auch im Hinblick auf die Wahrung der Würde des einzelnen bei der Gewährung von Sozialhilfe der Vorrang der Geldleistung zu beachten und nur in begründeten Einzelfällen oder falls der Betreffende dies von sich aus wünscht, eine Sachleistungsgewährung in Betracht zu ziehen.

In Zweifelsfällen kann möglicherweise zunächst versucht werden, über die Pflicht zur Vorlage einer Quittung einem Mißbrauch zu begegnen. Diese sollte allenfalls vorübergehend, beispielsweise für die Dauer der halbjährigen Gewährleistungsfrist, bei den Akten verwahrt werden, weil sich anderenfalls anhand der Quittungen ein Bild über das allgemeine Konsumverhalten (Einkaufsort, bevorzugtes Geschäft) des Betroffenen für das Sozialamt ergeben würde.

Auch in diesem Fall ist dem Betroffenen zu erläutern, warum ausnahmsweise eine Sachleistung in Betracht kommen soll. Auf Alternativen, deren Voraussetzungen und Folgen ihm darzulegen sind, ist er hinzuweisen. In den Ausnahmefällen, in denen Sachleistungen z. B. mittels eines Gutscheines gewährt werden, dürfen in diesem nur Sozialdaten enthalten sein, die unverzichtbar sind für den Zweck. In der Regel ist die Angabe von Name, Anschrift und Geburtsdatum des Betroffenen nicht erforderlich. Auch ein Hinweis auf das konkret auszahlende Amt läßt sich, wie in anderen Bundesländern praktiziert, vermeiden. Wesentlich ist eine solche Ausgestaltung der Gutscheine auch im Hinblick darauf, daß von den Sozialämtern nicht sichergestellt werden kann, daß sich Kaufleute für ihre Unterlagen Kopien der Gutscheine machen, was zur Folge hat, daß Sozialdaten sich unkontrolliert in den Händen privater Personen befinden.

Trotz seiner generellen Unterstützung meiner Behörde in dieser Angelegenheit mußte das MASGF sich letztlich auf den Standpunkt zurückziehen, daß es sich bei der Durchsetzung des Bundessozialhilfegesetzes überwiegend um eine Selbstverwaltungsangelegenheit der Landkreise und kreisfreien Städte handele und die Hinweise des Ministeriums zur Ausgestaltung von Formularen in der Sozialhilfe nur empfehlenden Charakter haben können.

7.2.2.5 Durchführung des Schwerbehindertengesetzes

Nach § 6 Abs. 1 Ausweisverordnung Schwerbehindertengesetz (SchwbAwV)[110] ist neben dem Gültigkeitsbeginn auf der Rückseite des Ausweises auch ggf. eine Änderung des Grades der Behinderung zu vermerken. Über einen längeren Zeitraum betrachtet kann so der Verlauf der Schwerbehinderung von jeder Stelle, der der Ausweis vorgelegt wird, nachverfolgt werden. Meine diesbezüglichen Bedenken habe ich sowohl dem Landesamt für Soziales und Versorgung als auch dem MASGF mitgeteilt. Letzteres hat sich auf Anfrage des Landesversorgungsamtes meiner Ansicht angeschlossen und diesem empfohlen, in den Fällen, in denen sich u. a. durch Neufeststellungen nach dem Schwerbehindertengesetz (SchwbG)[111] Veränderungen beim Grad der Behinderung ergeben und weitere Eintragungen erforderlich werden, die Schwerbehinderten gleichzeitig mit der Bescheiderteilung zu befragen, ob diese zusätzlichen Eintragungen im bereits vorhandenen Schwerbehindertenausweis vorgenommen werden können oder ob die Neuausstellung eines Schwerbehindertenausweises ohne die überholten Eintragungen gewünscht wird.

7.2.2.6 Erhebungsbogen zur Ermittlung Behinderter

Durch eine Petition wurde ich auf schon formal nicht datenschutzgerechte Erhebungsbögen zur Ermittlung des

---

110 vom 15. Mai 1981, BGBl. I S. 431, i. d. Fass. vom 25. Juli 1991, BGBl. I S. 1739

111 i. d. Fass. vom 26. August 1986, BGBl. I S. 1421, ber. S. 1550

Betreuungsbedarfs bei Behinderten aufmerksam gemacht. Das Landessozialamt, das diese Formulare verwendet hatte, bat mich daraufhin um Unterstützung bei deren Überarbeitung. Die mit mir abgestimmten Fragebögen sollen nun von den Sozialämtern einheitlich verwandt werden.

Das Landessozialamt übernahm in den Fragebögen im wesentlichen die Vorschläge, die ich ihm zu Datenschutzklauseln gemacht hatte.

Ursprünglich hatte das Landessozialamt geplant, in allen Fällen den Landesarzt i. S. v. § 126 a Abs. 1 BSHG[112] i. V. m. § 10 Gesetz zur Ausführung des Bundessozialhilfegesetzes (AG-BSHG) [113] einzuschalten. Dies erscheint mir datenschutzrechtlich nicht unproblematisch. § 126 a Abs. 1 BSHG schreibt die Bestellung von Landesärzten vor. Nach dem Wortlaut sind also mehrere Landesärzte zu bestellen, weil ein Arzt allein nicht die ganze Breite des Fachwissens über die verschiedenen Behinderungsarten (körperlich, geistig und seelisch) alleine abdecken könnte. § 10 AG-BSHG sieht demgegenüber nur die Bestellung eines Landesarztes vor. Dies hat zur Folge, daß dieser ggf. Fachärzte als Gutachter hinzuziehen muß, wenn er selbst für eine Behinderungsart die notwendige Fachkompetenz nicht besitzt. In einem solchen Fall, in dem der Landesarzt letztlich selbst keine eigene Begutachtung vornehmen kann, erscheint es aus datenschutzrechtlicher Sicht besonders bedenklich, ihn in das Verfahren einzubeziehen, weil damit unnötigerweise besonders heikle personenbezogene Daten ihm gegenüber offenbart werden. Ich habe weiter darauf hingewiesen, daß aus dem Bundessozialhilfegesetz hervorgeht, daß der Bundesgesetzgeber nicht an eine generelle Beteiligung der Landesärzte gedacht hatte, zumal deren Empfehlung für die entscheidungsbefugten Sozialhilfeträger nicht bindend ist.

Das MASGF hat auf meine Bedenken hin mitgeteilt, daß es nunmehr vorgesehen sei, nur in einzelnen Fällen den Landesarzt einzuschalten. Für den Fall, daß eine Behinderung betroffen sei, für deren Beurteilung die fachliche Kompetenz des Landesarztes fehlt, könne sich der Landesarzt weiterer festgelegter Fachärzte unter Beachtung der datenschutzrechtlichen Bestimmungen bedienen.

Die jetzt vorgestellte Verfahrensweise ist wesentlich datenschutzgerechter als die anfänglich vorgesehene Lösung. Allen meinen Bedenken wird sie jedoch immer noch nicht gerecht.

7.2.2.7 Offenbarung von Sozialhilfeempfängereigenschaften an die Schule

Ein Petent trug mir vor, daß er als einmalige Leistung nach dem Bundessozialhilfegesetz die Bezahlung eines Schulausfluges für sein Kind beantragt habe. Die Zahlungsfrist endete wenige Tage nach der Vorsprache des Sozialhilfeempfängers beim Sozialamt. Das Sozialamt ließ ihn deshalb eine Erklärung unterschreiben, daß die Klassenlehrerin seines Kindes berechtigt sei, den Unkostenbeitrag für die Klassenfahrt in Empfang zu nehmen. Dem Sozialamt schien diese Vorgehensweise die geeignetste, da der Sozialhilfeempfänger hoch verschuldet war, die Zeit drängte und die betroffene Familie außerhalb wohnte. Die Gründe für seine Vorgehensweise erläuterte das Sozialamt dem Betroffenen nicht. Er sah sich faktisch gezwungen, die Vollmacht zu unterschreiben, um seinem Kind die Klassenfahrt zu ermöglichen.

Nach § 35 Abs. 1 Satz 1 SGB I hat jeder Anspruch darauf, daß seine personenbezogenen Daten von den Leistungsträgern als

---

112 i. d. Fass. vom 23. März 1994, BGBl. I S. 646, ber. S. 2975, zul. geänd. d. das Gesetz zur Reform d. Sozialhilferechts vom 23. Juli 1996, BGBl. I S. 1088

113 vom 24. Juli 1991, GVBl. I S. 318, zul. geänd. d. das UGPflegeVG vom 27. Juni 1995, GVBl. I S. 130

Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Die Tatsache des Bezugs von Sozialhilfe sowie bereits des Bezuges von Sozialleistungen allgemein gehört zu den personenbezogenen Daten. Das Sozialamt hat sich angesichts der Sachlage dafür entschieden, mit Zustimmung des Betroffenen die Zahlung direkt an die Schule vorzunehmen, was eine zulässige Offenbarung seiner Sozialhilfeeigenschaft an die Klassenlehrerin bedeutet hätte. Eine Einverständniserklärung des Hilfesuchenden setzt jedoch voraus, daß dieser auf alternative Vorgehensweisen und deren Vor- und Nachteile hingewiesen wurde und sich selbst aufgrund dieser Information frei entscheiden konnte. Dieses Entscheidungsrecht hat das Sozialamt im vorliegenden Fall dem Betroffenen nicht zugestanden. Der Petent sah sich faktisch gezwungen, den ihm allein aufgezeigten Lösungsweg des Sozialamtes zu unterstützen und damit ein personenbezogenes Datum zu offenbaren.

Zur Bezahlung der einmaligen Hilfe für den Schulausflug unmittelbar an die Klassenlehrerin hat das Sozialamt noch bemerkt, daß diese Mitarbeiterin ja auch im öffentlichen Dienst tätig und vom Schulträger auf ihre Schweigepflicht hingewiesen worden sei. Eine solche Argumentation würde einen freien Datenaustausch zwischen den Behörden generell für zulässig erachten. Das Sozialamt, als Teil einer Gebietskörperschaft, ist nach § 67 Abs. 9 Satz 3 SGB X aber selbst im Verhältnis zu den anderen Funktionseinheiten der Gemeinde eine eigene datenverarbeitende Stelle, die nur unter bestimmten Voraussetzungen personenbezogene Daten an andere Stellen übermitteln darf. Den differenzierenden Regelungen der Datenschutzgesetze und dem besonderen Schutz des Sozialdatengeheimnisses wurde diese Argumentation des Sozialamtes daher nicht gerecht.

7.2.2.8 Offenbarung von Sozialdaten auf Überweisungsträgern

Bereits in meinem 4. Tätigkeitsbericht[114] habe ich darüber berichtet, daß ich mich bei verschiedenen Ministerien im Land Brandenburg dafür eingesetzt habe, daß das Urteil des Bundesverwaltungsgerichts vom 23. Juni 1994[115] eingehalten wird, wonach es unzulässig ist, bei der Auszahlung von Sozialhilfe die Überweisungsträger generell ohne Zustimmung des Sozialhilfeempfängers mit dem Vermerk "Sozialleistung" zu versehen.

Das MASGF hat zwischenzeitlich mitgeteilt, daß eine Rückfrage bei allen Sozialamtsleitern und kommunalen Spitzenverbänden ergeben habe, daß die Sozialämter das oben angesprochene Urteil kennen und beachten.

Das Ministerium für Bildung, Jugend und Sport hat mir mitgeteilt, daß es sich auf meine Anregung hin auch im Bereich der Pflegefamilien dafür eingesetzt habe, daß die Überweisungsträger nicht mehr den Namen des Pflegekindes oder einen Hinweis auf ein Pflegeverhältnis enthielten, sondern neutral gefaßt würden.

7.2.3 Kontrolle der TK-Anlage in einem Amt für Soziales und Versorgung

Bereits im Jahre 1995 wandten sich Mitarbeiter des Amtes für Soziales und Versorgung Frankfurt (Oder) mit der Bitte an mich, die Dienstvereinbarung über die Nutzung der internen Telekommunikationsanlage (TK-Anlage) datenschutzrechtlich zu prüfen. Den Anlaß dazu gaben Listen mit den ausgedruckten Verbindungsdaten von Dienst- und Privatgesprächen der Mitarbeiter des Amtes, die die Amtsleiterin mit der Bitte in Umlauf gegeben hatte, die privaten Gespräche für Abrechnungszwecke zu markieren. Da meine mehrfachen schriftlichen Bemühungen zur Behebung der datenschutzrechtlichen Mängel in der Dienstvereinbarung erfolglos verliefen und das von mir angebotene persönliche Beratungsgespräch dazu nicht in Anspruch genommen wurde, nahm ich im Oktober 1996 eine datenschutzrechtliche

---

114 s. unter 7.1.2.1

115 Az.: 5 C 16.92, RDV 1995 S. 28

Überprüfung der internen TK-Anlage vor.

Die Auswertung der Kontrolle führte neben zahlreichen Mängelfeststellungen gem. § 25 Abs. 1 Ziff. 1 BbgDSG zur Beanstandung folgender Verstöße gegen datenschutzrechtliche Vorschriften gegenüber dem MASGF:

1. Die am Vermittlungsplatz tätigen Mitarbeiterinnen machten sich in einer Kladde Notizen über vermittelte Telefongespräche. Es gab keine Festlegungen (z. B. in einer Dienstanweisung), wie mit diesen Aufzeichnungen umzugehen ist, obwohl diese über mehrere Monate, ja sogar Jahre vorgehalten wurden und Auskunft darüber geben, wer wann mit wem dienstlich oder privat telefoniert hat. Die vorliegenden Aufzeichnungen wurden auf meine Beanstandung hin vernichtet. In Zukunft wird auf deren Anfertigung verzichtet.

2. Während meines Kontrollbesuches wurde mir der Entwurf einer neuen Dienstvereinbarung zur Nutzung der internen TK-Anlage vorgelegt. Darin äußerten aber der Personalrat und die Dienststellenleitung lediglich ihre unterschiedlichen Auffassungen beim Gebührennachweis für Privatgespräche und bei der stichprobenartigen Überprüfung dienstlicher Gespräche, wobei beide Seiten Lösungen vorschlugen, die mit der vorliegenden Gebührensoftware nicht realisierbar waren.

Inzwischen wurde mir der Entwurf einer noch nicht bestätigten überarbeiteten Fassung übergeben, der sowohl den berechtigten Interessen des Arbeitgebers auf Kostenkontrolle als auch den Grundrechten der Beschäftigten weitestgehend gerecht wird.

3. Die Aufzeichnung der Verbindungsdaten aller abgehenden dienstlichen und privaten Telefongespräche durch die Gebührendatenverarbeitung entsprach nicht den Bestimmungen (u. a. in Pkt. 3.1.3) der allgemeinen Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher TK-Anlagen für die Verwaltung des Landes Brandenburg (DAV)[116]. Diese geht von dem datenschutzrechtlichen Grundsatz der Erforderlichkeit aus; insoweit ist die Speicherung der Verbindungsdaten aller Gespräche für eine Gebührenabrechnung auch unzulässig (s. unter 1.2).

Im Verlaufe einer Beratung mit Vertretern der Herstellerfirma und des Amtes für Soziales und Versorgung stellte sich heraus, daß die Gebührendatenverarbeitung der vorliegenden TK-Anlage die Anforderungen der DAV nicht erfüllen kann. Dies ist u. a. auch darauf zurückzuführen, daß diese Anforderungen vom Landesbauamt Frankfurt (Oder) als Auftraggeber zur Errichtung der TK-Anlage während der Ausschreibung gar nicht erst gestellt wurden. Denn die Herstellerfirma vertrat beim Angebot der TK-Anlage die irrige Meinung, bei der Umsetzung des Datenschutzes im Rahmen ihrer TK-Anlagen seien die einschlägigen Bestimmungen des Landes Nordrhein-Westfalen zu befolgen, die vom Land Brandenburg angeblich vollinhaltlich übernommen worden seien.

Ungeachtet der Verantwortlichkeiten lassen sich nach meiner Einschätzung die Mängel bereits durch geringfügige Veränderung der Software zur Gebührendatenverarbeitung beheben. Die Vertreter der Herstellerfirma haben zugesagt, diese Problematik mit ihren zuständigen Stellen zu beraten. Eine Rückmeldung steht noch aus.

4. Mit der derzeitigen Zugriffsmöglichkeit auf die auch zur Verhaltens- und Leistungskontrolle sehr geeigneten sowie sensiblen Datenbestände des Gebührencomputers durch einzelne Personen (Systemverwalter, Wartungspersonal usw.) waren datenschutzrechtliche Grundsätze nicht gewahrt. Inzwischen erfolgt der Zugriff auf den Gebührencomputer nach

[116] s. Runderlaß des Ministeriums der Finanzen Nr. 17-01340-180/93 vom 30. November 1993, ABl. S. 1775

dem Vier-Augen-Prinzip unter Beteiligung eines Mitgliedes des Personalrates oder des behördlichen Datenschutzbeauftragten.

5. Die vertraglichen Regelungen zur Fernwartung der TK-Anlage durch die Herstellerfirma enthielt keine ausreichenden Festlegungen zu den notwendigen technischen und organisatorischen Maßnahmen im Rahmen der Fernwartung. Ich habe verlangt, daß bis zur Erfüllung der folgenden Mindestforderungen von einer Fernwartung der TK-Anlage abzusehen ist:

- Das Modem wird nur für den Zeitpunkt der Fernwartung aktiviert und der Verbindungsaufbau erfolgt stets durch den Kunden (Rückrufverfahren).

- Die Veränderung von Leistungsmerkmalen der TK-Anlage ist nur bei gleichzeitiger Protokollierung beim Auftraggeber zulässig.

- Das Überspielen von Softwareänderungen im Rahmen der Fernwartung wird ausgeschlossen.

- Durch geeignete technisch-organisatorische Maßnahmen ist zu sichern, daß während der Wartungsarbeiten kein Zugriff auf Daten des Gebührencomputers erfolgen kann.

Neben den genannten Beanstandungen bemängelte ich u. a. das Fehlen der Dateibeschreibungen für die Dateien zur Gebührendatenverarbeitung gem. § 8 BbgDSG. Diese Unterlagen konnte das Amt für Soziales und Versorgung nicht erstellen, da sich die Lieferfirma u. a. aus "betrieblich-datenschutzrechtlichen Gründen" weigerte, dem Auftragnehmer eine Übersicht der Dateien zu übergeben, in denen personenbezogene Daten zur Gebührenverarbeitung gespeichert werden. Diese Begründung ist aber absurd. Eine Dateibeschreibung - bestehend aus den Angaben der für eine Datenverarbeitung vorgesehenen Datenfelder - beinhaltet gar keine personenbezogenen Daten.

Hier wird seitens des Auftragnehmers der Datenschutz als vorgeschobenes Argument mißbraucht. Dies kann durch den Auftraggeber nicht geduldet werden. Er muß für seine Belange wissen, welche personenbezogene Daten in seinen Projekten gespeichert und in welcher Form verarbeitet werden, um seinen Pflichten entsprechend dem Brandenburgischen Datenschutzgesetz nachkommen zu können.

Bisher wurden meine Beanstandungen seitens des Amtes für Soziales und Arbeit noch nicht abschließend bearbeitet. Ich werde weiterhin auf einer Anpassung der Gebührendatenverarbeitung an die Vorschriften der Dienstanschlußvorschrift bestehen.

7.3 Gesundheit

7.3.1 Gesetze, Verordnungen und Erlasse

7.3.1.1 Staatsvertrag über ein Gemeinsames Krebsregister der neuen Bundesländer und Berlin

In meinem 4. Tätigkeitsbericht[117] hatte ich ausführlich begründet, weshalb ich die vom MASGF befürwortete Lösung der Fortführung des Gemeinsamen Krebsregisters (GKR) in Berlin auf der Grundlage eines Verwaltungsabkommens mit Ausführungsgesetzen der einzelnen Länder ablehne und einen Staatsvertrag hierzu für zwingend erforderlich halte. Nachdem auch verschiedene Ministerien anderer Länder Bedenken gegen diese befürwortete Lösung äußerten, fiel zu guter Letzt doch noch eine Entscheidung zugunsten der Staatsvertrags-Lösung. Hierüber wurde ich zunächst von der Thüringer Datenschutzbeauftragten informiert.

Auf meinen Vorschlag hin fand im Dezember 1996 eine Besprechung der Datenschutzbeauftragten mit den Vertretern der Ministerien über den Entwurf statt. Dabei wurde auf Wunsch der Datenschutzbeauftragten eine Klausel aufgenommen, die dafür sorgt, daß die Regelungen des Krebsregistergesetzes (KRG), das gem. § 14 Abs. 2 zum 31.12.1999 außer Kraft treten wird, im wesentlichen weitergelten. Die Forderung, eine Datenschutzkontrolle im GKR auch durch andere Datenschutzbeauftragte als denjenigen des Sitzlandes Berlin im Staatsvertrag zu regeln, wurde von der Berliner Senatsverwaltung unter Hinweis auf das Zusammenarbeitsgebot des § 24 Abs. 4 Berliner Datenschutzgesetz[118] abgelehnt. Der Berliner Datenschutzbeauftragte hat mitgeteilt, daß diese Vorschrift ggf. dahingehend ausgelegt werde, daß die Zusammenarbeit auch eine gemeinsame Prüfung mit Kollegen aus anderen beteiligten Bundesländern ermögliche. Offen ist derzeit, ob für den Fall der Kündigung des Staatsvertrages durch ein Land ein Bedarf besteht, den aus dem betreffenden Land stammenden Datensatz aus dem GKR herauszulösen und eigenständig zu nützen.

7.3.1.2 Seuchenmeldeverordnung

In der Verordnung über die Erweiterung der Meldepflicht für übertragbare Krankheiten (SeuchMV)[119] sind trotz mehrfacher Erörterung der Problematik meine Bedenken gegen die Auffangklausel in § 2 Nr. 2 SeuchMV, die datenschutzrechtlich zu weit und zu unscharf ist[120], vom MASGF nicht berücksichtigt worden. Das Ministerium hat sich dabei auf ein Arbeitspapier zur Novellierung des Bundesseuchengesetzes[121] aus dem Jahre 1994 berufen, von dem mir nicht absehbar erscheint, ob sich diese Regelung, die ein Vorgehen gegen neu auftretende schwere Infektionskrankheiten ermöglichen soll, aber auch Meldungen wegen leichtester Formen zuläßt und deshalb unverhältnismäßig erscheint, durchsetzen wird.

7.3.1.3 Kinder- und Jugend-Gesundheitsdienst-Verordnung nebst einheitlichen Dokumentationsbögen zur Schulreihenuntersuchung

---

117 s. unter 7.3.1.3

118 i. d. Fass. vom 17. Dezember 1990, GVBl. 1991 S. 16, 54, zul. geänd. d. Ges. vom 17. Oktober 1994, GVBl. 1994 S. 428

119 vom 8. Oktober 1996, GVBl. II S. 766

120 s. 4. Tätigkeitsbericht unter 7.2.2.1

121 i. d. Fass. vom 18. Dezember 1979, BGBl. I S. 2262, zul. geänd. d. Ges. vom 25. Juli 1996, BGBl. I. S. 1118

Über die Problematik verschiedener Elternfragebögen zur Schulreihenuntersuchung, die im Land Brandenburg Verwendung fanden, habe ich mich ausführlich in früheren Tätigkeitsberichten[122] geäußert. Nunmehr wurde mir vom MASGF eine Verordnung über die Aufgaben des Kinder- und Jugend-Gesundheitsdienstes der Gesundheitsämter im Land Brandenburg (KJGDV)[123] zur Stellungnahme vorgelegt. Diese Verordnung ist zwischenzeitlich verabschiedet worden und schreibt in § 3 Abs. 2 die einheitliche Verwendung eines als Anlage beigefügten ärztlichen Dokumentationsbogens und eines ärztlichen Anamnesebogens vor. Letzterer ist bis auf die Reihenfolge der Fragen im Grunde identisch mit dem Elternfragebogen zur Einschulungsuntersuchung, der meinem 4. Tätigkeitsbericht zugrunde lag. Den bereits damals nicht berücksichtigten Bedenken wurde durch das MASGF weiterhin nicht Rechnung getragen. Vielmehr entschied sich das Ministerium, das diese Fragen erst als freiwillige Auskünfte handhaben wollte, letztlich dafür, daß die betroffenen Daten für die Gesundheitsämter erforderlich seien und benannte den Elternfragebogen in "Ärztlichen Anamnesebogen" um.

Einige aus datenschutzrechtlicher Sicht erfreuliche Änderungen erfuhr hingegen der ärztliche Dokumentationsbogen. Er enthält keinerlei Hinweis mehr auf die Staatsbürgerschaft der untersuchten Kinder bzw. Jugendlichen. Darüber hinaus wird nicht die Gemeindekennziffer des Wohnortes des Betroffenen, sondern der Einrichtung, die er besucht, angegeben.

Trotz meines Hinweises, daß die Dokumentationen in Ziff. 17 bis 19 Fragen zur Persönlichkeitssphäre Dritter betreffen, die gem. § 45 Abs. 2 Satz 3 BbgSchulG nicht gestellt werden dürften, wurden diese Fragen beibehalten. Im einzelnen handelt es sich dabei um die Anzahl der im Haushalt lebenden Personen, getrennt nach Kindern und Erwachsenen, wodurch beispielsweise Alleinerziehende oder Einzelkinder herausgefiltert werden können. Die weiteren Fragen zielen auf die Schulbildung und die Berufstätigkeit der Eltern ab. Hier sieht das Formular auch die Möglichkeit vor, keine Angaben zu machen. Dies zeigt, daß das MASGF selbst diese Angaben für nicht zwingend erforderlich hält. So war im Rahmen einer Besprechung vom Ministerium auch zugegeben worden, daß zwischen dem Abitur und dem Hochschulabschluß nicht zwingend ein Unterschied zu machen sei; ebensowenig wurde die Frage nach der Schichtarbeit als besonders relevant angesehen. Meines Erachtens hätte es dem MASGF gut angestanden, auf diese datenschutzrechtlich nicht unproblematischen Fragen ganz zu verzichten. Dabei wäre insbesondere zu bedenken gewesen, daß solche Fragen nicht den betroffenen Eltern selbst, sondern den Kindern und Jugendlichen bei der Untersuchung gestellt werden, und daß nicht sicher ist, ob diese bereits die notwendige Urteils- und Einsichtsfähigkeit haben, auch mit Fragen öffentlicher Stellen kritisch umzugehen. Einen Fall, der meine diesbezüglichen Bedenken bestätigt, habe ich unter 12.1 dargestellt.

Auch die Verordnung selbst war Gegenstand einer Besprechung sowie eines regen Schriftwechsels zwischen dem Ministerium und mir. Hierbei wurden einige meiner Anregungen aufgegriffen. So wurde mit dem MASGF beispielsweise Einigung darüber erzielt, daß die in § 1 Abs. 2 KJGDV erwähnte "enge Zusammenarbeit" des Kinder- und Jugend-Gesundheitsdienstes mit niedergelassenen Ärzten, Kliniken und Einrichtungen, die Kinder und Jugendliche betreuen, keine Datenübermittlungsbefugnis bedeuten kann, sondern personenbezogene Daten zwischen den o. g. Stellen nur insoweit ausgetauscht werden können, als hierfür aufgrund anderer Vorschriften eine Übermittlungsbefugnis besteht. Auch die Abstimmung hinsichtlich organisatorischer Fragen in § 4 Abs. 2 KJGDV stellt keine Grundlage für eine Datenübermittlung dar, sondern setzt eine solche, sofern beispielsweise Schülerlisten übermittelt werden sollen, voraus.

7.3.1.4 Landesrettungsdienstplan

---

122 s. 2. Tätigkeitsbericht unter 7.2.2.4 und 4. Tätigkeitsbericht unter 7.2.3.3

123 vom 25. Februar 1997, GVBl. II S. 96

Gemäß § 4 Abs. 2 Brandenburgisches Rettungsdienstgesetz[124] ist zur Gewährleistung eines bedarfsgerechten und flächendeckenden Rettungsdienstes ein Landesrettungsdienstplan zu erlassen. In diesem ist die medizinische Dokumentation nur für den größeren Schadensfall marginal enthalten. Das für die Verordnung über den Landesrettungsdienstplan[125] zuständige MASGF hat mir auf meine Bedenken hin mitgeteilt, daß es sich entschlossen habe, erst mit der beabsichtigten Novellierung des Brandenburgischen Rettungsdienstgesetzes eine grundsätzliche Regelung für die medizinische Dokumentation zu treffen. Da ich eine bereichsspezifische gesetzliche Regelung für vorzugswürdig halte und das Ministerium mich dahingehend informiert hat, daß ein Referentenentwurf bis Mitte 1997 vorliegen soll, habe ich mich bereit erklärt, darüber hinwegzusehen, daß vorübergehend ein aus datenschutzrechtlicher Sicht unbefriedigender Zustand besteht.

7.3.1.5 Umgang mit Impfdateien in den Gesundheitsämtern

In Ergänzung des interministeriellen Runderlasses zur Meldung, Aufbewahrung und Nutzung von Patientendaten aus ehemaligen Einrichtungen des Gesundheitswesens[126] hat das MASGF den Entwurf eines Runderlasses zur Behandlung von Impfdaten in den Gesundheitsämtern erarbeitet. Dabei hat mich das Ministerium in diesem Verfahren in vorbildlicher Weise beteiligt.

Letztlich erschien aber dem Ministerium dieser Runderlaß, der sich nur auf Altakten beziehen kann, als Problemlösung nicht befriedigend. Eine Änderung des Brandenburgischen Gesundheitsdienstgesetzes - die aus datenschutzrechtlicher Sicht beste Lösung, um auch den Umgang mit aktuellen Impfdaten zu regeln - ist nicht geplant. Vielmehr strebt das Ministerium eine Verwaltungsvorschrift über die Meldung von Impfungen an. Mit dieser soll eine Grundlage dafür geschaffen werden, über anonymisierte Meldungen von durchgeführten Impfungen eine Erfassung der Durchimmunisierungsgrade einzelner Bevölkerungsjahrgänge zu erreichen, um so die epidemiologische Situation einschätzen zu können. Damit wird der Landesgesetzgeber aber dem Gesetzesvorbehalt für Grundrechtseingriffe nicht gerecht.

7.3.1.6 Tauglichkeit für die Kindertagesstätte

[124] vom 8. Mai 1992, GVBl. I S. 170

[125] vom 24. Februar 1997, GVBl. II S. 106

[126] vom 22. November 1993, ABl. 1993 S. 1725

Nach § 11 Abs. 2 Kindertagesstättengesetz (Kita-Gesetz)[127] wird nunmehr von den Personensorgeberechtigten eine ärztliche - nicht notwendigerweise amtsärztliche oder vom öffentlichen Gesundheitsdienst durchzuführende - Untersuchung des Kindes verlangt, bevor sie ihr Kind in die Kindertagesstätte bringen. Damit sind mit der Novellierung dieses Gesetzes die Voraussetzungen und Folgen dieser Bestimmung insofern klarer gefaßt, als damit sichergestellt werden soll, daß bei gesundheitlichen Bedenken keine Aufnahme in eine Kita erfolgt. Zum anderen wird der Zweck der ärztlichen Untersuchung gegenüber der alten Gesetzesfassung präzisiert. Ziel und Zweck der Untersuchung beschränken sich auf die Feststellung einer "Tauglichkeit" für den Tagesstättenbesuch. Es handelt sich hierbei um eine ärztliche Prüfung von gesundheitlichen Gründen, die eine Betreuung in einer Tagesstätte mangels Tauglichkeit ausschließen oder die besondere Vorsorge oder Rücksicht in der Betreuung erforderlich machen.

Der im Zuge der Beratungen des federführenden Landtagsausschusses zur Novellierung des Kita-Gesetzes neu aufgenommene Absatz 3 verweist auf die Pflicht, bereits bei der Aufnahmeuntersuchung den Impfstatus zu überprüfen und ggf. zu ergänzen. Die Norm weist hin auf die hohe Bedeutung, die der Durchführung der Impfungen zur Gesundheitsvorsorge beigemessen wird. Gleichwohl gibt es keine Impfpflicht und sie wird auch nicht durch das Kita-Gesetz als Voraussetzung für eine Aufnahme in eine Kindertagesstätte geschaffen. Diese Entscheidung bleibt allein den Personensorgeberechtigten vorbehalten[128].

7.3.1.7 Umgang mit personenbezogenen Daten aus Leichenschauscheinen

Schon in meinem 4. Tätigkeitsbericht[129] hatte ich darauf hingewiesen, daß die Datenverarbeitung im Zusammenhang mit Leichenschauscheinen, wie sich auch aus praktischen Anfragen der Gesundheitsämter ergeben hat, dringend einer Regelung bedarf.

Obwohl mir Mitte 1994 mitgeteilt worden war, daß ein Gesetzentwurf zu dieser Problematik in Vorbereitung sei, habe ich diesen bis heute nicht zu sehen bekommen. Zunächst war wohl geplant gewesen, ein Gesetz über das Friedhofs- und Bestattungswesen zu erarbeiten, das diese Fragen
- wie in vielen anderen Bundesländern auch - regeln sollte. Dieses soll an der Mitarbeit des Innenministeriums gescheitert sein. Das MASGF hat mir aber immerhin mitgeteilt, daß es im Alleingang eine Regelung zur Frage des Leichenschauwesens treffen wolle und mich daran beteiligen werde. Es bleibt zu hoffen, daß ich im folgenden Jahr in diesem Zusammenhang einen positiveren Bericht werde erstatten können.

7.3.2 Aktuelle Fälle

7.3.2.1 Meldung von Patientenakten an das zuständige Gesundheitsamt

---

127 vom 10. Juni 1992, GVBl. I S. 178; geänd. d. 1. ÄndG vom 7. Juni 1996, GVBl. I S. 182

128 s. hierzu auch unter 5.3.1

129 s. unter 7.2.3.1

§ 34 BbgDSG regelt die grundsätzliche Zuständigkeit für personenbezogene Daten aus ehemaligen Einrichtungen und ansatzweise das Verfahren der Weiterleitung dieser Daten an die zuständigen Stellen. Für personenbezogene Altakten, die in den Aufgabenbereich der Gesundheitsämter fallen, ist ein gemeinsamer interministerieller Runderlaß[130] maßgebend. - Danach soll das Vorhandensein von Patientenunterlagen unmittelbar an das örtlich zuständige Gesundheitsamt namensbezogen bis zum 30. Juni 1994 gemeldet werden. Können Patientenunterlagen nicht anderweitig ordnungsgemäß aufbewahrt und genutzt werden, so müssen diese bei der Ärztin oder dem Arzt, in deren Verfügungsgewalt sie sich zum Zeitpunkt des Erlasses befanden, verbleiben. Die Patientenunterlagen sind durch das örtlich zuständige Gesundheitsamt zu katalogisieren und über 30 Jahre (gerechnet vom Tage des letzten Eintrags in die Patientenunterlage) aufzubewahren. Patientenunterlagen, die mit an Sicherheit grenzender Wahrscheinlichkeit nicht mehr zu Zwecken der medizinischen Behandlung bzw. für gutachterliche Bearbeitung genutzt werden und die ihre rechtlich festgelegten Aufbewahrungsfristen überschritten haben, sind zu vernichten.

Auf meine Anfrage hin hat das MASGF mir mitgeteilt:

- In jedem Gesundheitsamt befinden sich ca. 1 bis 1,5 Mio. Akten aus Einrichtungen des staatlichen Gesundheitswesens der DDR, des Betriebsgesundheitswesens und der sog. Sonderdienste. In 11 Kreisen ist die Übernahme der Patientenunterlagen aus Gesundheitseinrichtungen der ehemaligen DDR abgeschlossen. Sieben Gesundheitsämter haben die Unterlagen noch nicht bzw. noch nicht vollständig übernommen. Das bedeutet, daß die Ärzte, in deren Verfügungsgewalt sich die Akten befinden, diese weiterhin aufbewahren, sie auf Anforderung jedoch verpflichtet sind, diese an weiterbehandelnde Ärzte abzugeben. Drei Gesundheitsämter führen personelle, finanzielle und räumliche Probleme an, die derzeit eine Übernahme der Patientenunterlagen nicht gestatten.

- Namentliche Übersichten sind nicht vorhanden, da die niedergelassenen Ärzte und Zahnärzte namensbezogene Meldungen nur in Einzelfällen vornehmen.

- Sämtliche Patientenunterlagen, die übernommen wurden, sind sicher untergebracht. Entsprechend den personellen, räumlichen und finanziellen Möglichkeiten werden die Akten nun aufgelistet und gespeichert. In den meisten Fällen werden die Patientenakten noch unter den Bezeichnungen der ehemaligen Gesundheitseinrichtungen aufbewahrt.

- Den Patienten selbst ist der Verbleib der Unterlagen in den meisten Kreisen bekannt, weil er in den regionalen Presseorganen veröffentlicht wurde.

Es ist zu hoffen, daß die Übernahme der Patientendaten so bald wie möglich abgeschlossen werden kann.

7.3.2.2 Genehmigung Klinischer Krankheitsregister

[130] vom 22. November 1993, ABl. 1993 S. 1725

Seit Inkrafttreten der Krankenhausdatenschutzverordnung (KHDsV)[131] dürfen in Klinischen Krankheitsregistern personenbezogene Daten nur mit Genehmigung des für das Gesundheitswesen zuständigen Ministeriums (MASGF) und nach Anhörung meiner Behörde verarbeitet werden. Diese Register sind in § 11 Abs. 1 KHDsV als Krankheitsregister im Krankenhaus definiert, die neben Behandlungszwecken regelmäßig auch - nicht behandlungsbezogen - der wissenschaftlichen Erforschung einer bestimmten Krankheit dienen.

Auf meine Anfrage hin hat das Ministerium mir mitgeteilt, daß bislang keine förmlichen Genehmigungen zur Führung Klinischer Krankheitsregister nach § 11 KHDsV erteilt wurden, daß aber fünf Krankenhäuser Tumorbasisdokumentationen auf der Grundlage einer mit mir abgestimmten Einverständniserklärung vornähmen. Von einer förmlichen Genehmigung sei abgesehen worden, da diese Register bereits mehrere Jahre vor Inkrafttreten der Krankenhausdatenschutzverordnung auf ausdrücklichen Wunsch und mit Unterstützung des MASGF und in Abstimmung mit mir aufgebaut worden seien. Es hat in diesem Zusammenhang problematisiert, daß das Erfordernis einer nachträglichen Genehmigung bereits bestehender Register gegen das verfassungsrechtlich bestehende Verbot der Rückwirkung verstoßen könnte. Meinen weiteren Hinweis, daß nach § 11 Abs. 2 KHDsV eine Einverständniserklärung des Patienten für die Meldung an das Klinische Krankheitsregister nicht mehr nötig sei, sondern der Patient lediglich über ein Widerspruchsrecht gegen die Meldung verfüge, wollte das Ministerium hingegen aufgreifen.

Ich gab dem Ministerium zu bedenken, daß nach dem Wortlaut des § 11 Abs. 1 KHDsV die Verarbeitung personenbezogener Daten in einem Klinischen Krankheitsregister genehmigungsbedürftig ist und nicht die Errichtung des Registers selbst. Datenverarbeitungen finden dort jedoch regelmäßig statt, obwohl die entsprechende generelle Erlaubnis dafür fehlt. Die in § 11 Abs. 2 KHDsV enthaltene Widerspruchslösung beruht aber gerade darauf, daß die grundlegenden, das Klinische Krankheitsregister betreffenden Punkte dem förmlichen Verfahren nach Abs. 1 unterzogen wurden. § 11 Abs. 2 KHDsV anwenden zu wollen, ohne § 11 Abs. 1 KHDsV zu beachten, würde dem primär zu schützenden Vertrauen der Patienten in die Einhaltung geltenden Rechts zuwiderlaufen. Das MASGF hat sich meiner Argumentation letztlich angeschlossen und mir mitgeteilt, daß es die Krankenhäuser mit onkologischen Schwerpunkten und die Onkologischen Arbeitskreise gebeten habe, ihm die für die Beurteilung der Genehmigungsfähigkeit erforderlichen Angaben zuzuleiten. Für die Übergangszeit habe ich mich bereit erklärt, die bisherige Form der Datenverarbeitung wie bisher mit ausdrücklicher Einwilligung der Patienten zuzulassen.

7.3.2.3 Meldebogen für Tumorbasisdokumentation

Im Nachgang zur Besprechung des Staatsvertrages über das Gemeinsame Krebsregister der neuen Bundesländer und Berlins (s. unter 7.3.1.1) hat mir das MASGF Entwürfe für Meldebögen zur Kenntnis gegeben, durch die die bisher getrennte Meldung an Klinische Krebsregister und das Gemeinsame Krebsregister in Berlin (GKR) zusammengeführt werden sollen. Es handelte sich dabei um sechs Meldebögen für folgende Fälle:

- Erstmeldung einer Primärerkrankung,
- Erstmeldung eines sekundären Tumorgeschehens,
- Behandlungsmeldung,
- Nachsorgemeldung,
- onkologisches Konzil und
- Abschlußmeldung.

[131] vom 4. Januar 1996, GVBl. II S. 54

Meldungen an das GKR sind dabei nur für die Erstmeldung einer Primärerkrankung, die Behandlungsmeldung und die Abschlußmeldung vorgesehen.

Über diese Meldebögen fand Anfang des Jahres eine Besprechung statt, an der insbesondere die beteiligten Datenschutzbeauftragten und Fachleute der betroffenen Register teilnahmen. Dabei wurden von den Datenschutzbeauftragten etliche zusätzliche Schwärzungen bei dem Durchschriftblatt, das für das GKR vorgesehen ist, gefordert. Vorübergehend gilt dies auch für Daten, die erst aufgrund des noch nicht abgeschlossenen Staatsvertrages an das GKR übermittelt werden dürfen. Um ein jeweils korrektes Verfahren bei den einzelnen Meldungen zu gewährleisten, wurde ein Deckblatt mit entsprechenden Kurzhinweisen für die Meldebögen entwickelt. Noch zu erarbeiten ist ein Merkblatt für den Arzt mit datenschutzrechtlichen Hinweisen sowie Muster von Einwilligungserklärungen bzw. Informationen über das Widerrufsrecht für die Patienten.

7.3.2.4 Prüfung der Datenverarbeitung in einem Krankenhaus

Schwerpunkte der Prüfung in einem Kreiskrankenhaus waren u. a. die Kontrolle der datenschutzgerechten Ausgestaltung des Krankenhausinformationssystems (KHIS) sowie die Umsetzung der Krankenhausdatenschutzverordnung[132], wobei insbesondere die Aufbewahrung von Behandlungsunterlagen, der Zugriff auf diese und die Dokumentation in den Krankenakten thematisiert wurden. Der Kontrollbesuch wurde von mir noch nicht abschließend bewertet; im folgenden wird lediglich auf ausgewählte technisch-organisatorische Aspekte eingegangen:

Im Krankenhaus werden ein zentraler UNIX-Rechner und mehrere PC's mit Terminalemulationen betrieben und ein KHIS mit folgenden Modulen eingesetzt:

- Patientendatenerfassung,
- Kostensicherung (§ 301 SGB V),
- zentrale Leistungserfassung,
- Finanzbuchhaltung.

Mit dem vorhandenen System befindet sich jeder Nutzer nach dem Anmelden auf Betriebssystemebene. Dadurch erhält dieser Personenkreis die Möglichkeit, Patientendaten zu lesen oder sogar komplett zu löschen, auch wenn dies nicht zu seinen Aufgaben zählt. Dies ist mit Datenschutzanforderungen an jedwedes System nicht zu vereinbaren. Der Zugriff auf die Betriebssystemebene durch den Nutzer muß ausgeschlossen werden.

Die Möglichkeiten der Paßwort- und Rechtevergabe sind im KHIS ebenfalls nicht datenschutzgerecht. So ist es z. B. einem "normalen" Nutzer des Systems nicht möglich, sein Paßwort selbständig zu ändern. Hierzu ist der Start eines Programms erforderlich, auf das nur der Systemverwalter durch Eingabe eines Paßwortes zugreifen kann. Mit Hilfe des UNIX-Kommandos "grep" konnten im Datenverzeichnis Dateien gefunden werden, die das Anwendungspaßwort des Systemverwalters enthielten. Daraus könnte man schlußfolgern, daß Paßwörter im KHIS nicht verschlüsselt abgelegt werden.

Die bisherigen Rechte des Systemverwalters sind zu weitgehend. Nach den derzeitigen Möglichkeiten kann er sich die

[132] vom 4. Januar 1996, GVBl. II S. 54

Paßwörter der Nutzer ausdrucken lassen. Der Systemverwalter darf aber weder eine Möglichkeit zur Anzeige noch zum Ausdruck von Paßwörtern haben und lediglich in der Lage sein, das Paßwort eines Nutzers - nachdem dieser es z. B. vergessen hat - ändern zu können. Darüber hinaus sollten Paßwörter im ADV-System grundsätzlich verschlüsselt abgelegt werden.

Die Vergabe von Paßwörtern ist im System sehr stark an die Vergabe der Nutzerrechte gebunden. Daraus resultiert, daß z. B. ein Nutzer für verschiedene Programm-Module verschiedene Paßwörter eingeben muß, da er für diese Module unterschiedliche Rechte besitzt. Erfahrungsgemäß wird unter diesen Bedingungen das Paßwort zur eigenen Absicherung auf einem Zettel vermerkt (sog. "unter-die-Tastatur-Schreiben").

Auf Anwendungsebene besteht keine Möglichkeit, Datensätze zu löschen. Die Dateien werden im KHIS jahrgangsweise angelegt. Das führt dazu, daß nur komplette Jahrgänge zu löschen sind. Ob man auf Arbeitsebene auch einzelne Datensätze löschen kann, ließ sich nicht abschließend klären.

Eine telefonische Rückfrage des Systemverwalters bei der Softwarefirma ergab, daß im KHIS Protokolldateien geführt werden, in denen die Zugriffe auf die entsprechenden Module protokolliert werden, die aber vom Systemverwalter nicht eingesehen werden können. Ein Zugriff auf diese Dateien kann nur mit Hilfe der Fernwartung von der Softwarefirma aus erfolgen.

Lediglich bei der Bearbeitung von Daten der medizinischen Basisdokumentation wird festgehalten, welcher Nutzer einen Datensatz zu welchem Zeitpunkt erstellt hat.

Eine Softwarefirma aus Nordrhein-Westfalen führt ca. 2 - 3 mal monatlich eine Fernwartung im Krankenhaus durch. Ein Vertrag zur Fernwartung existiert nicht. Eine Fernwartung wird erforderlich, wenn

- nach einem Systemabsturz sich bestimmte Patientendatensätze nicht mehr bearbeiten lassen,
- technische Probleme während der Datensicherung auftreten,
- Programmupdates in das System eingespielt werden.

Die Fernwartung wird mit Systemverwalter-Rechten durchgeführt. Eine für den Systemverwalter nachvollziehbare, revisionssichere Protokollierung findet seitens des Krankenhauses nicht statt.

Die Übermittlung von Abrechnungsdaten gem. § 301 SGB V (s. unter 7.3.2.5) an die Krankenkassen wird gegenwärtig im Krankenhaus vorbereitet. Ende März d. J. soll mit der Testphase begonnen werden. Im Krankenhaus wurde dazu ein Kommunikationsrechner im Netzwerk implementiert, der derzeit durch Fernwartung konfiguriert wird. Ein Vertrag mit der Deutschen Krankenhausgesellschaft (DKG) war zum Zeitpunkt der Kontrolle in Vorbereitung.
Die Stationen sind mit PC's ausgestattet, auf denen u. a. die Arztbriefe und OP-Berichte abgefaßt werden. Mit den gespeicherten Textdateien wird von Station zu Station sehr differenziert umgegangen. Auf einer Station werden die Dateien nach dem Ausdruck sofort gelöscht, auf einer anderen erfolgt die Speicherung über mehrere Monate. Das Ziel sollte jedoch sein, nicht mehr benötigte Dateien auf allen Stationen sofort zu löschen. Man sollte dabei beachten, daß die Dateien regelmäßig physisch - nicht nur logisch - gelöscht werden. Entsprechende Tools sind auf dem Markt verfügbar.

Aus dem Kontrollbesuch ergeben sich aus technisch-organisatorischer Sicht u. a. folgende Forderungen, die teilweise nur gemeinsam mit den Herstellerfirmen durchgesetzt werden können:

1. ADV-System

- Sperrung der Betriebssystemebene für den Benutzer
- verschlüsseltes Ablegen von Paßwörtern
- verschlüsseltes Abspeichern sensibler personenbezogener Daten mit sicheren Kryptoverfahren
- Dunkelschaltung des Bildschirms bei Arbeitsunterbrechung

2. Paßwort- und Rechtevergabe im ADV-System

- datenschutzgerechte Paßwortverwaltung
- restriktive und für den Nutzer transparente Vergabe von Zugriffsrechten

3. Löschen von Daten

- Definiertes Löschen von Datensätze auf Anwendungsebene

4. Protokollierung

- revisionssichere Protokollierung der Zugriffe auf sensible personenbezogene Daten im Krankenhausinformationssystem
- Festlegung der Zuständigkeiten bzgl. Protokolldateienauswertung
- personelle und zeitliche Festlegungen über die Löschung von Protokolldateien

5. Fernwartung

- Reduzierung der Fernwartung (z. B. Verzicht auf Programmupdates) auf das unumgängliche Maß
- Aufbau der Verbindung gem. § 9 Abs. 2 Nr. 1 KHDsV ausschließlich durch das Krankenhaus
- revisionssichere Protokollierung der Fernwartungsaktivitäten im Krankenhaus gem. § 9 Abs. 2 Nr. 3 KHDsV
- Abschluß eines Vertrages zur Fernwartung
- ständiges Mitverfolgen der Fernwartungsaktivitäten am Bildschirm

6. Datenübermittlung gem. § 301 SGB V an die Krankenkassen

- sichere Speicherung der geheimen Schlüssel im System
- Sperrung sämtlicher Fernwartungsaktivitäten auf dem Kommunikationsserver, solange sich die geheimen Schlüssel im Zugriff befinden
- regelmäßige Änderung der Paßwörter der Mailbox und des Kommunikationsrechners
- digital signierte Übertragung personenbezogener Daten

7. Arbeitsplatzcomputer in den Sekretariaten der Stationen

- Löschen nicht mehr benötigter Texte

Das geprüfte Kreiskrankenhaus wird nach eigenen Angaben noch in diesem Jahr in einen Neubau umziehen. Dabei ist u. a. auch beabsichtigt, ein völlig neues Krankenhausinformationssystem einzusetzen. Ich gehe davon aus, daß wenigstens in diesem meine vorgenannten Forderungen realisiert werden und habe daher vorerst von einer förmlichen Beanstandung gem. § 25 Abs. 1 Ziff. 2 BbgDSG abgesehen.

7.3.2.5 Umsetzung der Datenübermittlung nach § 301 SGB V

Mit § 301 Abs. 1 Satz 1 SGB V werden Krankenhäuser verpflichtet, den Krankenkassen bei Krankenhausbehandlungen bestimmte Angaben maschinell zu übermitteln. Dazu wurde gemäß Abs. 3 a. a. O. eine Vereinbarung zwischen den Spitzenverbänden der Krankenkassen und der Deutschen Krankenhausgesellschaft (Datenübermittlungs-Vereinbarung)[133] abgeschlossen. Noch in diesem Jahr wird mit der elektronischen Übertragung der Daten begonnen. Gem. § 3 Datenübermittlungs-Verordnung sollen dabei folgende Datensätze übertragen werden:

vom Krankenhaus zur Krankenkasse

- Aufnahmesatz,
- Verlängerungsanzeige,
- medizinische Begründung,
- Rechnungssatz,
- Entlassungsanzeige,
- Rechnungssatz Ambulante Operation.

von der Krankenkasse zum Krankenhaus

- Kostenübernahmesatz,
- Anforderungssatz medizinische Begründung,
- Zahlungssatz,
- Zahlungssatz Ambulante Operation.

Da es sich hierbei um sensible personenbezogene Daten handelt, sind entsprechende technisch-organisatorische Maßnahmen (z. B. Verschlüsselung und digitale Signatur) zum Schutz dieser Daten vorgesehen. Im Anhang zur Technischen Anlage der Datenübermittlungs-Vereinbarung wurde daher eine Security-Schnittstelle entworfen, in der u. a. folgende Schnittstellenparameter definiert wurden:

- Datenformate nach PEM
- Verschlüsselungsverfahren DES und RSA (Schlüssellänge: 768)
- Hash-Funktion MD5 (s. oben unter 6.1.)
- Namenskonvention der öffentlichen Schlüssel entsprechend ASN.1 und X.509

Zur Verwaltung der Schlüssel wurde ein Trust-Center eingerichtet. Dieses Trust-Center hat die Aufgabe, für alle beteiligten Stellen authentische öffentliche Schlüssel bereitzustellen. Die Daten werden verschlüsselt und digital signiert zwischen

---

133 Vereinbarung gem. § 301 Abs. 3 SGB V über das Verfahren zur Abrechnung und Übermittlung der Daten nach § 301 Abs. 1 SGB V zwischen den Spitzenverbänden der Krankenkasse und der Deutschen Krankenhausgesellschaft, Stand: 9. Juli 1996

den Krankenhäusern und den Krankenkassen, unter Zwischenschaltung einer Mailbox, übertragen. Als wichtig erachte ich hierbei, daß die geheimen Schlüssel sicher auf den Kommunikationsservern der beteiligten Stellen abgelegt werden und daß auf diese kein unberechtigter Zugriff von außen erfolgen darf.

7.4 Durchführung des Landesgleichstellungsgesetzes

Nach § 26 Landesgleichstellungsgesetz (LGG)[134] hat die Landesregierung im Abstand von zwei Jahren dem Landtag über die Durchführung des Gesetzes und über die Entwicklung des Frauenanteils in der Landesverwaltung zu berichten. Während zum zweiten Teil auf statistische Daten des Landesamts für Datenverarbeitung und Statistik zurückgegriffen wird, hat das MASGF bzgl. des ersten Teils zwei gesonderte Fragebögen entwickelt, mit denen sowohl von den Leitungen der mittelbaren und unmittelbaren Landesverwaltungen als auch von den dortigen Gleichstellungsbeauftragten (GBA) die jeweiligen Erfahrungen mit der Umsetzung des Gesetzes auch im Verhältnis untereinander abgefragt werden.

Ich hatte Gelegenheit zur datenschutzrechtlichen Bewertung der Fragebögen. Leider sind meine Empfehlungen aus von mir nicht zu vertretenden Gründen zumindest bei der ersten Befragungsaktion nicht unmittelbar in die Vordrucke eingeflossen. Das MASGF hat jedoch unmittelbar nach Verteilung in einem gesonderten Rundschreiben hinreichend auf meine Empfehlungen und Hinweise aufmerksam gemacht und ausdrücklich um deren Berücksichtigung gebeten. Ich gehe davon aus, daß die Formulare bei der nächsten Befragungsaktion entsprechend überarbeitet sein werden.

Meine Empfehlungen zielten insbesondere darauf ab, daß durch die Beantwortung der einzelnen Fragen

- kein konkreter Personenbezug zum Bediensteten hergestellt wird und
- insbesondere den GBA verdeutlicht wird, für welche Fragen sich eine Pflicht zur Beantwortung unmittelbar aus dem Gesetz heraus ergibt und in welchen Fällen die Beantwortung ohne konkrete Rechtsgrundlage allenfalls mit dem Hinweis auf die Freiwilligkeit erbeten werden kann.

Im einzelnen richteten sich meine Vorschläge auf Fragen an die Dienststellen

- an welchen dienst- oder arbeitsrechtlichen Maßnahmen die jeweilige GBA beteiligt worden ist
- in welchen stichwortartig zu nennenden Fällen ein Widerspruch der GBA erfolgreich war

und auf die entsprechenden Fragen an die GBA sowie auf die zusätzlich an diese gestellten Fragen

- worin die Gründe bestanden, GBA zu werden
- nach der Beteiligung an Fortbildungsveranstaltungen zum LGG
- zum Kontakt zu GBA anderer Dienststellen sowie
- zum Geburtsjahr, Familienstand, zur Anzahl eigener Kinder, zum Ausbildungsabschluß der derzeitigen beruflichen Tätigkeit, der derzeitigen Laufbahn und zu einer evtl. Mitgliedschaft im jeweiligen Personalrat.

[134] Gesetz zur Gleichstellung von Frauen und Männern im öffentlichen Dienst im Land Brandenburg vom 4. Juli 1994, GVBl. I S. 254

Es entspricht der gesetzlichen Voraussetzung zu einer ordnungsgemäßen Datenerhebung[135], daß das MASGF bzgl. der Daten zum Personenstand sowie zum sozialen und dienstlichen Umfeld zusätzlich zum Hinweis auf die Freiwilligkeit mangels gesetzlicher Grundlage erläutert, daß eine Beantwortung doch wünschenswert ist, weil dadurch Informationen über die soziale Situation der GBA sowie deren Einordnung in die jeweilige Verwaltungshierarchie und dortige Akzeptanz gewonnen werden können.

8 Ernährung, Landwirtschaft und Forsten

8.1 Gesetze und Verordnungen

8.1.1 Novellierung des Tierschutzgesetzes

Bereits im 4. Tätigkeitsbericht[136] hatte ich im Zusammenhang mit der geplanten zentralen Erfassung von Zirkusbetrieben in der Bundesrepublik Deutschland darauf hingewiesen, daß der Bundesgesetzgeber im Rahmen des Tierschutzgesetzes eine gesetzliche Grundlage für die Einrichtung des zentralen Registers und der damit verbundenen Verarbeitung personenbezogener Daten schaffen muß.

135 vgl. § 4 Abs. 1 Buchst. b u. Abs. 2 BbgDSG

136 s. unter 8.2

Inzwischen hat die Bundesregierung einen umfangreichen Entwurf zur Novellierung des Tierschutzgesetzes[137] vorgelegt. Der Gesetzentwurf enthält insbesondere Neuregelungen über die Anforderungen an die Sachkunde von Tierhaltern und -betreuern, die Verwendung von Tieren in Forschung und Lehre sowie über Eingriffe an und Behandlung von Tieren. So ist u. a vorgesehen, den Personenkreis, der die Sachkunde im Umgang mit Tieren nachzuweisen hat, auszudehnen, den Kreis der Tätigkeiten, die der tierschutzrechtlichen Erlaubnispflicht unterliegen, zu erweitern und die Altersgrenze für Personen, die Wirbeltiere erwerben dürfen, von 14 auf 16 Jahre zu erhöhen. Kritisch ist hervorzuheben, daß der Entwurf der Bundesregierung die Frage einer zentralen Erfassung von Zirkusbetrieben sowie den gesamten Bereich des Datenschutzes ausgeklammert hatte, obwohl einige Bundesländer (u. a. Brandenburg) seit längerem Vorschriften auf diesen Gebieten fordern. Das Ministerium für Ernährung, Landwirtschaft und Forsten (MELF) hat mich wenige Tage vor der Sitzung des Agrarausschusses des Bundesrates Ende November 1996 um eine Stellungnahme zu diesem Entwurf und zu einzelnen Änderungsanträgen anderer Bundesländer gebeten.

Eine ausführliche Stellungnahme unter Berücksichtigung und Prüfung sämtlicher rechtlicher und tatsächlicher Aspekte des Gesetzentwurfs war aus Zeitgründen und rechtzeitig zur Ausschußsitzung nicht mehr möglich. Deshalb habe ich mich inhaltlich in der Hauptsache mit den Anträgen und Vorschlägen der Bundesländer auseinandergesetzt und angeregt, eine möglichst allgemein formulierte und von anderen Einzelvorschriften getrennte Regelung zum Datenschutz in das Gesetz aufzunehmen. Darüber hinaus habe ich noch einmal auf die rechtlichen Probleme hingewiesen, die im Zusammenhang mit der Einrichtung eines Zentralregisters für Zirkusbetriebe bestehen. Der Bundesgesetzgeber kann, auch im Rahmen einer Verordnungsermächtigung, grundsätzlich nur die Einrichtung eines bundesweiten Zentralregisters regeln bzw. anordnen. Die Länder Hamburg und Niedersachsen waren dafür, neben den Zirkusbetrieben mit ständig wechselnden Standorten, auch Tierauffangstationen zentral zu erfassen und in das geplante Register mit aufzunehmen.

Letztlich dürfte der Entwurf der Bundesregierung nicht allein aufgrund der bereits angesprochenen Probleme im Bundesrat auf Kritik gestoßen sein. Der Agrarausschuß des Bundesrates hat eine Reihe von Änderungsanträgen u. a. zum oben genannten Zentralregister gestellt. Hervorzuheben ist aus meiner Sicht die Entscheidung des Bundesrates, eine übergreifende Regelung zum Datenschutz in das Tierschutzgesetz aufzunehmen.

Inzwischen liegt der Entwurf dem Bundestag zur Beratung und Beschlußfassung vor. Die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates die Mehrzahl der Änderungsanträge des Bundesrates, so auch die Forderung nach der zentralen Erfassung von Zirkusbetrieben, abgelehnt. Aus Sicht des Datenschutzes erfreulich ist, daß die Bundesregierung sich wenigstens dazu durchgerungen hat, dem Antrag des Bundesrates zur Einführung einer allgemeinen datenschutzrechtlichen Regelung in das Tierschutzgesetz ohne Einschränkung zuzustimmen. Dies könnte daran liegen, daß die vom Bundesrat vorgeschlagene Regelung u. a. vorsieht, daß das Bundesministerium für Ernährung, Landwirtschaft und Forsten (BML) die Erhebung, Speicherung, Veränderung, Nutzung und Übermittlung personenbezogener Daten, deren Kenntnis zur Erfüllung der Aufgaben nach dem oder aufgrund des Tierschutzgesetzes notwendig ist, durch Rechtsverordnung näher bestimmen kann.

8.1.2 Tierschutztransportverordnung

[137] BR-Drs. 763/96

Das BML hat Anfang November 1996 eine Tierschutztransportverordnung (TierSchTrV)[138] vorgelegt und dem Bundesrat zur Zustimmung zugeleitet. Die Verordnung dient in erster Linie der Umsetzung der Richtlinie 95/29/EG des Rates[139] zur Änderung der Richtlinie 91/628/EWG[140] über den Schutz von Tieren beim Transport und löst die bislang geltende Verordnung zum Schutz von Tieren beim grenzüberschreitenden Transport aus dem Jahre 1983 ab.

Der Tierschutztransportverordnung kommt nicht nur aus tierschutzrechtlicher, sondern auch aus datenschutzrechtlicher Sicht Bedeutung zu. Sie enthält nämlich Vorschriften über

- die Einführung einer Anzeigepflicht für Unternehmen, die gewerbsmäßig Tiere befördern, sowie die Einrichtung entsprechender Register,

- die Einführung einer Sachkundeprüfung für Begleiter von Tiertransporten und

- das Erstellen, Vorlegen und Mitführen von Transportplänen und Transportbescheinigungen bei grenzüberschreitendem Transport,

bei deren Umsetzung durch die jeweils zuständigen Landesbehörden eine Fülle personenbezogener Daten erhoben und verarbeitet werden müssen. Dennoch enthält die Bundesverordnung keine entsprechende datenschutzrechtliche Regelung.

Diesen Umstand habe ich zum Anlaß genommen, das MELF zu drängen, daß sich die Vertreter des Landes Brandenburg im Bundesrat dieser Frage annehmen und sich im Zuge der dort stattfindenden Beratungen für die Aufnahme einer entsprechenden allgemeinen Regelung zum Datenschutz in die Verordnung einsetzen. Des weiteren habe ich aus Gründen der Rechtssicherheit und der Transparenz angeregt, den Verordnungstext um einen Hinweis auf die entsprechenden Verfahrensvorschriften, die von den jeweils zuständigen Behörden im Zusammenhang mit der Einrichtung und Führung der Register erlassen werden müssen, zu ergänzen.

Besonders hervorzuheben ist in diesem Zusammenhang, daß die Richtlinie des Rates zwar ein Genehmigungsverfahren über die Zulassung einzelner gewerblicher Transportunternehmen vorschreibt, dagegen die Verordnung an dieser Stelle lediglich ein Anzeigeverfahren und eine damit verbundene Registrierung der Unternehmen vorsieht. Hier hat es der Verordnungsgeber versäumt, den Spielraum der Richtlinie auszuschöpfen und ein wichtiges Instrumentarium zur Beseitigung der mehrfach in der Vergangenheit bekanntgewordenen Mißstände zu schaffen. Die Einführung einer Genehmigungspflicht würde ein besonders wirksames Mittel zur Bekämpfung von Verstößen darstellen, da den betroffenen Unternehmen im Wiederholungsfall regelmäßig der Entzug der Genehmigung drohen würde.

---

138 BR-Drs. 836/96

139 vom 29. Juni 1995, ABL. EG Nr. L 148 S.52

140 ABl. EG Nr. L 340 S.17

Im Ergebnis hat der Bundesrat der vom BML vorgelegten Verordnung[141] Ende Januar 1997 zugestimmt, ohne die von mir angesprochenen Problemstellungen abzuändern. Bedauerlicherweise konnte ich meine Bedenken erst kurz vor der abschließenden Beratung im Bundesrat - die Verordnung hatte bereits den Agrarausschuß passiert - äußern. Dies ist vor allem darauf zurückzuführen, daß ich auf das Vorhaben des BML erst aufgrund der Veröffentlichung der Vorlage als Bundesratsdrucksache aufmerksam geworden bin. Dies bedauere ich um so mehr, als die Zusammenarbeit mit dem MELF im allgemeinen sehr konstruktiv ist.

8.2 Sonstiges

8.2.1 Umsetzung des Waldverzeichnisses

Ein Petent wandte sich im Zusammenhang mit der für Brandenburg geplanten Einrichtung eines Waldverzeichnisses an mich und bemängelte unter anderem, daß die in der zugrundeliegenden Waldverzeichnisverordnung[142] vorgesehene "anonyme" Erfassung, Speicherung und Aktualisierung der Daten einzelner Waldbesitzer nicht gewährleistet sei. Nach seiner Auffassung sei eine erstmalige "anonyme" Erfassung und Aktualisierung von Daten nicht möglich, wenn, wie hier vorgesehen, die Angaben von den unteren Forstbehörden inhaltlich geprüft und bestätigt werden müssen.

Ich habe mich deshalb in dieser Angelegenheit an das MELF gewandt und darum gebeten, mich über den Stand der Einrichtung des Waldverzeichnisses und der bislang vom MELF getroffenen bzw. geplanten Maßnahmen zu unterrichten. Daraufhin hat mir die Landesanstalt für Forstplanung mitgeteilt, daß sie vom MELF mit der Erarbeitung einer Verfahrensvorschrift zur Umsetzung der Waldverzeichnisverordnung beauftragt worden ist und hat mir einen vorläufigen Entwurf dieser Verfahrensvorschrift zur Verfügung gestellt. Die Befürchtung des Petenten erwies sich als grundlos.

Der Entwurf sieht vor, die Daten, die sowohl zur Erstellung als auch zur Aktualisierung des Waldverzeichnisses benötigt werden, ausschließlich von den zuständigen Ämtern für Forstwirtschaft unter Verwendung entsprechender Formblätter bei den jeweiligen Waldbesitzern erheben zu lassen. Die Walddaten sollen ohne Angaben zur Person des Waldeigentümers von den Ämtern für Forstwirtschaft gespeichert und anschließend in Form von Disketten an die Landesanstalt für Forstplanung weitergeleitet werden. Eine eigentümerbezogene Betriebsnummer soll nur auf Antrag des Eigentümers vergeben werden. Die zur erstmaligen Erstellung des Waldverzeichnisses erforderliche Zuordnung von Forstadressen und Flurstückdaten soll ebenfalls von den zuständigen Ämtern für Forstwirtschaft vorgenommen werden.

Gegen diese Verfahrensweise habe ich grundsätzlich nichts einzuwenden. Die Revierförster in den jeweiligen Ämtern für Forstwirtschaft erlangen bereits im Zusammenhang mit der Erfüllung ihrer nach dem Landeswaldgesetz[143] zugewiesenen Aufgaben Kenntnis von Besitzverhältnissen und Waldzustand in ihrem Zuständigkeitsbereich.

Im einzelnen habe ich u. a. vorgeschlagen, sämtliche Formblätter mit dem ausdrücklichen Hinweis zu versehen, daß die Angaben zur Person des Waldeigentümers nicht an die Landesanstalt für Forstplanung weitergeleitet oder anderweitig gespeichert werden, und daß eine listenmäßige Erfassung dieser Angaben nur erfolgt, soweit eine Betriebsnummer auf

---

141 BR-Drs. 836/96 (Beschluß)

142 vom 29. April 1996, GVBl. II S.395

143 vom 17. Juni 1991, GVBl. S. 213

Antrag erteilt worden ist. Darüber hinaus habe ich die Aufnahme einer den Anforderungen des § 19 Abs. 2 BbgDSG entsprechenden allgemeinen Löschungsvorschrift in die Verfahrensordnung angeregt.

Im Ergebnis wäre somit eine weitgehende und aus datenschutzrechtlicher Sicht akzeptable Form der Anonymisierung, die spätestens nach der Erhebung und Prüfung der Angaben und noch vor der Übermittlung der Daten an die Landesanstalt für Forstplanung einsetzt, erreicht. Die entsprechenden Regelungen der Waldverzeichnisverordnung sollten jedoch aus Gründen der Rechtssicherheit und Rechtsklarheit bei einer künftigen Änderung der Verordnung in ihrem Wortlaut angepaßt, d. h. eindeutiger formuliert werden.

Die endgültige Fassung der Verfahrensordnung liegt mir bisher nicht vor.

8.2.2 Bundes-Agrarstatistik aus InVeKoS

Bereits im Vorjahr[144] hatte ich berichtet, daß die Bundesregierung bemüht ist, amtliche Statistiken einzuschränken und zu rationalisieren. Inzwischen liegt ein Gesetzentwurf[145] vor, der in Art. 13 Änderungen der Agrarstatistik vorsieht. Danach soll es zukünftig u. a. zulässig sein, Angaben, die der Verwaltung im Agrarbereich erteilt wurden, sekundärstatistisch für die Agrarstatistik zu nutzen. Dazu zählen neben den personenbezogenen Hilfsmerkmalen (Namen oder Firma und Anschrift) Angaben zur Bodennutzungshaupterhebung und zur Viehzählung, soweit sie für dieselben Erhebungszeiträume vorliegen. Auskunftspflichtig für Antragsteller zur Beihilfe wäre in diesem Fall die jeweils zuständige landwirtschaftliche Verwaltungsbehörde.

Solche Verwaltungsdaten fallen regelmäßig jährlich bei der Beantragung von landwirtschaftlichen Beihilfen im Zusammenhang mit dem Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) der EU an. Da sich nun nach dem vorliegenden Gesetzentwurf die sekundärstatistische Erhebung einerseits ganz im Rahmen des InVeKoS bewegt - sowohl bzgl. der Erhebungsmerkmale als auch der Erhebungszeiträume - und andererseits die Erhebung zur Beihilfegewährung bei InVeKoS selbst bereits durch automatisierte Abgleiche und andere Verwaltungsmaßnahmen abgesichert wird und ferner im Falle falscher Angaben unter Strafandrohung[146] steht, kann wohl davon ausgegangen werden, daß in diesem Fall das statistische Ergebnis einigermaßen objektiv und das Erhebungsverfahren für den angestrebten Zweck geeignet ist. Da ferner sog. überschießende Merkmale, die nur der Statistik dienen würden, durch die Verwaltung nicht erhoben werden und weitergehende Erklärungen des Antragstellers nicht vorgesehen sind, bestehen datenschutzrechtlich keine grundsätzlichen Bedenken.

Sollte das Gesetz verabschiedet werden, wäre zukünftig auf dem Förderantrag bei der Erklärung zur Datenverarbeitung ein Hinweis auf die Rechtmäßigkeit solcher Datenübermittlungen an die Statistik vorzusehen, damit der Antragsteller informiert ist.

9 Umwelt, Raumordnung und Naturschutz

---

144 s. 4. Tätigkeitsbericht unter 3.4.4 und unter 3.6.3

145 s. BR-Drs. 965/96: Entwurf eines Dritten Gesetzes zur Änderung statistischer Rechtsvorschriften (3. Statistikbereinigungsgesetz - 3. StatBerG)

146 s. "Hinweise und Erklärungen zu Rechts-, Kontroll- und Strafvorschriften sowie zur Datenverarbeitung" auf dem Förderantrag 1997 für das Land Brandenburg

9.1 Brandenburgisches Abfallgesetz

Nachdem das Kreislaufwirtschafts- und Abfallgesetz[147] des Bundes im Oktober vergangenen Jahres in Kraft getreten ist und sich der bundesgesetzliche Rahmen geändert hat, ist eine Änderung der Landesabfallgesetze in allen Bundesländern notwendig geworden. Daher hat mir das Ministerium für Umwelt, Naturschutz und Raumordnung (MUNR) mehrere Entwürfe für ein neues Brandenburgisches Abfallgesetz (BbgAbfG) vorgelegt, mit dem das bis jetzt geltende Vorschaltgesetz abgelöst werden soll. Nach einem längeren Gedankenaustausch hierüber liegt jetzt eine Entwurfsform vor, die im großen und ganzen auch den datenschutzrechtlichen Anforderungen gerecht wird.

Grundsätzlich begrüßenswert ist die vorgesehene bereichsspezifische Datenschutzregelung in § 40 E-BbgAbfG. Zwar gehen aus der Regelung selbst Voraussetzungen und Umfang von Beschränkungen des Rechts auf informationelle Selbstbestimmung nicht hervor, zumindest enthält die Regelung jedoch in Absatz 2 die Ermächtigung für eine Rechtsverordnung, in der die Eingriffsbefugnisse festgelegt werden sollen. Mit dieser Vorgehensweise, den Datenschutz in einer allgemeinen, übergreifenden Vorschrift zu regeln, wollte das MUNR eine Überfrachtung der einzelnen Verfahrensvorschriften mit datenschutzrechtlichen Voraussetzungen verhindern.

Ergänzungsbedürftig waren die Datenschutzvorschriften insoweit, als der Regierungsentwurf eine Löschungsmöglichkeit von Daten nicht vorsah. Dieser Umstand, den schließlich auch das MUNR für korrekturbedürftig hielt, ließ sich im Verlaufe der parlamentarischen Behandlung auf meine Empfehlung hin abstellen. § 40 Abs. 1 als auch Abs. 2 E-BbgAbfG ist nunmehr um eine Löschungsbefugnis ergänzt.

Unbestritten ist die Notwendigkeit von Katastern und sonstigen Informationssammlungen über Altlasten, -flächen usw. Mit den in ihnen enthaltenen Daten, ist jedoch durch den Grundstücksbezug gleichzeitig ein Personenbezug möglich. Der betroffene Personenkreis muß aber vor unberechtigten Eintragungen geschützt werden. Die Feststellung einer Kontamination des Grundstückes hat nämlich einerseits Auswirkungen auf den Verkaufswert, und andererseits zieht sie möglicherweise auch die Verpflichtung einer Sanierung nach sich, so daß hier eine Falscheintragung erhebliche Auswirkungen haben kann. Daraus wird die Erforderlichkeit einer Löschungsregelung deutlich.

Darüber hinaus müssen Verbindlichkeiten und Rechtssicherheit für den Bearbeiter wie den Betroffenen hergestellt werden. Das Ministerium ist daher aufgefordert, die Ermächtigung in eine Rechtsverordnung umgehend umzusetzen.

Positiv zu bewerten ist, daß die Möglichkeit der Behörden, Informationen und Hinweise zu veröffentlichen, in § 41 E-BbgAbfG ausdrücklich geregelt wird. Hiernach muß bei der Abwägung des Informationsbedürfnisses der Öffentlichkeit gegenüber den schutzbedürftigen Interessen des Betroffenen das Recht auf informationelle Selbstbestimmung besonders berücksichtigt werden.

9.2 Immissionsschutzdatenverordnung - noch immer überfällig

[147] vom 27. September 1994, BGBl. I S. 2705

Nachdem ich bereits im 2. Tätigkeitsbericht[148] über die geplante Umsetzung der Ermächtigungsvorschrift für eine Immissionsschutzdatenverordnung in § 20 Abs. 2 Landesimmissionsschutzgesetz (LImschG)[149] berichtet hatte, bin ich erneut zu einer Stellungnahme zu dem jetzt vorliegenden, in einigen Punkten veränderten Entwurf aufgefordert worden.

Der Verordnungsentwurf, der gerade den datenschutzrechtlichen Belangen dienen soll, wird in der vorliegenden Fassung seinem Schutzzweck immer noch nicht gerecht, auch wenn zwischenzeitlich einige aus datenschutzrechtlicher Sicht positive Änderungen und Ergänzungen hineingekommen sind. Die in der Verordnungsermächtigung in § 20 LImschG vorgesehenen materiellen Regelungen zum informationellen Selbstbestimmungsrecht sind zum Teil nicht umgesetzt worden:

- Eine Einzelnennung der zu verarbeitenden Daten ist in der Verordnung nicht erfolgt, da sich diese aus dem jeweiligen Gesetzeszweck ergeben soll.

- Auch eine genauere Bestimmung, für welche Verwendungszwecke eine Datenverarbeitung zulässig ist, findet sich in der Verordnung nicht, statt dessen ist eine Aufzählung, die jedoch nach Angaben des MUNR nie vollständig sein könne, in die zugehörige Verwaltungsvorschrift gewandert. Dies entspricht aber nicht dem Gesetzesvorbehalt für die mit den Verwendungszwecken verbundenen Grundrechtseingriffe.

- Ebenso fehlen nähere Bestimmungen zu Auskunftspflichten und -rechten mit der Begründung, daß sich dies schon im einzelnen aus dem anzuwendenden, die Materie regelnden Gesetz ergebe.

Abgesehen von den zuvor genannten Punkten sind jedoch einige meiner Anregungen aufgegriffen worden, so daß die Ermächtigungsnorm zumindest teilweise durch den jetzt vorliegenden Entwurf ausgefüllt wird:

- Die vorher bestehenden Unklarheiten der Begriffsbestimmungen sind insofern aus dem Wege geräumt, als jetzt diejenigen des § 20 LImschG Anwendung finden und ansonsten das Brandenburgische Datenschutzgesetz gilt. Dies trägt insgesamt zur Normenklarheit der Verordnung bei.

- Außerdem sollen sich aus der subsidiären Anwendbarkeit des Brandenburgischen Datenschutzgesetzes auch Art und Umfang der Auskunftsrechte ergeben.

- Hinzugekommen ist eine eigene Vorschrift zu den Voraussetzungen und Fristen für die Löschung von Daten, während die von mir geforderte Möglichkeit der Sperrung lediglich durch die subsidiäre Anwendung des Brandenburgischen Datenschutzgesetzes erreicht werden soll.

Der Verordnungsentwurf liegt nun den Spitzenverbänden vor und wird, soweit von dort keine gravierenden Bedenken geäußert werden, in dieser datenschutzrechtlich nur teilweise befriedigenden Form dem Kabinett zur Beschlußfassung vorgelegt werden.

---

148 s. unter 8.3

149 vom 3. März 1992, GVBl. I S. 78

10 Stadtentwicklung, Wohnen und Verkehr

10.1 Stadtentwicklung

10.1.1 Brandenburgisches Architektengesetz

In dem inzwischen verabschiedeten Brandenburgischen Architektengesetz (BbgArchG)[150] sind meine Empfehlungen zu § 24 (Daten, Auskunfts- und Verschwiegenheitspflicht) weitgehend unberücksichtigt geblieben. Das Gesetz bleibt in dieser Vorschrift zu unbestimmt, daß für den Bürger entgegen den eindeutigen verfassungsrechtlichen Vorgaben[151] die Beschränkungen seines Grundrechts auf informationelle Selbstbestimmung nicht klar und erkennbar werden. Dies wird durch die mehrfache Verwendung des Begriffs "grundsätzlich" deutlich. Obgleich die allgemeinen Grundsätze der Datenverarbeitung im Brandenburgischen Datenschutzgesetz normiert sind und es gerade die Aufgabe des Gesetzgebers ist, diese Grundsätze bereichsspezifisch so zu spezifizieren, daß sich eine eindeutige aufgabenbezogene Befugnis ergibt, wiederholt § 24 BbgArchG im wesentlichen nur die allgemeinen Aussagen des Brandenburgischen Datenschutzgesetzes. Unbestimmt bleibt jedoch, welche Datenverarbeitungsbefugnisse der datenverarbeitenden Stelle im Vollzug des Gesetzes konkret zustehen sollen.

Im einzelnen habe ich u. a. auf folgende Mängel hingewiesen:

- Die Überschrift ist hinsichtlich des tatsächlichen Regelungsinhalts irreführend.
- Unterschiedliche Definitionen der datenverarbeitenden Stelle innerhalb der Vorschrift.
- Unzulängliche Regelung der Voraussetzungen für die Veröffentlichungs- und Übermittlungsbefugnisse der datenverarbeitenden Stelle.

10.1.2 Neufassung von Verwaltungsvorschriften für die Wohnungsämter

Das Ministerium für Stadtentwicklung, Wohnen und Verkehr (MSWV) hat zwei Verwaltungsvorschriften für die Arbeit der Wohnungsämter neu gefaßt[152]. Zu den datenschutzrechtlich bedeutsamen Regelungen hat sich das MSWV dabei eng mit mir abgestimmt und mir zwischenzeitlich zugesagt, daß es meine Empfehlungen in den Endfassungen der Vorschriften berücksichtigen werde:

- Die Verwaltungsvorschrift zum Wohnungsbindungsgesetz

Zum Entwurf des MSWV waren lediglich einige kleinere Verbesserungen anzuregen, bei denen es sich im wesentlichen um Klarstellungen der Aussagen und Hinweise auf erfahrungsgemäß nicht bekannte oder häufig übersehene datenschutzrechtliche Vorschriften handelte. So wird in der Verwaltungsvorschrift nunmehr z. B. auf die Regelungen zur Form einer Einwilligung nach § 4 Abs. 2 BbgDSG ebenso hingewiesen werden, wie auf die Rechtslage bei der Benennung von Wohnungssuchenden für Wohnraum (s. unter 12.5.1). Ferner werden die Vorgaben der Verwaltungsvorschrift für die Inhalte der Einwilligungserklärung zur Benennung und für die Einzelangaben im Wohnberechtigungsschein konkretisiert werden.

---

150 vom 7. April 1997, GVBl. I S. 20

151 vgl. BVerfGE 65, 1 (44)

152 Die Neufassungen waren bei Redaktionsschluß noch nicht im Amtsblatt bekannt gemacht.

- Der Einkommensprüfungserlaß

Hier konnte zum einen mit dem MSWV eine geeignete Formulierung für die Hinweise zur Datenverarbeitung nach § 12 Abs. 3 BbgDSG entwickelt werden, die das Ministerium in das Merkblatt "Erläuterungen zu den Einkommenserklärungen" aufnehmen wird, das den Betroffenen mit den als Anlage zu dem Erlaß vorgegebenen Erklärungsvordrucken auszuhändigen ist. Zum anderen konnten unter Berücksichtigung einer Stellungnahme des Landesrechnungshofes, die ich dazu vorab eingeholt hatte, die Anforderungen an die Dokumentation von Einkommensnachweisen präzisiert werden. Die Regelung in dem Einkommensprüfungserlaß wird diesbezüglich künftig im wesentlichen folgendes vorsehen:

Den Einkommenserklärungen sind geeignete Einkommensnachweise (z. B. Steuerbescheid, Einkommensbescheinigung des Arbeitgebers, Rentenbescheid u. ä.) beizufügen. Die Nachweise sind im Original oder in beglaubigter Abschrift vorzulegen. Eine Kopie der vorgelegten Nachweise muß mit den Einkommenserklärungen zu den Akten genommen werden. Dabei brauchen in entsprechender Anwendung von § 14 Abs. 2 BbgDSG i. V. m. § 4 Abs. 1 Buchst. b BbgDSG etwaige zur Überprüfung der Einkommensverhältnisse nicht erforderliche Angaben (z. B. über die Religionszugehörigkeit, über den Arbeitgeber u. ä.) nicht unkenntlich gemacht zu werden; eine Nutzung solcher Angaben ist allerdings unzulässig. Die Betroffenen können selbst Kopien vorlegen, in denen die zum Nachweis ihrer Einkommensverhältnisse nicht benötigten Angaben unkenntlich gemacht sind; dann sind diese Kopien zu den Akten zu nehmen. Bezüglich der für die Einkommensprüfung erforderlichen Angaben ist die Übereinstimmung der von den Betroffenen vorgelegten Kopien mit den Originalen zu überprüfen. Im übrigen sind Art und Ergebnis der Einkommensprüfung aktenkundig zu machen.

Die zu den Akten genommenen Einkommenserklärungen und -nachweise sind bei einer vollständigen oder auch nur teilweisen Bewilligung der beantragten Leistung für fünf Jahre aufzubewahren. Nach Ablauf dieser Aufbewahrungsfrist sind sie zu vernichten. Wird dagegen der Antrag insgesamt abgelehnt, so sind diese Unterlagen bereits spätestens sechs Monate nach Eintritt der Bestandskraft der Entscheidung zu vernichten oder an den Antragsteller zurückzugeben.

10.1.3 Anträge auf Wohnungsbauförderung

Das Zweite Wohnungsbaugesetz (II. WoBauG)[153] sieht in den §§ 88 ff. II. WoBauG auf unterschiedlichen Förderungswegen die Förderung des Wohnungsbaues durch besondere Maßnahmen und Vergünstigen vor. Der einheitliche Vordruck, mit dem die Bauherren ihren Antrag auf Aufnahme in das Förderprogramm bei der Investitionsbank des Landes Brandenburg (ILB) stellen, wurde vom MSWV im Berichtszeitraum überarbeitet. Dabei ist das MSWV meinen Empfehlungen für eine datenschutzgerechte Gestaltung des Hinweises zur Datenverarbeitung nach § 12 Abs. 3 BbgDSG[154] in vollem Umfang gefolgt.

Hinsichtlich der einkommensorientierten Wohnungsbauförderung sieht ein vom MSWV begleitetes kommunales Modellprojekt gem. § 88 e II. WoBauG neben der Grundförderung durch Gewährung eines Baudarlehens an den Bauherren eine Zusatzförderung durch Gewährung eines einkommensabhängigen Zuschusses an die Mieter vor. Dabei soll das Einkommen nach Maßgabe des Einkommensprüfungserlasses[155] nur gegenüber dem zuständigen Wohnungsamt

---

153 i. d. Fass. vom 19. August 1994, BGBl. I S. 2137, zul. geänd. d. Ges. vom 18. Dezember 1995, BGBl. I S. 1959

154 s. 4. Tätigkeitsbericht unter 2.3

155 s. unter 10.1.2

nachzuweisen sein, so daß es zu keiner Offenlegung der Einkommensverhältnisse der Mieter gegenüber dem Vermieter (Bauherren) käme. Die datenschutzrechtliche Ausgestaltung des Mietvertrages ist allerdings derzeit noch nicht abschließend geklärt. Das MSWV hat mir insoweit mitgeteilt, daß es sich dazu an mich wenden werde, sobald die für Anfang 1998 angekündigte Bezugsfertigkeit der Wohnungen des Modellprojekts konkret absehbar sei.

10.1.4 Datenverarbeitung durch private Planungsbüros als Sanierungsbeauftragte

Nachdem im Berichtszeitraum die Kontrollkompetenzen bzgl. privater Planungsbüros einvernehmlich geklärt worden sind, hat das MSWV mir inzwischen zugesagt, die Belange des Datenschutzes bei der Beauftragung privater Planungsbüros mit der Vorbereitung und Durchführung von Maßnahmen zur Stadterneuerung in dem Mustertreuhändervertrag über die Durchführung städtebaulicher Sanierungsmaßnahmen, der sich zur Zeit als Anlage 21 der Förderrichtlinie ´96 zur Stadterneuerung[156] in Vorbereitung befindet, so konkret und detailliert zu berücksichtigen, wie dies vom MI und mir übereinstimmend empfohlen wurde. Insbesondere sollen Hinweise zum technisch-organisatorischen Datenschutz nach Maßgabe von § 9 BDSG gegeben und darauf hingewiesen werden, daß die Beschäftigten des Sanierungsbeauftragten gem. § 5 Satz 2 BDSG schriftlich auf das Datengeheimnis zu verpflichten sind. Ferner wird die strikte Zweckbindung nach § 138 Abs. 2 Baugesetzbuch (BauGB) in den Mustervertrag ausdrücklich mit aufgenommen. Schwerwiegende Verstöße gegen den Datenschutz als besonderer Kündigungsgrund ebenso wie eine umfassende Herausgabepflicht bezüglich sämtlicher Unterlagen mit personenbezogenen Daten sollten vereinbart werden. Ich hoffe, daß - wie vom MI empfohlen - auch noch Regelungen zur Ausübung der datenschutzrechtlichen Kontrolle durch den betrieblichen Datenschutzbeauftragten des Sanierungsbeauftragten sowie durch die auftraggebende Verwaltung mit in den Mustervertrag aufgenommen werden.

Das MI und das MSWV haben sich im übrigen bereit erklärt, die datenschutzrechtlichen Aspekte der Beauftragung privater Planungsbüros bei der Vorbereitung oder Durchführung städtebaulicher Sanierungsmaßnahmen in einem für die Kommunalverwaltungen bestimmten Beitrag, der in einer der nächsten Ausgaben der vom MI herausgegebenen Informationsschrift "Brandenburg Kommunal" und/oder der vom MSWV herausgegebenen Informationsschrift "MSWV - aktuell" erscheinen wird, zusammenfassend darzustellen.

10.2 Bau- und Wohnungswesen

10.2.1 Wohnungskarteien der ehemaligen DDR

[156] vom 18. März 1996, ABl. S. 526

Die Wohnungskarteien, die in der ehemaligen DDR bei den Gemeinden in der Regel im Bereich der Wohnraumlenkung zum Zweck der Wohnungsbestandsfortschreibung geführt und bis zum 31. Dezember 1989 regelmäßig aktualisiert wurden, dürften in ihrer ursprünglichen Form und in ihrem ursprünglichen Umfang eigentlich nicht mehr vorhanden sein[157]. Doch noch immer gibt es diese Karteien nicht nur rechtmäßig als kommunales Archivgut in den Gemeindearchiven, sondern auch in den Ablagen des Verwaltungsvollzugs bei den Wohnungsämtern. Dies hat sich nach einer Auswertung einer vom MSWV nachdrücklich beförderten Umfrage bei den Kommunalverwaltungen bestätigt.

Mit Rundschreiben vom 11. April 1996 hatte das MSWV meiner Empfehlung entsprochen und die Landkreise und kreisfreien Städte noch einmal darauf hingewiesen, daß aus den Karteien die personenbezogenen Daten zu Wohnungen, die weder unter das Wohnungsbindungsgesetz[158] noch unter das Brandenburgische Belegungsbindungsgesetz[159] fallen, zu löschen sind. Insbesondere bei größeren Wohnraumverwaltungen sind die danach notwendigen partiellen Löschungen jedoch vor allem bei den kreisfreien Städten mit einem Verwaltungsaufwand verbunden. Ich habe es deshalb als Übergangslösung für vertretbar gehalten, die Löschung der Daten erst im Rahmen des Aufbaus einer neuen und vorzugsweise automatisierten Wohnraumdatei vorzunehmen, und die zu löschenden Angaben bis dahin als gesperrt zu behandeln.

Nach den mir bislang vorliegenden Rückmeldungen wurden nach 1990 die alten Wohnraumkarteien bei einigen Verwaltungen vollständig vernichtet und im Rahmen des zur gesetzlichen Aufgabenerfüllung Erforderlichen neue Dateien aufgebaut. Andere Verwaltungen haben die Karteien komplett dem Kommunalarchiv übergeben und wieder andere haben sie in einem Kellerraum der Verwaltung weggelegt. Der letzte Fall, bei dem die Datensammlung jedoch im Verwaltungsvollzug verbleibt, scheint gelegentlich mit einer Übergabe an das Kommunalarchiv verwechselt worden zu sein. Einige Verwaltungen haben es unternommen, die nicht benötigten und offenbar meist mit Bleistift vermerkten personenbezogenen Angaben auf den Karteikarten auszuradieren.

Bei der Anzahl der Gemeinde- und Amtsverwaltungen ist es mir nicht möglich, die Angaben der Kommunen im einzelnen zu überprüfen. Hinsichtlich der weiteren Bereinigung der Altdatenbestände im Bereich der Wohnraumverwaltungen nach Maßgabe des o. g. Rundschreibens des MSWV sehe ich insoweit neben den datenverarbeitenden Stellen selbst in erster Linie die Landkreise im Rahmen ihrer Sonderaufsicht gefordert.

Die Gemeinde- und Amtsverwaltungen sind meiner Bitte eher zögerlich nachgekommen. Anfang November 1996 lagen mir erst von knapp einem Drittel der Kommunalverwaltungen (darunter sämtliche kreisfreien Städte) Rückmeldungen vor. Von den Landkreisen hatten lediglich vier geantwortet, wobei nur in zwei Fällen die Antworten sachgemäß waren. Den Landkreisen Ostprignitz-Ruppin und Prignitz war es möglich gewesen, mir die Rückmeldungen der kreisangehörigen Kommunalverwaltungen in einer übersichtlichen Zusammenstellung zu übermitteln. In der Folge erinnerte das MSWV auf meine Bitte hin die Landkreise noch zweimal, an die Beantwortung meiner im Juni 1996 übermittelten Anfrage. Bis zum Ende des Berichtszeitraums erhielt ich daraufhin auch von den übrigen Landkreisen mit Ausnahme der Landkreise Elbe-Elster und Oberhavel eine Antwort.

---

157 s. 3. Tätigkeitsbericht unter 9.1.2

158 i. d. Fass. vom 19. August 1994, BGBl. I S. 2166

159 vom 26. Oktober 1995, GVBl. I S. 256

11 Finanzen und Wirtschaft

11.1 Errichtung der Zentralen TK-Anlage in Wünsdorf

Im September 1995 bat mich das für die Errichtung einer zentralen Telekommunikationsanlage (TK-Anlage) in der Waldstadt Wünsdorf zuständige Landesbauamt Potsdam um die Bestätigung der datenschutzrechtlichen Unbedenklichkeit für den Betrieb der TK-Anlage. Da dem Antrag als Unterlagen lediglich ein Liegenschaftsplan und eine Auflistung der als Nutzer vorgesehenen Einrichtungen und Behörden beigefügt war, konnte ich dem Wunsch nicht nachkommen und bat daher das Landesbauamt zunächst einmal um weitere Informationen

- zu den in der TK-Anlage aktivierten Leistungsmerkmalen,
- zum gewählten Verfahren der Gebührendatenverarbeitung,
- zur Organisation der Abrechnung von Dienst- und Privatgesprächen und
- zur räumlichen Unterbringung der TK-Anlage und der Gebührencomputer.

Aufgrund meiner bei der Prüfung von TK-Anlagen gemachten Erfahrungen habe ich Informationsmaterialien mit meinen Vorstellungen zu einem datenschutzschutzgerechten Betrieb derartiger Anlagen beigefügt. Darüber hinausgehend verwies ich insbesondere auf die Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher TK-Anlagen für die Verwaltung des Landes Brandenburg (Dienstanschlußvorschrift - DAV)[160] und die Musterdienstvereinbarung über die Nutzung der ISDN-Telekommunikationsanlagen des TK-Verbundes der obersten Landesbehörden, die als Muster für alle Landesbehörden Brandenburgs dienen soll. Ich halte es für nicht akzeptabel, wenn einzelne untergeordnete Landesbehörden in datenschutzrelevanten Punkten hinter dieser Musterdienstvereinbarung zurückbleiben.

[160] Runderlaß des Ministeriums der Finanzen Nr. 17 - 01340/180/93 vom 30. November 1993, ABl. S. 1775

Bei einem gemeinsamen Gespräch mit dem Landesbauamt Potsdam, dem zukünftigen Betreiber und der für die Lieferung und Programmierung der TK-Anlage verantwortlichen Firma stellte sich heraus, daß dem Anlagenlieferanten offensichtlich weder die für das Land Brandenburg geltenden Vorschriften zum Betrieb von TK-Anlagen noch meine bereits in früheren Tätigkeitsberichten erläuterten Forderungen zu ihrem datenschutzgerechten Betrieb bekannt waren. Das Landesbauamt hatte nämlich verabsäumt, diese Forderungen in die Anlagenausschreibung einfließen zu lassen, so daß sie die Lieferfirma auch nicht berücksichtigen konnte. Für zukünftige Ausschreibungen verweise ich deshalb besonders auf meine Ausführungen unter 1.3.2 dieses Berichtes, in dem ich wesentliche Forderungen zur Nutzung interner TK-Anlagen dargestellt habe[161].

Insgesamt würde ich es begrüßen, wenn meine Behörde zukünftig in vergleichbaren Fällen frühzeitig in die datenschutzgerechte Gestaltung neuer TK-Anlagen einbezogen würde, da ich glaube, daß durch eine vorherige Beratung und Beteiligung im Ergebnis mehr für die Einhaltung datenschutzrechtlicher Bestimmungen erreicht werden kann als mit nachträglichen Kontrollen. Bisher gehe ich davon aus, daß meine Hinweise in der TK-Anlage in Wünsdorf noch genügend Berücksichtigung finden werden. Zu einem späteren Zeitpunkt werde ich mich davon überzeugen.

11.2 Sonstiges

11.2.1 Datenschutz bei der Feuersozietät/Öffentliche Leben Berlin Brandenburg

Die Feuersozietät hatte in bundesweiter Abstimmung der Versicherungsunternehmen mit den für den nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden für den Datenschutz Ende 1995 die sog. Allfinanzklausel auch in bereits bestehende Versicherungsverträge eingeführt und dabei die Einwilligung der betroffenen Versicherungsnehmer für den Fall fingiert, daß diese der danach erlaubten Nutzung der Versichertendaten auch für anderweitige Leistungsangebote des Versicherungsunternehmens nicht widersprachen. Zwei Betroffene hatten dies gegenüber der Feuersozietät getan und zugleich nach § 34 BDSG Auskunft über die dort zu ihrer Person gespeicherten Daten verlangt. Als die Antwort der Feuersozietät nicht zu ihrer Zufriedenheit ausfiel, wandten sie sich an mich, mit der Bitte, die Rechtmäßigkeit der Datenverarbeitung bei der Feuersozietät zu überprüfen.

In der Folge ergab sich eine sehr kooperative Erörterung der Sach- und Rechtslage zwischen der Feuersozietät, dem Berliner Datenschutzbeauftragten und mir, in deren Ergebnis die Feuersozietät die Petenten über das Maß ihrer gesetzlichen Verpflichtungen hinaus mit einer umfassenden Auskunft zufriedenstellte. Im Hinblick darauf, daß zum Zeitpunkt der Eingaben die Einführung der Allfinanzklausel in die bestehenden Versicherungsverträge bereits praktisch abgeschlossen war, stellte ich meine Bedenken gegen die dazu von der Feuersozietät vorgenommene Fiktion der Einwilligung in die Vertragsänderung durch Schweigen zurück.

[161] s. hierzu auch 2. Tätigkeitsbericht unter 1.4.1 sowie 11.1 und 3. Tätigkeitsbericht unter 10.3

Im übrigen nahm ich die Eingaben zum Anlaß, die Zuständigkeit zur Ausübung der datenschutzrechtlichen Kontrolle bei der Feuersozietät mit dem Berliner Datenschutzbeauftragten zu klären. Dabei ergab es sich, daß sich mangels einer anderweitigen Regelung gem. § 3 Satz 2 des Staatsvertrages[162] auch die datenschutzrechtliche Kontrolle formal und inhaltlich ausschließlich nach Berliner Landesrecht und also nach § 24 Abs. 1 i. V. m. § 2 Abs. 2 Berliner Datenschutzgesetz bestimmt. Daher habe ich - unbeschadet der zwischen dem Berliner Datenschutz-beauftragten und mir bereits früher vereinbarten engen Abstimmung[163] - keine Kontrollkompetenz gegenüber der Feuersozietät Berlin Brandenburg und der Öffentlichen Lebensversicherung Berlin Brandenburg.

11.2.2 Mitteilung von Prüfungsergebnissen an die Ausbildungsbetriebe

Innerhalb des sog. dualen Ausbildungssystems ist es erforderlich, daß die Ausbildungsbetriebe auch Kenntnis vom Leistungsstand des Auszubildenden in den theoretischen Ausbildungsabschnitten erhalten. Dazu muß ihnen die zuständige Ausbildungsstelle ggf. die Ergebnisse theoretischer Leistungsprüfungen übermitteln dürfen, und zwar nicht nur dann, wenn es sich um eine Abschlußprüfung handelt, durch die eine einzelne Ausbildungsmaßnahme oder die Ausbildung insgesamt beendet wird, sondern auch dann, wenn die Prüfung lediglich einen einzelnen Ausbildungsabschnitt innerhalb der jeweiligen Ausbildungsmaßnahme beendet. Denn auch für eine verantwortliche Wahrnehmung der praktischen Ausbildung ist es für den Ausbildenden wichtig zu wissen, ob die von ihm getroffenen Ausbildungsmaßnahmen hinreichend sind, um ein qualifiziertes Bestehen der beruflichen Abschlußprüfung zu ermöglichen oder ob ggf. nach Art und Umfang Änderungen der von ihm zu verantwortenden Ausbildung gerade auch im Hinblick auf etwaige Theoriedefizite notwendig sind.

Zwar hat das Bundesverwaltungsgericht[164] zwischenzeitlich entschieden, daß es für den in der Übermittlung der Prüfungsergebnisse liegenden Eingriff in das Recht auf informationelle Selbstbestimmung im Berufsbildungsgesetz (BBiG)[165] eine hinreichende Rechtsgrundlage gibt. Die Rechtslage ist jedoch insgesamt nicht normenklar und hat bundesweit zu kontroversen Diskussionen geführt. Ich habe deshalb empfohlen, die Rechtsgrundlagen für eine Mitteilung von Ergebnissen aus theoretischen Leistungsprüfungen an die Ausbildungsbetriebe im Berufsbildungsgesetz normenklar zu präzisieren. Das Ministerium für Wirtschaft, Mittelstand und Technologie hat mir mitgeteilt, daß es sich im Rahmen einer nächsten Novellierung des Gesetzes für eine entsprechende Änderung von § 45 BBiG einsetzen werde.

11.2.3 Zustellung von Lohnsteuerkarten an Ehegatten

Das im wesentlichen bundeseinheitlich verwendete Merkblatt über die Ausstellung und Übermittlung der Lohnsteuerkarten durch die Gemeinden hatte auch im Land Brandenburg vorgesehen, die Lohnsteuerkarten für Ehegatten in nur einem Briefumschlag zuzustellen. Mit der Neufassung des Merkblatts für 1997[166] ist das Ministerium der Finanzen (MdF) auf meine Anregung hin in Übereinstimmung mit den übrigen Bundesländern der Empfehlung der Datenschutzbeauftragten gefolgt, die Lohnsteuerkarten auch bei Ehegatten einzeln in gesonderten Umschlägen zu versenden.

---

162 über die Feuersozietät Berlin Brandenburg und die Öffentliche Lebensversicherung Berlin Brandenburg vom 2. April 1993, GVBl. I S. 217

163 s. 2. Tätigkeitsbericht unter 1.2.3

164 BVerwG, Beschl. vom 31. Mai 1995 - 1 B 73.95

165 vom 14. August 1969, BGBl. I S. 1112

166 Vordruck LSt 20 - 1996 BB Nr. 645/501 (08/96) - OFD CB - St 11

11.2.4 Abwicklung der Bodenreform

Bei der Abwicklung der Bodenreform handelt es sich um eine zeitlich begrenzte Aufgabe[167], die im wesentlichen darin besteht, dem Landesfiskus diejenigen Flächen zur Verwertung und Verwaltung zuzuführen, für die er Berechtigter i. S. v. § 12 Abs. 2 EGBGB[168] ist. Die Durchführung dieser Aufgabe setzt voraus, daß die Berechtigung des Landesfiskus festgestellt und ggf. auf dem Rechtsweg durchgesetzt wird. Dazu sind umfangreiche Recherchen zu den Besitz- und Eigentumsverhältnissen an den Grundstücken erforderlich. Da die Fiskalverwaltung dafür nicht über genügend eigenes Personal verfügt, hat sich das MdF entschlossen, private Planungs- und Beratungsbüros mit der Durchführung der notwendigen Ermittlungen zu beauftragen.

In enger Abstimmung des MdF mit mir sowie unter Einbeziehung auch des Ministeriums des Innern konnte dazu eine Vertragsgestaltung gefunden werden, bei der die Auftragnehmer im Außenverhältnis grundsätzlich nur unselbständig als Erklärungs- bzw. Empfangsboten der Fiskalverwaltung auftreten und die für jene entscheidungserheblichen Informationen lediglich im Sinne einer Datenverarbeitung im Auftrag bei den Grundbuchämtern und anderen öffentlichen Stellen entgegennehmen (erheben) und zusammenstellen (speichern). Für diese Datenverarbeitungen werden die Auftragnehmer vertraglich in sorgfältiger Konkretisierung umfassend zum Datenschutz verpflichtet, so daß die Einhaltung der Vorschriften über den Datenschutz bei der Durchführung des Auftrags im Umfang von § 10 BbgDSG bestmöglich gewährleistet erscheint.

12 Kommunale Probleme

12.1 Gesundheitsämter - Schulärztliche Reihenuntersuchung

Zur Vorbereitung einer Schulreihenuntersuchung brachte das Kind einer Petentin einen Elternfragebogen[169] mit nach Hause. Die Petentin vermerkte darauf mit Datum und Unterschrift, daß ihr Kind an dieser Untersuchung nicht teilnehmen solle. Da die schulärztliche Untersuchung mit Inkrafttreten des Brandenburgischen Schulgesetzes[170] eine Pflichtveranstaltung der Schule ist, mußte das Kind an der Untersuchung teilnehmen. Dort wurde es vor anderen Schülern eingehend über die Familienverhältnisse - also auch zu Sozialdaten seiner Eltern - befragt. Danach erhob der Arzt medizinische Daten.

Ich habe das zuständige Gesundheitsamt darauf hingewiesen, daß für Untersuchungen und evtl. Befragungen im Rahmen einer schulärztlichen Reihenuntersuchung Räume zu wählen sind, die den Betroffenen nicht in die Lage bringen, vor Dritten personenbezogene Daten offenbaren zu müssen. Darüber hinaus ist es das gute Recht des Betroffenen, die im unmittelbaren Zusammenhang mit der Untersuchung erforderlichen Fragen nur gegenüber dem Arzt zu beantworten. Darüber ist der Betroffene vorher zu informieren. Die Erhebung von Angaben über andere Personen - wie im vorliegenden Fall der Eltern - setzt, sofern sie überhaupt erforderlich ist, voraus, daß diese damit einverstanden sind. Im vorliegenden Fall hatte die Mutter ihr Einverständnis jedoch durch ihren Hinweis, daß ihr Kind nicht an der Untersuchung teilnehmen soll,

---

167 vgl. die Richtlinie des Ministeriums für Ernährung, Landwirtschaft und Forsten dazu = Anl. 3 zu LT-Drs. 2/3398

168 Einführungsgesetz zum Bürgerlichen Gesetzbuch vom 18. August 1896, RGBL. S. 604; i. d. Fass. vom 21. September 1994, BGBl. I S. 2494

169 s. 4. Tätigkeitsbericht unter 7.2.3.3 sowie 2. Tätigkeitsbericht unter 7.2.2.4

170 vom 12. April 1996, GVBl. I S. 102

gerade ausgeschlossen.

Ich hoffe, daß die Darstellung des Einzelfalls dazu beitragen wird, Wiederholungsfälle, die ich förmlich beanstanden müßte, an anderer Stelle zu vermeiden. Das betreffende Gesundheitsamt hat sich unterdessen bei den Betroffenen entschuldigt und mir versichert, in Zukunft bei schulärztlichen Untersuchungen streng auf die Einhaltung datenschutzrechtlicher Belange zu achten und die unzulässig erhobenen Daten unverzüglich zu löschen.

12.2 Jugendämter

12.2.1 Unerlaubte Tonbandaufnahme

Während eines Gespräches mit einer Mitarbeiterin des Jugendamtes hatten die Eltern eines dort betreuten Kindes heimlich Tonbandaufzeichnungen mitgeschnitten. Erst nach Beendigung des Gespräches gab der Vater zu erkennen, daß er das Gespräch aufgezeichnet habe und zu Beweiszwecken verwenden wolle. Das Jugendamt bat mich um eine datenschutzrechtliche Bewertung des Vorfalls.

Ungeachtet eventuell bestehender zivilrechtlicher Ansprüche erfüllt dieser Sachverhalt den Straftatbestand des § 201 Abs. 1 Nr. 1 StGB[171]. Danach wird die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger unter Strafe gestellt. Ein zulässiger Mitschnitt hätte nur mit Zustimmung aller Beteiligten erfolgen dürfen. Ohne ihr Wissen ist der Schutzbereich des Persönlichkeitsrechts verletzt. Dies gilt grundsätzlich auch für Gespräche in Ämtern. Da der Tonbandmitschnitt ohne Zustimmung der Mitarbeiterin des Jugendamtes erfolgte und damit unzulässig war, habe ich dieser anheim gestellt, einen Strafantrag gem. § 205 Abs. 1 StGB wegen der Verletzung des vertraulich nichtöffentlich gesprochenen Wortes bei einem Gericht oder der Staatsanwaltschaft innerhalb der Antragsfrist von drei Monaten zu stellen.

12.2.2 Datenweitergabe zwischen Sozialamt und Jugendamt

Zu klären war die Frage, ob das Amt für Soziales und Wohnen im Sinne des "Kindeswohls" nach SGB VIII[172] das Jugendamt über die bevorstehende Räumung einer Wohnung, in der Kinder leben, informieren darf.

---

171 i. d. Fass. vom 10. März 1987, BGBl. I S. 49, ber. S. 1160

172 i. d. Fass. vom 3. Mai 1993, BGBl. I S. 637, zul. geänd. d. Ges. vom 15. März 1996, BGBl. I S. 477

Als Grundlage für eine solche Datenübermittlung käme lediglich § 69 Abs. 1 Nr. 1 SGB X[173] in Betracht. Danach ist die Übermittlung von Sozialdaten nur zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe des Empfängers. Hier ist jedoch zu fragen, ob vorbeugende Maßnahmen zum Wohle des Kindes aus Sicht des Jugendamtes notwendig werden.

Die Kenntnis der Obdachlosigkeit müßte somit für eine Leistungsgewährung im Sinne des SGB VIII erforderlich sein. Verschiedene Hilfearten (wie z. B. die Sozialpädagogische Familienhilfe gem. § 31 SGB VIII) können nur gewährt werden, wenn die Familie wenigstens grundsätzlich bereit ist, an einem Gelingen des Hilfekonzeptes mitzuarbeiten. Die Hilfeart führt nicht zum gewünschten Erfolg, sofern es sich hierbei um eine Familie handelt, die gleichzeitig vom Jugend- und vom Sozialamt betreut wird, und die das Jugendamt nicht selbst über den Umstand der drohenden Obdachlosigkeit informiert. In diesen Fällen sollte das Sozialamt von einer Datenübermittlung absehen und statt dessen den Betroffenen empfehlen, sich im Interesse des Kindeswohls selbst an das zuständige Jugendamt zu wenden.

In einem interministeriellen Merkblatt[174] wird zusätzlich auf die Beratungs- und Unterstützungsaufgaben des Jugendamtes zur Vermeidung von Obdachlosigkeit und zur Verbesserung der Lage obdachloser Personen - darunter Jugendlicher - in den Kommunen des Landes Brandenburg hingewiesen. In diesem Zusammenhang soll insbesondere auf folgenden Punkt aufmerksam gemacht werden:

Ist das Wohl eines Minderjährigen allgemein oder im Zusammenhang mit Wohnungsnot gefährdet, leitet das Jugendamt, möglichst in Zusammenarbeit mit dem Personensorgeberechtigten, Maßnahmen zum Schutz des Minderjährigen ein. Sofern die Personensorgeberechtigten nicht bereit oder in der Lage sind, die Gefährdung abzuwenden, informiert das Jugendamt gem. § 50 Abs. 3 SGB VIII das Vormundschaftsgericht. Gem. § 42 SGB VIII besteht die Verpflichtung des Jugendamtes, Minderjährige im Rahmen vorläufiger Maßnahmen zum Schutz von Kindern und Jugendlichen in Obhut zu nehmen. Die Verpflichtung zur Inobhutnahme besteht dann, wenn Kinder oder Jugendliche das wünschen, was z. B. bei obdachlosen Jugendlichen möglich ist.

12.3 Gewerbeämter

12.3.1 Prüfung von Gewerbeämtern

Bei zwei kreisfreien und einer kreisangehörigen Stadt sowie bei zwei Ämtern kontrollierte ich die Einhaltung datenschutzrechtlicher Vorschriften in Gewerbeämtern. Dabei wurden zum Teil Rechtsfragen aufgeworfen, die im nachhinein einvernehmlich mit dem Ministerium für Wirtschaft, Mittelstand und Technologie (MW) geklärt werden konnten. Eine gemeinsame Auswertung meiner Feststellungen und der in den Beratungen aufgetretenen Fragen hat das MW inzwischen in Abstimmung mit dem MI in einem mit mir erarbeiteten Rundschreiben an die Gewerbeämter[175] zu einer Art praxisorientierter Kommentierung der maßgeblichen gewerbe- und datenschutzrechtlichen Bestimmungen, darunter u. a.

---

173 vom 18. August 1980, BGBl. I S. 1469, ber. S. 2218; vom 4. November 1982, BGBl. I S. 1450, zul. geänd. d. Art. 6 des UVEG vom 7. August 1996, BGBl. I S. 1254

174 Gemeinsame Empfehlungen des MASGF, des MBJS, des MSWV und des MI zur Vermeidung von Obdachlosigkeit und zur Verbesserung der Lage obdachloser Personen in den Kommunen des Landes Brandenburg vom 24. Januar 1997, ABL S. 100

175 Nr. 6/1997 vom 8. April 1997 nebst Anlage

- Aktenführung,
- Aufbewahrungsfristen,
- Formulargestaltung,
- Anforderungen von Zentralregisterauskünften,
- Überprüfung der Zuverlässigkeit der Gewerbetreibenden,
- Gewerbeanzeigen an Krankenkassen,
- Auskunftserteilung an Finanzbehörden und
- Datenübermittlung an Ausländerbehörden

zusammengefaßt. Es ist zu hoffen, daß sie den Gewerbeämtern helfen wird, Verstöße gegen die Vorschriften über den Datenschutz bei der Wahrnehmung ihrer Aufgaben zu vermeiden.

Unter den festgestellten technisch-organisatorischen Mängeln fielen die folgenden besonders auf; aufgrund meiner Hinweise sind sie zwischenzeitlich beseitigt worden:

- Dateibeschreibung und Geräteverzeichnis

Dateibeschreibungen nach § 8 Abs. 1 BbgDSG und Geräteverzeichnisse nach § 8 Abs. 4 BbgDSG fehlten oder waren nur unvollständig ausgefüllt. Ich verweise an dieser Stelle auf die Verordnung zur Dateibeschreibung (DBeschrV)[176], in der als Anlage die entsprechenden Musterformblätter enthalten sind.

- Dokumentation zur Netzwerkkonfiguration

Die meisten Datenverarbeitungssysteme der Gewerbeämter werden auf lokalen Netzen betrieben. Die Netzwerke sind zwar meist schematisch dargestellt und die Zugriffsrechte auf dem Rechner abrufbar. In den meisten Fällen fehlten jedoch die Dokumentationen zur Netzwerkkonfiguration.

- Zugriffsrechte der Softwarehersteller

In zwei Fällen mußte festgestellt werden, daß der Softwarelieferant noch als Nutzer mit Supervisorrechten eingerichtet war oder er als Vertreter des Systemverwalters fungierte und ihm das Supervisorpaßwort bekannt war. Auf meine Forderung hin hat die Behörde diese Verfahrensweise abgestellt, die allen Geboten des Datenschutzes widerspricht, und einen eigenen Mitarbeiter der Behörde als Vertreter benannt. Bezüglich der Fragen der Wartung/Fernwartung verweise ich hier lediglich auf Anlage 9 dieses Tätigkeitsberichtes.

- Sicherheit der Server

Server von Netzwerken unterliegen einer besonderen Sicherheitsstufe. Sie sollten in einem gesonderten Raum untergebracht werden, der dementsprechend geschützt ist. Vor Ort fand ich Server, die in Sekretariaten aufgestellt waren. In einem anderen Amt wurde zwar ein spezieller Rechnerraum beim Neubau eingeplant. Beim Bezug entschied man jedoch, den Server in einem anderen Raum unterzubringen, der jedoch nicht ausreichend gesichert war.

---

[176] vom 7. Oktober 1996, GVBl. II S. 695

- Datensicherung

Eine regelmäßige Datensicherung erfolgte in allen Ämtern. Teilweise mußte ich jedoch die Lagerung der Sicherungsdatenträger bemängeln. Sicherheitskopien sollten nie im gleichen Raum aufbewahrt werden, in dem sich der Rechner mit den Originaldaten befindet. Weiterhin ist zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (§ 10 Abs. 2 BbgDSG).

- Aktenführung

Der Eindruck, den ich hierzu aus einigen Stichproben gewonnen habe, ist sehr uneinheitlich. Er hat mir zu folgendem allgemeinen Hinweis Veranlassung gegeben:

Zu jedem Vorgang muß eine schriftliche, abschließend gezeichnete Verfügung ergehen, die die bearbeitende Person und die geschäftsmäßige und sachliche Erledigung erkennen läßt und deren Nachprüfung ermöglicht. Diese Verfügungen sind Urkunden, die im Original in der Akte dokumentiert sein müssen. Eine Kopie der Reinschrift kann die Verfügung nicht ersetzen. Es empfiehlt sich, Akten grundsätzlich chronologisch zu führen und ggf. in Teilakten zu untergliedern; letzteres insbesondere dann, wenn für die Unterlagen in einer Akte unterschiedliche Aufbewahrungsfristen laufen.

Aus der Akte muß jeder rechtlich erhebliche Bearbeitungsschritt hervorgehen. Dies gilt insbesondere für Auskünfte, die aus der Akte erteilt werden und sonstige Übermittlungen personenbezogener Daten an Dritte einschließlich der Datenweitergabe innerhalb der Verwaltungseinheit (z. B. Gemeinde), der das Gewerbeamt angehört. Dazu kann es sich insbesondere auch im Hinblick auf die nach § 14 Abs. 5 GewO[177] vorgesehenen Regelübermittlungen empfehlen, die Akte mit einem Vorblatt zu versehen, auf dem verfügte und ausgeführte Übermittlungen und Datenweitergaben angekreuzt werden können.

Akten mit Unterlagen aus der ehemaligen DDR habe ich nur in einem Fall überprüft, in dem die nach dem geltenden Gewerberecht nicht mehr benötigten Daten (Ableistung des Wehrdienstes, Mitgliedschaften in Massenorganisationen, Auszeichungen einschließlich der damit verbundenen Geldprämien) aus der Akte noch nicht entfernt worden waren. Das betreffende Gewerbeamt hat mir inzwischen mitgeteilt, daß es daraufhin eine Bereinigung seiner Altdatenbestände durchgeführt habe.

- Formulargestaltung

[177] i. d. Fass. vom 1. Januar 1987, BGBl. I S. 425; zul. geänd. d. G. vom 7. August 1996, BGBl. I S. 1246

Die Formulargestaltung erwies sich durchgängig als nicht datenschutzgerecht. Dies ist zum einen auf die Bedingungen zurückzuführen, unter denen bei Aufnahme der Tätigkeit in den Gewerbeämtern die Vordrucke beschafft oder selbst erstellt werden mußten. Zum anderen liegt es jedoch ganz wesentlich daran, daß die Vorschrift des § 12 Abs. 3 BbgDSG[178], die zu einer Aufklärung des Betroffenen bei der Datenerhebung verpflichtet, noch immer nicht hinreichend bekannt ist und daß die Verwaltungen naheliegende organisatorische Maßnahmen, mit der die Beachtung der Vorschrift ohne nennenswerten Aufwand sichergestellt werden könnte (vgl. § 10 Abs. 1 BbgDSG), nicht treffen.

Grundsätzlich empfiehlt es sich durch Dienstanweisungen festzulegen, daß Vordrucke mittels deren beim Bürger personenbezogene Daten erhoben werden, nicht ohne eine vorherige Förmlichkeitsprüfung (z. B. durch einen behördlichen Datenschutzbeauftragten) verwendet werden dürfen. Dadurch ließe sich - zugleich kostensparend - ohne größeren Aufwand der Gefahr vorbeugen, daß nicht datenschutzgerecht gestaltete Formulare beschafft und verwendet werden.

- Aufbewahrungsfristen für gewerberechtliche Unterlagen

In der Fortführung der Diskussion zwischen dem MW und mir zu dieser Problematik[179], ergab sich als gemeinsamer Standpunkt, daß die Speicherung von rechtmäßig zu den Akten gelangten Zentralregisterauszügen in gewerberechtlichen Verfahren grundsätzlich auch über den Zeitpunkt ihrer Verwertbarkeit nach §§ 51, 52 Bundeszentralregistergesetz (BZRG)[180] hinaus für die Nachprüfbarkeit der auf ihrer Grundlage getroffenen Entscheidungen erforderlich ist. Soweit bei Auskünften aus dem Bundeszentralregister das Verwertungsverbot nach §§ 51, 52 BZRG greift, darf eine neue Entscheidung allerdings nicht mehr auf die dem Verwertungsverbot unterliegenden Angaben gestützt werden. Zentralregisterauskünfte, die nicht mehr verwertet werden dürfen, sind ebenso wie andere Unterlagen, die nur nach Maßgabe von § 47 Abs. 2 Satz 3 BbgPolG[181] nicht vernichtet werden, zu sperren und mit einem Sperrvermerk zu versehen (§ 23 Nr. 2 Buchst. f OBG[182] i. V. m. § 47 Abs. 2 Satz 4 BbgPolG).

Die generellen Aufbewahrungsfristen für gewerberechtliche Unterlagen hat das Ministerium für Stadtentwicklung, Wohnen und Verkehr in einem Rundschreiben an die Gewerbeämter[183] bestimmt.

12.4 Meldestellen

12.4.1 Prüfung von Meldeämtern

Im Berichtszeitraum haben meine Mitarbeiter je eine Meldebehörde in allen 14 Landkreisen (11 amtsangehörige und 3 amtsfreie Gemeinden) kontrolliert. Damit war das besondere Anliegen verbunden, vor Ort bei den Anwendern der

178 s. 4. Tätigkeitsbericht unter 2.3

179 s. 4. Tätigkeitsbericht unter 11.1

180 i. d. Fass. vom 21. September 1984, BGBl. I S. 1229, ber. 1985 I S. 195

181 vom 29. Februar 1996, GVBl. I S. 274

182 vom 13. Dezember 1991, GVBl. I S. 636, zul. geänd. d. Art. 2 d. Gesetz zur Neurordnung des Polizeirechts im Land Brandenburg vom 29. Februar 1996, GVBl. I S. 274

183 Nr. 24/1996 vom 22. Oktober 1996, Az.: 33/1-St/Br-(rs24-96)

melderechtlichen Vorschriften in Erfahrung zu bringen, ob und ggf. inwieweit

- es bereits jetzt aufgrund welcher evtl. Mängel Schwierigkeiten bei der praktischen Umsetzung der bestehenden melderechtlichen Regelungen gibt,

- die erforderlichen technisch-organisatorischen Maßnahmen ergriffen sind,

- die bisher gestellten Forderungen auch Gesichtspunkten der Praktikabilität entsprechen,

- aufgrund der Erfahrung im täglichen Umgang mit den Vorschriften oder aufgrund meiner Feststellungen weiterer Regelungsbedarf abgeleitet werden muß (vgl. hierzu auch unter 3.1.1).

Ganz allgemein war in den Meldestellen durchweg eine hohe Sensibilität für die datenschutzgerechte Behandlung der Meldedaten bei regelmäßig auch guten Kenntnissen über melderechtliche Bestimmungen feststellbar. Im Vorfeld zu den Besuchen hatte ich mir vom MI sämtliche Informationsschriften an die Landkreise und kreisfreien Städte zu speziellen Melderechtsfragen, die häufig zuvor auch mit mir abgestimmt waren, zukommen lassen.

Nur in zwei Fällen war an Hand der Sammlung festzustellen, daß diese Informationen nicht durchgängig an die Meldebehörden der Kommunen weitergereicht werden. Beide Gemeinden gehören Landkreisen an, in denen sich - dem Vernehmen nach - die Kreisverwaltung jeden unmittelbaren Kontakt mit dem MI vorbehält. Daraus ist zu schließen, daß zumindest in diesen Landkreisen datenschutzrechtlich wichtige Informationen zur korrekten Rechtsanwendung und ordnungsgemäßen organisatorischen Handhabung auch für weitere Kommunen verlorengehen. Ich würde es begrüßen, wenn auch hier eine bessere Durchgängigkeit der Informationen im Meldebereich erreicht würde. Dazu könnte auch die Annahme des besonders hervorzuhebenden Angebots der Mitarbeiter/-innen im zuständigen Referat des MI, Informationsveranstaltungen auch vor Ort durchzuführen, dienen. Die überwiegende Anzahl der besuchten Meldebehörden hat von diesem Angebot - oft mit koordinierender Unterstützung der jeweiligen Kreisverwaltung - bereits Gebrauch gemacht.

12.4.1.1 Technisch-organisatorische Mängel

Die Erfüllung der technisch-organisatorischen Maßnahmen zum Datenschutz hat sich - sofern kein grundsätzliches Problem vorliegt - erfahrungsgemäß insbesondere in Abhängigkeit von den sehr unterschiedlichen räumlichen Verhältnissen und von der jeweils eingesetzten Software gezeigt. Meine die jeweilige Situation berücksichtigenden Vorschläge zur Behebung diesbezüglicher Mängel haben die besuchten Gemeinden schriftlich erhalten. Besonders häufig mußte ich auf die Beseitigung diesbezüglicher Mängel in folgenden Punkten hinweisen:

- Vertraulichkeit des nichtöffentlich gesprochenen Wortes

Sofern die Meldebehörde über einen Besucherraum mit mehreren PC-Arbeitsplätzen verfügt, besteht die Gefahr, daß die Vertraulichkeit des Wortes und das Meldegeheimnis nicht hinreichend gewährleistet werden können. In diesen Fällen muß dem Benutzer ein deutlicher Hinweis darauf gegeben werden, daß er auch die Möglichkeit der Einzelabfertigung wählen kann. Hierzu geeignet ist ein entsprechendes Hinweisschild an der Eingangstür zum Abfertigungsraum oder an zentraler Stelle des Warteraums. In Großraumbüros müssen - ungeachtet der Wahl einer Einzelabfertigung - z. B. schallisolierende Wandteile zwischen den einzelnen Arbeitsplätzen eingebaut werden.

- Bildschirmsperre

Bei Mehrplatzarbeitsräumen, ansonsten bei von Besuchern einsehbaren PC-Einzelarbeitsplätzen, müssen Bildschirmschoner zur Bildschirmsperre eingesetzt werden, die erst wieder mittels Eingabe des Paßwortes deaktiviert werden können.

- Einsatz von Reinigungspersonal

Aus Sicherheitsgründen sollte der Einsatz von Reinigungspersonal nur während der Dienstzeit und unter Beobachtung der zuständigen Mitarbeiter in den Diensträumen der Meldestelle zugelassen werden.

- Verschlüsselungssoftware

Selbst wenn die äußeren Sicherheitsbedingungen (Haus- und Raumsicherung) mehr als ausreichend sind, sollte zur Sicherung der Daten so stark personenbezogener Programme wie im Meldebereich unbedingt Verschlüsselungssoftware eingesetzt werden. Durch eine solche, nach dem heutigen Stand der Technik erschwingliche Maßnahme könnten die Daten nicht nur vor - auch verwaltungsinternem - unbefugtem Zugriff geschützt werden. Hierdurch kann auch die Wartung der Rechenanlagen entproblematisiert werden, weil hiermit beauftragten Fremdfirmen die konkrete Einsicht in die Datenbestände verwehrt wird. Hierzu ist näher ausgeführt in meiner Broschüre "Technisch-organisatorische Aspekte des Datenschutzes"[184].

- Funktionstrennung

Begrüßenswert ist es, wenn Gemeindeverwaltungen einen behördlichen Datenschutzbeauftragten bestellen. Jedoch darf diese Funktion nicht dem EDV-Verantwortlichen bzw. Systemverwalter übertragen werden, weil durch die mangelnde Funktionstrennung praktisch eine unzulässige Interessenkollision wegen der damit zwangsläufig verbundenen Selbstkontrolle entsteht.

- Systemverwaltung

Regelmäßig haben die für die Systemverwaltung Verantwortlichen die Möglichkeit, in alle Dateien einsehen zu können, obwohl hierfür zumindest in dieser Funktion grundsätzlich keine Erforderlichkeit besteht. Unvermeidbar ist eine Kenntnisnahme von konkreten personenbezogenen Daten immer dann, wenn sie in dieser Funktion Arbeiten auf der Basis des Betriebssystems durchzuführen haben. Dies verleiht ihnen einerseits eine gewisse "Allmacht", andererseits können sie dadurch aber auch ständig latenten Verdächtigungen ausgesetzt sein. Weil das erste von vornherein, das zweite wegen der mangelnden Nachweismöglichkeit datenschutzrechtlich unzulässig ist, empfiehlt es sich, daß das Paßwort des Systemverwalters in zwei Teile aufgeteilt ist, von denen nur der erste Teil dem jeweiligen Funktionsträger selbst bekannt ist, für den zweiten Teil aber ein weiterer Bediensteter benötigt wird. Dieses sog. Vier-Augen-Prinzip bietet sich insbesondere dann an, wenn im Behördennetz noch keine Verschlüsselungssoftware als zusätzliche Sicherheitsmaßnahme eingesetzt ist.

- Dienstanweisung zum Datenschutz

---

184 s. unter S. 48 ff. sowie Anlagen 14 und 27 der 1. Aufl. Oktober 1996 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert"

Allein wegen der intensiven Verarbeitung personenbezogener Daten im Meldebereich sollten die Kommunen eine allgemeine Dienstanweisung zum Datenschutz für ihre automatisierte Datenverarbeitung entwickeln[185].

12.4.1.2 Regelungsdefizite

Von grundsätzlicherer Bedeutung sind allerdings die bei der Prüfung festgestellten Mängel, die auf Regelungsdefizite im Brandenburgischen Meldegesetz[186] selbst zurückzuführen sind. Aufgrund dieser Mängel kann und muß ich meinen bislang bereits vorgetragenen Katalog an Regelungs- bzw. Änderungsforderungen bzw. -vorschlägen (s. unter 3.1.1) näher präzisieren und noch um einige wesentliche Punkte erweitern:

- Protokollierung

Es fehlt die Verpflichtung, Arbeitsgänge, wie Datenübermittlungen oder die Erteilung von Auskünften, zu protokollieren. Da nicht einmal vorgeschrieben ist, ob und in welcher Weise Anfragen und die jeweiligen Aktivitäten der Meldebehörden zu dokumentieren sind, können häufig Nachweise über die Ordnungsgemäßheit des Verwaltungshandelns nicht erbracht werden. Insoweit ist auch eine Kontrollmöglichkeit nicht gegeben.

Solange (auch wegen der eingesetzten unterschiedlichen Software) eine automatisierte Protokollierung durchgängig nicht möglich ist, muß zumindest eine Verpflichtung bestehen, daß in allen Fällen von Auskunftserteilungen und Datenübermittlungen der diesbezügliche Schriftwechsel aufbewahrt wird, zumindest aber (auch bei einfachen Melderegisterauskünften) in fortlaufender Kladde ein formloses Protokoll geführt wird, wann an wen über wen welche Art von Auskunft erteilt wurde. Bei regelmäßigen Datenübermittlungen könnte eine Notiz über die Tatsache und den Weg der komplexen Übermittlung mit Datumsangabe ausreichen.

Ungeachtet des bisherigen Regelungsmangels habe ich diese Empfehlung an die Meldebehörden weitergegeben, nachdem das MI in einem Informationsschreiben[187] zumindest schon einmal darauf hingewiesen hatte, in welchen Fällen sich die Aufbewahrung schriftlicher Unterlagen zur Erfüllung der Nachweispflicht empfiehlt. Den befragten Mitarbeitern war klar, daß diese Maßnahmen auch ihrem eigenen Schutz vor möglichen ungerechtfertigten Verdächtigungen dienen.

- Aufbewahrungsfristen

Soweit schriftliche Dokumentationen, Übermittlungskontrollnachweise, Ausdrucke zu Speichereingaben, Auskunftsnotizen u. ä. vorlagen, bestanden Unsicherheiten, wielange die nach mehreren Jahren sehr umfangreich gewordenen Sammlungen aufzubewahren seien. Tatsächlich muß der Gesetzgeber hier eine eindeutige Entscheidung treffen, welche Aufbewahrungsfristen er als ausreichend ansieht. Nach meinem Dafürhalten könnte mit einer Frist von 2 Jahren seit jeweiligem Ereignis dem Schutzbedürfnis derjenigen ausreichend Rechnung getragen sein, über die eine Melderegisterauskunft eingeholt wurde.

---

185 s. vorherige Fußnote

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

187 vom 5. März 1993, Az.: I.4/lie

- Kreismeldekarteien

Offensichtlich werden hier und da Kreismeldekarteien und parallele Altdatensammlungen (Nebenkarteien, Haus-/Straßenkarteien) in den Meldebehörden nicht nur aufbewahrt, sondern zugänglich gehalten und zu Zwecken der Meldebehörde genutzt.

Aufgrund der Tatsache, daß die Frist im Brandenburgischen Meldegesetz zur Löschung dieser Datenbestände seit dem 31.12.1993 abgelaufen ist, hatte ich in Ergänzung zu meinen Ausführungen im 3. Tätigkeitsbericht[188] bei Anfragen bislang darauf hingewiesen, daß diese Datenbestände in Erwartung einer gesetzlichen Neuregelung zumindest als gesperrt zu behandeln sind. Das bedeutet, daß Karteikarten bzw. Informationen hieraus lediglich noch den Betroffenen selbst zur Verfügung gestellt werden dürfen, sie ansonsten ohne Zustimmung der Betroffenen aufgrund des mangelnden rechtlichen Rahmens und aufgrund der Befürchtung, daß im Einzelfall völlig unzulässige melderechtsfremde Angaben (z. B. Hinweise auf "Republikflucht", PKZ) vorhanden sind, letztlich nur zur Behebung einer bestehenden Beweisnot herangezogen werden dürfen.

Eine weitere Verlängerung dieser "Übergangslösung" kann aber nun nicht mehr länger hingenommen werden. Eine datenschutzgerechte Weiternutzung müßte zum frühestmöglichen Zeitpunkt im Brandenburgischen Meldegesetz geregelt werden. Für diesen Fall müßte im Gesetz normenklar definiert werden, für welche Zwecke die Nutzung der Daten - entgegen meinen Zweifeln - weiterhin erforderlich ist.

- Auskunftssperren

Wird eine Auskunft über eine Person beantragt, für die eine Auskunftssperre im Melderegister eingetragen ist, muß die Meldebehörde grundsätzlich die Auskunft verweigern, wenn dem Betroffenen oder einer anderen Person hieraus eine Gefahr z. B. für Leben, Gesundheit, persönliche Freiheit erwachsen kann. Entsprechende Sperren werden häufig insbesondere von Frauen beantragt, nachdem sie sich von ihrem bisherigen Partner wegen dessen ständiger Bedrohungen getrennt haben und an einen anderen Ort gezogen sind.

Diese Schutzvorschrift wird durch das Gesetz selbst unterlaufen und dadurch ad absurdum geführt, daß der suchende Partner auf Anfrage im vermuteten Zuzugsgebiet die Auskunft erhält: "Auskunft muß gem. § 32 Abs. 6 BbgMeldeG verweigert werden" oder "Es ist eine Auskunftssperre nach § 32 Abs 6 BbgMeldeG eingetragen". Damit wird dem Auskunftsersuchenden klar, daß die Gesuchte zumindest im Bereich der betreffenden Meldebehörde ihre Wohnung hat, so daß er - insbesondere in kleineren Gemeinden - gute Chancen hat, durch Nachbarschaftsbefragungen alsbald den konkreten Aufenthalt seiner bisherigen Partnerin zu erfahren.

Mitarbeiter von Meldestellen haben mir bestätigt, daß sie bei entsprechenden Auskunfts-verweigerungen "kein gutes Gefühl haben". Als sinnvolle Lösung kommt für mich nur in Betracht, daß gesetzlich vorgeschrieben die Auskunft gegeben wird: "... ist im Zuständigkeitsbereich nicht gemeldet". Diese "gesetzlich sanktionierte Lüge" halte ich aus dem besonderen Schutzbedürfnis Betroffener heraus für gerechtfertigt, zumal dem Sperreintrag ein Verfahren vorangeht, in dem recht eingehend geprüft werden muß, ob hierfür die vom Gesetz vorgeschriebenen Gefährdungsmerkmale vorliegen.

Bei den allerdings auch in diesen Fällen möglichen (konkreten) Auskünften an Behörden muß der mit der Auskunft

188 s. unter 3.2.1.2

verbundene Hinweis auf den Sperreintrag noch einmal mit dem ausdrücklichen Zusatz versehen werden, daß die Auskunft ausschließlich dem dortigen Verwendungszweck zu dienen hat und nicht weiter übermittelt werden darf.

Im übrigen muß in § 32 Abs. 6 BbgMeldeG zukünftig zweifelsfrei formuliert sein, daß die Abwägung der Interessen des Antragstellers auf Auskunftserteilung gegen die Interessen des Betroffenen an einer Auskunftsverweigerung nicht auch bei Auskunftsersuchen in den zuletzt behandelten Fällen vorzunehmen ist, hier vielmehr stets von der Wirksamkeit der Sperre mit den o. g. Konsequenzen ausgegangen werden muß.

- Umsetzung des Transsexuellengesetzes

Um den besonderen schutzwürdigen Belangen einer weiteren Personengruppe im Rahmen ihrer Persönlichkeitsrechte hinreichend gerecht zu werden, muß unbedingt auch eine den §§ 5 Abs. 1 und 10 Abs. 2 Transsexuellengesetz[189] entsprechende Auskunftssperre für die Fälle vorgesehen werden, in denen die dort genannten Voraussetzungen vorliegen.

- Art der Sperrung

In mehreren Fällen mußte ich feststellen, daß dem Bearbeiter bei Aufrufen eines Datensatzes zwar der Hinweis auf die Tatsache einer vorhandenen Auskunftssperre gegeben wird, nicht jedoch auch darauf, um welche Art der Sperre es sich handelt. In diesen Fällen war es aufgrund des eingesetzten Software-Programms nicht möglich, die weiteren Unterscheidungsmerkmale automatisiert zu erfassen, so daß zur näheren Unterscheidung auf parallel geführte Aktenvorgänge zurückgegriffen werden muß. Dies kann so nicht hingenommen werden.

Wenn Datenverarbeitung in automatisierter Form vorgenommen wird, muß sichergestellt sein, daß die verarbeiteten Daten dem absolut authentischen Stand entsprechen und insoweit aus sich heraus verständlich sind, ohne einer zusätzlichen anderweitigen Interpretation zu bedürfen. Daß diese Erforderlichkeit im Brandenburgischen Meldegesetz selbst festgeschrieben werden muß, läßt sich beispielhaft allein aus den Gefahren für Betroffene ableiten, wenn z. B. im Falle eines persönlich vorgetragenen Auskunftsersuchens zunächst eine auffällige Recherche - mit allen Rückschlußmöglichkeiten für den Auskunftsersuchenden - durchgeführt werden muß, bei der sich erst am Ende herausstellt, daß eine besonders behutsam zu behandelnde Sperre aufgrund einer Gefahr für Leib, Leben und Gesundheit des Meldepflichtigen (s. oben unter Auskunftssperren) vorliegt.

- Unvollständige Angaben

Einige Meldebehörden, in deren Zuständigkeitsbereich sich Asylbewerberheime befinden, beklagten, daß sie bei der Bearbeitung melderechtlicher Vorgänge durch die praktischen Gegebenheiten ständig gezwungen seien, gegen Bestimmungen des geltenden Melderechts zu verstoßen, wollten sie nicht gänzlich auf die Erfüllung ihrer Aufgaben bezüglich der Personen, die der dortigen Unterkunft zugewiesen sind, verzichten. In solchen Fällen werden Zuzugsmeldungen häufig durch die Ausländerbehörde oder die Heimleitung in Listenform vorgenommen, ohne daß eine Identifizierung durch persönliche Vorstellung der Meldepflichtigen möglich wäre. Dabei erhalten die Meldebehörden oft unvollständige Angaben oder - wie sich mitunter erst später herausstellt - auch Angaben zu Namen, Geburtsorten usw. in falscher Schreibweise, so daß bei evtl. Anfragen kaum gesicherte Auskünfte gegeben werden können. Im übrigen müssen

[189] Gesetz über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen (Transsexuellengesetz - TSG) vom 10. September 1980, BGBl. I S. 1654

die Meldebehörden wohl regelmäßig davon ausgehen, daß zu den Asylbewerbern auch keine ordnungsgemäßen Abmeldungen erfolgen, häufig auch keine Anmeldung an evtl. anderem Wohnort erfolgt. Zusammenfassend ist festzustellen, daß die betroffenen Meldebehörden nicht einmal ihre originäre Aufgabe, "die in ihrem Zuständigkeitsbereich wohnhaften Personen zu registrieren, um deren Identität und Wohnungen feststellen und nachweisen zu können", erfüllen können. Ähnliche Probleme treten dem Vernehmen nach auch bei Heimen zur Betreuung Drogenabhängiger auf.

Um den Meldebehörden eine dem gesetzlichen Auftrag entsprechende und insoweit ordnungsgemäße Aufgabenerfüllung zu ermöglichen, muß der Gesetzgeber - wollte er keine besonderen Melderegelungen schaffen - im Gesetz selbst festschreiben, daß die Meldebehörden in vergleichbaren Sonderfällen mit nicht gesicherten spekulativen Daten operieren dürfen.

- Datenverarbeitung im Auftrag

Ein besonderes Problem stellt auch im Meldebereich die Datenverarbeitung im Auftrag dar. Bei einigen (im östlichen Landesteil gelegenen) Meldebehörden konnte ich feststellen, daß sie nach wie vor einen Teil ihrer Aufgaben, nämlich die regelmäßigen Datenübermittlungen, einer privaten Firma, die offenbar einem weltweiten Unternehmen angehört, übertragen haben und dieser hierfür regelmäßig im Datenträgeraustausch den aktuellen Datenbestand übermittelt. Nach § 35 Abs. 1 Satz 2 BbgMeldeG ist aber eine Datenverarbeitung im Auftrag bei nicht-öffentlichen Stellen nur zulässig, wenn der öffentlichen Hand die Mehrheit der Anteile gehört bzw. der Stimmen zusteht. Zwar hatten die betreffenden Meldebehörden nach meinen Feststellungen ursprünglich ihre Vereinbarungen mit einer kommunalen (also öffentlich-rechtlichen) Datenzentrale getroffen, jedoch ist diese unterdessen in eine private Rechtsform übergegangen, ohne daß die o. g. Voraussetzungen zutreffen. Insoweit handeln die beteiligten Meldebehörden nach geltender Rechtslage rechtswidrig.

Möglicherweise wird es sich aus wirtschaftspolitischen und aufgrund der faktischen Gegebenheit auch aus ökonomischen Gründen nicht vertreten lassen, daß an der bestehenden Rechtslage und deren praktischer Umsetzung festgehalten wird. Dies wäre insoweit hinnehmbar, als auch private Firmen gem. § 11 BbgDSG hinreichend zu datenschutzgerechter Handhabung zu verpflichten sind und sich der Kontrolle des Landesbeauftragten für den Datenschutz zu unterwerfen haben.
Da bei konzentrierter Datenverarbeitung im Auftrag - unabhängig davon, ob diese durch private oder öffentliche Stellen ausgeübt wird - immer die Gefahr der unerlaubten Zusammenführung von Datenbeständen besteht, scheint es mir entscheidender zu sein, daß der Gesetzgeber im Meldegesetz ungeachtet der Rechtsform des Auftragnehmers festschreibt, daß die jeweiligen Datenbestände der Meldebehörden untereinander abgeschottet bleiben, nicht zusammengeführt und Informationsaustausche unter den Meldebehörden nur durch diese selbst vorgenommen werden dürfen. Darüber hinaus muß - ungeachtet o. g. Schwierigkeiten - spezialgesetzlich verankert werden, daß sich private Auftragnehmer der Kontrollbefugnis meiner Behörde unterwerfen. Die zuletzt genannte Forderung müßte auch erhoben werden, wenn Behörden oder sonstige öffentlich-rechtliche Stellen außerhalb meines Zuständigkeitsbereichs - wie ich dies ebenfalls feststellen konnte - beauftragt werden. Da solche Stellen aber durch landesgesetzliche Zuständigkeitsregelungen Brandenburgs nicht gebunden werden können, muß ich jede diesbezügliche Form der auftragsweisen Datenverarbeitung im Meldebereich ablehnen, weil wegen der hier sehr intensiven Verarbeitung elementarer personenbezogener Daten aus dem Kommunalbereich Brandenburgs eine (nur) mittelbare Kontrollmöglichkeit durch zuständige andere Datenschutzbeauftragte nicht hingenommen werden kann. Dies ist mit dem Schutzbedürfnis Betroffener einschließlich ihres erwarteten Vertrauensschutzes nicht vereinbar.

Zudem sind gerade bei Übermittlungen über die Landesgrenzen hinaus besondere Gefahren hinsichtlich der Datensicherung zu befürchten. Aber selbst bei auftragsweiser Datenverarbeitung innerhalb Brandenburgs sollte jede Form der Meldedatenübermittlung - ob online oder im Datenträgeraustausch - wegen der hier besonders intensiven Häufung personenbezogener Daten nur in Verschlüsselung[190] zulässig sein (s. auch oben unter Verschlüsselungssoftware und auch unter 3.1.1).

Wegen der besonderen Sensitivität der im Meldebereich verarbeiteten personenbezogenen Daten sollte vor einer Neuregelung eingehend geprüft werden, ob nicht das Landesamt für Datenverarbeitung und Statistik (LDS) in seiner Funktion als Landesrechenzentrum in solchen Fällen diese speziellen Aufgaben der Meldebehörden in auftragsweiser Datenverarbeitung übernehmen sollte, weil dort die technisch-organisatorischen und rechtlichen Voraussetzungen sowohl für den Datenschutz und die Datensicherheit als auch für meine Kontrollmöglichkeiten in besonderem Maße gegeben sind. Ich würde es daher begrüßen, wenn eine dementsprechende Regelung zustande käme.

12.4.1.3 Organisationsmängel

Über die rechtlichen Defizite hinaus haben sich noch weitere allgemeine Probleme herausgestellt, die auf Umsetzungsfehler oder auf verwaltungstechnische und -organisatorische Regelungsdefizite zurückzuführen sind:

- öffentlich einsehbare Wählerverzeichnisse

190 s. 4. Tätigkeitsbericht unter 3.1.1

Wiederholt mußte ich darauf hinweisen, daß gem. § 17 Abs. 3 BbgLWahlG[191] in die öffenlich ausliegenden Wählerverzeichnisse nicht auch die personenbezogenen Daten derjenigen Wahlberechtigten, für die eine generelle Auskunftssperre im Melderegister eingetragen ist, erscheinen dürfen, weil damit die im Brandenburgischen Meldegesetz selbst eingeräumte Maßnahme zum situationsbedingt besonderen Persönlichkeitsschutz Betroffener unterlaufen wird (s. oben). Dies gilt selbstverständlich nicht für jene Wählerlisten, die lediglich dem Wahlvorstand für dessen Aufgabenerfüllung am Wahltag zur Verfügung stehen. Sofern auf Anfrage Auskünfte zur Wahlberechtigung einer bestimmten anderen Person unmittelbar aus dem Meldedatensatz am PC heraus gegeben werden, muß verfahrensmäßig sichergestellt werden, daß dem anfragenden Dritten im Falle einer solchen Auskunftssperre keine Rückschlußmöglichkeiten gegeben sind.

- Eintrag "Ohne festen Wohnsitz" im Personalausweis

Personen, die keinen festen Wohnsitz haben, erhalten auf ihrem Personalausweis einen Aufkleber mit dem Eintrag "Ohne festen Wohnsitz". Diese Formulierung ist durch das Brandenburgische Personalausweisgesetz (BbgPAuswG)[192] nicht gedeckt. Soweit Meldedaten vorhanden sind, ist bei der Ausstellung eines Personalausweises ausschließlich auf dortige, nach melderechtlichen Bestimmungen zulässige, nämlich konkrete, Angaben zur Anschrift zurückzugreifen. Diesem Erfordernis entspricht der besagte Eintrag nicht. Im übrigen ist die Aussage äußerst spekulativ und bereits dann falsch, wenn der Betroffene - zwar ordnungswidrig, so doch aber - lediglich seinen Meldepflichten nicht nachgekommen ist. Vor diesem Hintergrund stellt der Eintrag in jedem Fall eine besondere Verletzung der Persönlichkeitsrechte Betroffener wegen der damit verbundenen gesellschaftlichen Herabwürdigung dar. Eine Formulierung unter Wohnanschrift "Nicht bekannt" würde die stigmatisierende Außenwirkung zumindest mindern, aber auf jeden Fall dem tatsächlichen Sachstand entsprechen. Daß eine solche Forderung nicht überzogen sein kann, wird bereits dadurch deutlich, als selbst eine unzutreffende Angabe über die gegenwärtige Anschrift gem. § 5 Abs. 2 Nr. 3 BbgPAuswG die Gültigkeit des Personalausweises nicht beeinträchtigt. Insoweit ist sogar zu bezweifeln, ob ggf. überhaupt ein Eintrag zur Wohnanschrift erforderlich ist, wenn den Schilderungen entsprechend Umstände vorliegen.

- Postlauf

In einigen Ämtern verlangen die Amtsdirektoren, daß ihnen im internen Postlauf mit anderer Behördenpost auch der gesamte Schriftwechsel des Meldeamts zugeleitet wird. Dies ist mit dem in § 14 Abs. 5 BbgDSG verankerten Prinzip der informationellen Gewaltenteilung in der Kommunalverwaltung nicht vereinbar. Grundsätzlich gilt, daß Post, die erkennbar an eine bestimmte Stelle gerichtet ist, diese auch ungeöffnet zu erreichen hat, weil nur im Rahmen dortiger gesetzlicher Aufgabenerfüllung die Kenntnisnahme von hierzu verarbeiteten bzw. zu verarbeitenden personenbezogenen Daten erforderlich ist. Das gleiche gilt für die Ausgangspost. Dabei steht es dem Behördenleiter frei, z. B. zu organisatorischen oder personellen Dispositionen den Postein- und -ausgang in ungeöffneter Form zu beobachten. Nur, wenn die absendende oder empfangende Stelle nicht eindeutig erkennbar ist, sowie bei konkretem Verdacht unsachgemäßer Bearbeitung und/oder begründeten Anhaltspunkten für dienst- oder arbeitsrechtliche Verstöße (z. B. gegen das Datengeheimnis) kann sich der Leiter der Kommunalbehörde im Einzelfall oder für einen vorübergehenden Zeitraum auch aus dem Meldebereich (aber nur) im Rahmen der Erforderlichkeit Postein- und -ausgänge vorlegen lassen.

- Standards an Sicherheitsvorkehrungen

---

191 vom 2. März 1994, GVBl. I S. 38, geänd. d. Art. 2 d. SWG vom 7. Juli 1994, GVBl. I S. 294

192 Personalausweisgesetz für das Land Brandenburg vom 7. April 1994, GVBl. I S. 100

Wiederholt war im Berichtszeitraum bei mehreren brandenburgischen Meldebehörden eingebrochen worden. Dabei war das Interesse der Einbrecher - nach Auffassung der Verantwortlichen - insbesondere darauf ausgerichtet, in den Besitz von Ausweis- und Paßvordrucken sowie Dienstsiegeln zu gelangen. Immerhin ist daraus zu ersehen, daß Meldebehörden bereits aus diesen Gründen von besonderem Interesse sein können und daher die Standards an Sicherheitsvorkehrungen besonders hoch angesetzt werden müssen.

In einigen Meldeämtern fand ich bestätigt, daß wichtige Dokumente wie ausgefertigte Personalausweise und Dienstsiegel sowie datenschutzrechtlich sehr sensible melderechtliche Vorgänge wie Anträge auf Auskunftssperren, Adoptionsmitteilungen, als gesperrt geltende Karteikarten der ehemaligen Kreismeldekartei (s. oben) u. ä. nur unzureichend gesichert aufbewahrt werden. Dies mußte ich wegen des hohen Schutzbedürfnisses der genannten Daten bzw. -sammlungen auch dann bemängeln, wenn ansonsten die Gebäude- und Raumsicherung ausreichend waren. In diesen Fällen habe ich dringend empfohlen, spezielle Sicherungsschränke mit einem hohen Widerstandswert anzuschaffen, bei mangelnder Raumsicherung auch darüber hinaus die Kombination mit Bewegungsmeldern, die möglichst bei einer Polizeidienststelle aufgeschaltet oder zumindest mit einem Tonmelder gekoppelt sind, herzustellen (s. unter 12.4.2.2).

12.4.2 Besondere Probleme

12.4.2.1 Veröffentlichungen von Alters- und Ehejubiläen in Amts- und Gemeindeblättern

Meldebehörden dürfen gem. § 33 Abs. 2 BbgMeldeG auf Anfrage Auskünfte über Alters- oder Ehejubiläen erteilen, sofern kein Widerspruch Betroffener gegen eine Auskunftserteilung in solchen Fällen vorliegt. Darüber, daß dieses Recht nicht auch die Berechtigung für den Anfragenden einschließt, die erhaltenen Informationen in Zeitungen, Amts- oder Gemeindeblättern, Rundfunksendern oder durch öffentlichen Aushang bekanntzugeben, weil mangels Rechtsgrundlage gem. § 4 Abs. 1 Buchst. b BbgDSG hierfür zusätzlich die Einwilligung Betroffener eingeholt werden müßte, hatte ich in meinem 4. Tätigkeitsbericht[193] näher ausgeführt. Der Oberbürgermeister der Landeshauptstadt wählt jetzt ein Verfahren, das datenschutzrechtlich vertretbar ist und in Vergleichsfällen auch andernorts zur Anwendung kommen könnte:

Nach § 4 Abs. 2 BbgDSG bedarf die Einwilligung Betroffener grundsätzlich der Schriftform, "soweit nicht wegen besonderer Umstände eine andere Form angemessen ist". Insbesondere unter dem Aspekt, daß erfahrungsgemäß Altersjubilare bis auf wenige Ausnahmen eine Gratulation im Amtsblatt o. ä. erwarten, teile ich die dortige Ansicht, daß es hochbetagten Jubilaren kaum zugemutet werden kann, jedesmal ausdrücklich die Einwilligung schriftlich zu erklären und für die tatsächliche Versendung ihrer Erklärung zu sorgen mit der Gefahr, bei entsprechendem Versäumnis bei der nächsten Veröffentlichung nicht erwähnt zu werden.

Daher halte ich die sog. Widerspruchslösung im Interesse der Betroffenen für vertretbar. Das bedeutet, daß alle Jubilare rechtzeitig angeschrieben und in geeigneter Form auf die beabsichtigte Veröffentlichung ihrer Daten sowie darauf hingewiesen werden, daß sie ihre Einwilligung auch verweigern können. Dem Interesse Betroffener wäre in konsequenter Beachtung ihrer altersbedingten Situation aber erst dann hinreichend Rechnung getragen, wenn ihnen zusätzlich eingeräumt würde, ihren Widerspruch auch für die Zukunft erklären zu können. Verwaltungsintern würde dann sichergestellt werden, daß Alters- und Ehejubilare in diesen - vermutlich wenigen - Fällen nicht mehr angeschrieben werden.

---

193 s. unter 12.2.1

12.4.2.2 Sicherheit der Panzerschränke

Unabhängig von den unter 12.4.1 behandelten Kontrollen habe ich bei zusätzlichen Besuchen in kommunalen Behörden geprüft, inwieweit wichtige und sensible Unterlagen sicher verwahrt werden. Im Berichtszeitraum erhielt dieses Problem eine besondere Brisanz dadurch, daß Einbrüche in Einwohnermeldeämter Gegenstand von parlamentarischen Erörterungen waren[194].

Es zeigte sich, daß die Anforderungen an eine sichere Verwahrung sensibler Unterlagen unterschiedlich erfüllt waren. In einer Reihe von Fällen habe ich Empfehlungen zur Anschaffung von modernen Sicherungsschränken gegeben. Problematisch ist dabei, daß es - anders als in einigen anderen Bundesländern[195] - im Land Brandenburg bisher keine Richtlinie o. ä. über technische Standards von Sicherungsschränken (Wertschutzschränke) gibt. Dies halte ich aber für dringend geboten. Wenigstens sollten fallbezogene Empfehlungen zu technischen Standards (Feuerresistenz, Schlösserkombinationen, Wandstärken u. ä.) gegeben werden, um den kommunalen Behörden Kenntnisse zu vermitteln, die eine angemessene und sinnvolle Anschaffung von Sicherungsschränken ermöglichen.

12.5 Sonstige Stellen

12.5.1 Benennung des Inhabers eines Wohnberechtigungsscheins

194 LT-Drs. 2/2868 und 2/3079 "Sicherheit der Panzerschränke der Einwohnermeldeämter vor unbefugten Zugriffen Dritter?"

195 z. B. Schleswig-Holstein und Sachsen-Anhalt

Bei der Zuweisung kommunalen Wohnraums an Inhaber eines Wohnberechtigungsscheines (WBS) lassen die Kommunalverwaltungen sog. "Sozialausschüsse" der Gemeindevertretungen darüber entscheiden, ob und ggf. welche Wohnungen den WBS-Inhabern jeweils zugewiesen werden. Dazu müssen den "Sozialausschüssen", denen neben Mitgliedern der Gemeindevertretung gem. § 50 Abs. 7 Gemeindeordnung (GO)[196] beratend auch sachkundige Einwohner der Gemeinde angehören können, die nicht Bedienstete der Gemeinde oder des Amtes sind, die für die Entscheidung maßgeblichen Antragsakten mit zahlreichen z. T. sehr sensiblen Angaben zu den Antragstellern vorgelegt werden. Durch die mit einer Beteiligung der "Sozialausschüsse" verbundene Ausweitung des Kreises der Entscheidungsträger führt das Verfahren zu sehr viel stärkeren Eingriffen in das Recht auf informationelle Selbstbestimmung, als dies bei einer durchaus ebenso gut möglichen Entscheidung durch die Verwaltung der Fall wäre. Auch deshalb halte ich das durch die derzeitige Verfahrensweise bedingte Mehr an Datenverarbeitung zur Erfüllung der gesetzlichen Aufgaben der Kommunen bei der Wohnraumverwaltung nicht für erforderlich.

Als ich im Berichtszeitraum von einer Gemeinde auf die Problematik angesprochen wurde und daraufhin die Rechtslage überprüfte, mußte ich im übrigen feststellen, daß das Verfahren bislang einer ausdrücklichen gesetzlichen Grundlage entbehrt. Insoweit hat mir das Ministerium des Innern bestätigt, daß eine Beteiligung der "Sozialausschüsse" in jedem Fall voraussetze, daß sich die Gemeindevertretung amtsfreier Gemeinden dies entweder nur für den konkreten Einzelfall (§ 35 Abs. 3 Satz 1 GO) oder generell in der Hauptsatzung (§ 35 Abs. 3 Satz 2 GO) ausdrücklich vorbehalten hat, und daß dies bei amtsangehörigen Gemeinden nicht möglich sei. Auch aus Sicht der obersten Kommunalaufsichtsbehörde besteht also keine Rechtsgrundlage, aufgrund derer den sog. "Sozialausschüssen" amtsangehöriger Gemeinden personenbezogene Daten von Wohnungssuchenden übermittelt werden dürften.

Das MSWV hat hierauf inzwischen als zuständige oberste Sonderaufsichtsbehörde in einem Rundschreiben vom 16.11.1996 an die Landkreise darum gebeten, die Ämter und Gemeinden anzuweisen, daß die Weitergabe personenbezogener Daten an die Gemeindevertretungen und deren sog. "Sozialausschüsse" in Verfahren der Nennung von WBS-Inhabern für kommunalen Wohnraum künftig unterbleibt, es sei denn, daß sich die Gemeindevertretungen amtsfreier Gemeinden die Beschlußfassung nach Maßgabe von § 35 Abs. 3 Satz 1 oder Satz 2 GO vorbehalten haben. Auch mit Rücksicht auf das in Rede stehende datenschutzrechtliche Interesse, etwaige Satzungsänderungen der amtsfreien Gemeinden, durch die die Beschlußfassung über die Nennung von WBS-Inhabern für kommunalen Wohnraum der Gemeindevertretung vorbehalten werden sollen, von der Kommunalaufsicht nicht genehmigt werden sollten.

12.5.2 Anpassung an das neue Straßenverkehrsgesetz

Mit den Änderungen des Straßenverkehrsgesetzes[197], die zum 1. Januar 1998 in Kraft treten sollen, werden auch die für die Tätigkeit der Führerscheinstellen wesentlichen Rechtsgrundlagen der Straßenverkehrszulassungsordnung in einer Fahrerlaubnisverordnung neu geregelt werden. Diese befand sich bei Redaktionschluß noch in einem mir unbekannten Entwurfsstadium. Zwischen dem MSWV und mir besteht Übereinstimmung, daß das neue Recht insbesondere bedingt durch die Einführung eines Zentralen Fahrerlaubnisregisters beim Kraftfahrt-Bundesamt[198] eine bundeseinheitliche Formulargestaltung erforderlich machen wird, zu der das MSWV in Abstimmung mit mir bereits einen ersten Entwurf zur Diskussion gestellt hat. Im übrigen ist das MSWV meiner Empfehlung gefolgt und hat nach eingehender Erörterung mit den

---

196 vom 15. Oktober 1993, GVBl. I. S. 398; geänd. d. Art. 3 d. 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

197 s. 4. Tätigkeitsbericht unter 10.1

198 s. 4. Tätigkeitsbericht unter 10.1.2

Leitern der Führerscheinstellen und meiner Dienststelle, vorläufige Regelungen zum Datenschutz bei den Führerscheinstellen getroffen, die zum Inkrafttreten der gesetzlichen Neuregelungen in eine Verwaltungsvorschrift umgesetzt werden sollen. Die Regelungen beziehen sich insbesondere auf die Dokumentation von Zentralregisterauszügen, Strafurteilen, fachärztlichen Gutachten und medizinisch-psychologischen Untersuchungsberichten in den Akten der Führerscheinstelle und legen für diese und andere Unterlagen Aufbewahrungsfristen fest. Vor allem diese Fristen werden nach Maßgabe des neuen Rechts noch einmal zu überprüfen sein.

12.5.3 Absenderstempel: Verkehrsordnungswidrigkeiten

Ein Bürger fühlte sich in seinen Persönlichkeitsrechten dadurch beeinträchtigt, daß er einen Brief erhalten hatte, aus dessen Absenderstempelung "Verkehrsordnungswidrigkeiten" als Absender die Bußgeldstelle zu erkennen war. Die öffentliche Stelle, in diesem Fall das Landratsamt, entschied auf die Eingabe des Bürgers hin, daß das Wort "Verkehrsordnungswidrigkeiten" aus dem Stempelausdruck herausgenommen wird. Auch wenn von der absendenden Stelle nicht nur Verkehrssünder angeschrieben werden, so kann doch gemutmaßt werden, daß diejenigen, die den Absenderstempel lesen, häufig davon ausgehen werden, daß der Adressat eine Verkehrsordnungswidrigkeit begangen habe.

Ich habe das Landratsamt darauf hingewiesen, daß es verpflichtet ist, dazu beizutragen, Mißverständnisse solcher Art gar nicht erst aufkommen zu lassen. Aus dem Stempelausdruck kann sich eine Diskriminierung ergeben, auch wenn dies überhaupt nicht beabsichtigt gewesen sein sollte, weil lediglich eine korrekte und vollständige Absenderangabe beabsichtigt war. Die korrekte Absenderangabe kann auch durch eine neutrale Benennung erreicht werden, im Zweifel würde eine Durchnumerierung der Absenderstellen der Gemeinden oder des Landratsamtes und demzufolge eine bestimmte Referatsnummer den Ansprüchen genügen, die die absendende Stelle und auch die Post an die Eindeutigkeit der Zuordnung zu stellen haben.

12.5.4 Befugnisse des Rechnungsprüfungsamtes

Das Personalamt einer kreisfreien Stadt hatte Zweifel, ob das Rechnungsprüfungsamt der Stadtverwaltung berechtigt sei, in das zur Lohn- und Gehaltsabrechnung genutzte Datenverarbeitungsprogramm Einsicht zu nehmen.

Aus den gesetzlichen Grundlagen für die Tätigkeit des Rechnungsprüfungsamtes (§§ 112 ff. GO)[199] läßt sich ableiten, daß das Hauptaufgabenfeld für das Rechnungsprüfungsamt die Prüfung der Jahresrechnung sein soll (§ 114 i. V. m. § 113 Abs. 1 GO), ergänzt und ergänzbar durch weitere Prüfungsaufgaben, die wie die Jahresrechnung und der Haushaltsplan in ihrer Zielrichtung keinen Bezug zu personenbezogenen Daten haben. Allerdings sind in der Regel auch die jeweils zugehörigen Belege zu prüfen, und so können in einem gewissen Umfang auch Daten mit Personenbezug mit zum Prüfungsprogramm gehören. Weder im Haushaltsplan noch in der Jahresrechnung werden die einzelnen Vorgänge der Lohn- und Gehaltsabrechnung zu finden sein. Selbst die laufende Prüfung der Kassenvorgänge (§ 113 Abs. 1 Ziff. 3 GO) führt nicht zu der Überprüfung des einzelnen Vergütungsfalles, da die Vergütung für jeden Mitarbeiter durch Tarifvertrag bzw. Stellenplan im voraus festgelegt und daraufhin errechnet ist. Zur Kontrolle genügt die Prüfung der Auszahlung der jeweiligen Bruttobeträge.

Auch die Prüfung der Wirtschaftsführung (§ 113 Abs. 2 Ziff. 4 GO) führt nicht dazu, die einzelnen Vergütungszahlungen zu

[199] vom 15. Oktober 1993, GVBl. I S. 398; geänd. d. Art. 3 d. 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

überprüfen. Ich habe allerdings darauf hingewiesen, daß sich die Prüfung der Wirtschaftsführung sinnvollerweise auf das Verfahren bei der Auszahlung der Vergütung beziehen könnte, das Verfahren betrifft nämlich die Zweckmäßigkeit oder die Ordnungsmäßigkeit. Umständliche und veraltete Verfahrensweisen können bei sehr vielen Vorgängen zu Unwirtschaftlichkeit führen.
Vereinfacht läßt sich das Ergebnis meiner Überlegungen so formulieren: Die Prüfung durch das Rechnungsprüfungsamt soll sich erstens auf die Planung für die Jahresausgaben (Haushaltsplan) und zweitens auf das Ergebnis des Wirtschaftens (Jahresrechnung) beziehen, soweit es um Zahlen und Belege geht; sie soll sich drittens auf Verfahren bezüglich der dem Rechnungsprüfungsamt übertragenen weiteren Aufgaben beziehen.

Die Unabhängigkeit und Weisungsfreiheit, die dem Rechnungsprüfungsamt gesetzlich garantiert ist, wird dadurch nicht geschmälert. Unabhängigkeit und Weisungsfreiheit sind zwar für die wirkungsvolle und sinnvolle Tätigkeit des Rechnungsprüfungsamtes erforderlich, erstrecken sich jedoch nur auf die "sachliche Beurteilung der Prüfungsvorgänge". Darin, um welche Prüfungsvorgänge es sich handelt, ist das Rechnungsprüfungsamt dem Wortlaut des Gesetzes zufolge nicht unabhängig und weisungsfrei, denn es gibt gesetzlich festgelegte Prüfungsgegenstände und außerdem Prüfungsgegenstände, die u. a. die Gemeindevertretung dem Rechnungsprüfungsamt vorgibt.

Selbst wenn unterstellt würde, dem Rechnungsprüfungsamt würden durch die Gemeindevertretung Prüfungsaufgaben übertragen, die die Einsicht in die Lohn- und Gehaltsunterlagen beträfen, so wäre das nicht zu rechtfertigen, da nicht erkennbar wäre, weshalb die Einsichtnahme oder die Offenlegung dieser Unterlagen erforderlich ist, da durch die Einsichtnahme in das zur Lohn- und Gehaltsabrechnung verwendete Datenverarbeitungsprogramm das Prüfergebnis nicht zu verbessern wäre.

12.6 Sonstiges

12.6.1 Entrümpelung eines behördlichen Bodens

Nach wie vor kommt es vor, daß bei Aktionen zur Entsorgung von alten Unterlagen mit Personenbezug nicht mit der gebotenen Sorgfalt vorgegangen wird. Eine Stadtverwaltung hatte ein Gebäude übernommen, auf dessen Dachboden Papierunterlagen gefunden worden waren, die aus Gründen des Brandschutzes fortgeschafft werden sollten. Eine Entsorgungsfirma warf dieses Material über den Balkon in einen bereitstehenden LKW. Dabei wurden diverse Papierseiten und Karteikarten über den Vorhof bis auf die angrenzende Straße verstreut. Ein Bürger hatte mich telefonisch über diesen Vorgang informiert.

Mitarbeiter meiner Behörde fanden bei einer sofort vorgenommenen Ortsbesichtigung die Beschreibung des Anrufers bestätigt und konnten einige Unterlagen mit Namen, Geburtstagsangaben, Anschriften, Versicherungsangaben u. ä. als Beweismittel sicherstellen. Recherchen bei der Entsorgungsfirma und dem zuständigen Amt der Stadtverwaltung ergaben, daß man sich dort über die Tatsache, daß hier personenbezogene Altdaten aus DDR-Zeiten vorlagen, nicht im klaren war. Jedenfalls wurden durch den laxen Umgang mit solchen Daten die Persönlichkeitsrechte der Betroffenen eindeutig verletzt. Denn § 10 Abs. 3 BbgDSG regelt klar, daß bei dem Transport und der Vernichtung von personenbezogenen Daten in nicht-automatisierten Dateien oder Akten Maßnahmen zu treffen sind, die den Zugriff Unbefugter ausschließen. Früher schon habe ich mich zu der Erstellung von Dienstanweisungen für die praktische Regelung des Datenschutzes

einschließlich der kontrollierten Datenträgervernichtung geäußert[200].

Immerhin sind die zuständigen Bearbeiter der besagten Stadtverwaltung sofort tätig geworden, um den weiteren Fortgang der Entsorgungsaktion zu kontrollieren. Der Leiter der Stadtverwaltung hat mich später unterrichtet, daß er in Auswertung des Vorfalls eine interne Dienstanweisung zur Entsorgung von Altpapierbeständen erlassen will.

12.6.2 Fragebogen zur Reduzierung der Betreuungszeit in Kindergärten

In der Fragebogenaktion einer Kommune wurden Eltern mit dem Fragebogen u. a. darüber informiert, daß von 1997 die Regelbetreuungszeit in Kindergärten und im Krippenbereich von derzeit 10 auf 8 Stunden reduziert werden solle. Der Fragebogen, der der Ermittlung der konkreten Bedarfssituation dienen sollte, ließ weder den Urheber erkennen, noch enthielt er einen Hinweis über die Rechtsgrundlage der Erhebung sowie den Zweck der Verarbeitung oder Nutzung der Daten.

Das zuständige Amt informierte mich auf Nachfrage darüber, daß sämtliche Namensangaben auf den Fragebögen vernichtet worden seien und lediglich eine prozentuale Auswertung erfolgt sei, aus der hervorgehe, wieviele Eltern Schwierigkeiten mit einer Verkürzung der Regelöffnungszeit hätten. Dem Jugendamt, das die Umfrage durchgeführt hatte, teilte ich mit, daß eine personenbezogene Datenerhebung hier nicht erforderlich gewesen war. In Zukunft sollte deshalb vor der Befragung geprüft werden, ob die Befragung überhaupt namensbezogen durchgeführt werden muß. Darüber hinaus empfahl ich, auf die Freiwilligkeit der Angaben hinzuweisen, soweit - wie hier - keine gesetzliche Auskunftspflicht besteht. Meine Hinweise wurden in einer Dienstberatung mit den Sachgebietsleitern des Jugendamtes ausgewertet und die Mitarbeiter angewiesen, die §§ 61 bis 68 SGB VIII stärker zu beachten. In Zukunft werde das Jugendamt zur Vermeidung datenschutzrechtlicher Beanstandungen meine Behörde rechtzeitig einschalten.

12.6.3 Zweitwohnungssteuer

Einige Eingaben bezogen sich auf die Grundlagen zur Erhebung der Zweitwohnungssteuer. Die Tatsache, daß im Zusammenhang mit der Erhebung dieser Abgabe die Größe, d. h. die Wohn- und Nutzfläche, oder die Qualität der Ausstattung der Wohnung erfragt wird, ist oft für die Betroffenen befremdlich. Gerade die Ausstattung wird als sehr privates Datum empfunden.

Da über die Größe und über die Kategorien, durch die die Art der Ausstattung bestimmt wird, ein fiktiver Wert für die zu besteuernde Zweitwohnung errechnet werden kann, der von der tatsächlich gezahlten Miete unabhängig ist, ergibt sich für die eine Zweitwohnungssteuer erhebenden Gemeinden ein relativ einfacher Weg, die Steuer so objektiv wie möglich festzusetzen, sofern die Satzung in ordnungsgemäßer Weise die Grundlage für ein derartiges Vorgehen bietet.

Probleme haben sich gezeigt, wenn in Fragebögen zur Vorbereitung der Steuererhebung auch nach den Namen von Mietern, der Höhe der Miete gefragt oder der komplette Mietvertrag verlangt wird. Die Frage nach den näheren Umständen der Vermietung zielt darauf ab, herauszufinden, ob sich der Vermieter trotz der Vermietung die Möglichkeit vorbehält, die betreffende Wohnung auch selbst zu nutzen. Gleichwohl bin ich der Meinung, daß Namensangaben der Mieter und erst recht die Überlassung einer Kopie des ganzen Mietvertrages der Gemeinde einen Überschuß an Informationen bringt, der zur Steuerfestsetzung nicht erforderlich ist. In der Regel sollte eine Erklärung des Eigentümers

[200] s. 3. Tätigkeitsbericht unter 1.3.2

über die Art und den Umfang der Vermietung ausreichen. Auch die Höhe der Miete wird meist allenfalls als Hinweis, nicht aber als Beweis dafür genutzt werden können, daß eine Wohnung nur von den Mietern und nicht auch zeitweise vom Eigentümer selbst genutzt wird. Aus der Angabe, wann ein Mietverhältnis begonnen hat bzw. wann es endet, kann nichts verbindlich gefolgert werden. Die Angabe kann nur ein Hinweis sein. Wohnungsleerstand bedeutet nicht zwingend, daß der Mieter die Wohnung in der Zeit der Nichtvermietung als Zweitwohnung nutzt.

Soweit die Frage nach Mietverhältnissen allerdings auf die Art der Nutzung durch den Mieter gerichtet ist, kann sie nicht gerechtfertigt sein. Der Vermieter weiß nicht, wie der Mieter oder welcher der Mieter die vermietete Wohnung nutzt. Die Gemeinde wird es nicht vermeiden können, Personen, die mit Zweitwohnsitz gemeldet sind, jeweils immer selbst zur Erklärung aufzufordern, um auf Grund der Erklärung die Steuer erheben zu können.

12.6.4 Selbstauskunftsaufforderung und Datenverarbeitung der Zweckverbände

In dem Bestreben, möglichst flächendeckend den Anschluß der bewohnten oder genutzten Grundstücke an die Kanalisation voranzutreiben (vgl. §§ 66, 68 BbgWG[201], §§ 3, 15 GO[202], §§ 1, 6 GKG[203]), sind die Wasser- und/oder Abwasserzweckverbände auf Informationen der Grundstückseigentümer zu der bestehenden Wasser- und Abwassersituation der Grundstücke angewiesen. In diesem Zusammenhang haben mich zahlreiche Anfragen von Betroffenen, die sowohl über Art und Umfang, als auch über die Vorgehensweise bei der Informationsermittlung verunsichert waren, erreicht.

Um die für ihre Bestandsaufnahmen, Planungen und Abrechnungen erforderlichen Daten zu erhalten, versenden die Abwasserzweckverbände entsprechende Fragebögen, die von den Betroffenen ausgefüllt zurückgeschickt werden sollen.

Bei Prüfung des gesamten Verfahrens hat sich wieder einmal gezeigt, wie wichtig die Gestaltung von Fragebögen ist. In den meisten Fällen war es nämlich durchaus so, daß die Verbände die Beantwortung der Fragen verlangen durften, daß jedoch die Darstellung der Fragen bzw. die Hinweise zum Ausfüllen der Fragebögen häufig zu wünschen übrig ließen[204].

Den genannten Verbänden obliegt originär die Aufgabe der Wasserversorgung und der Abwasserentsorgung. Für eine rechtmäßige und sinnvolle Aufgabenerfüllung ist die Kenntnis bestimmter Daten erforderlich. Rechtlicher Maßstab für das Handeln zur Erfüllung der Aufgaben sind die jeweiligen Satzungen, die aufgrund des Brandenburgischen Wassergesetzes und des Brandenburgischen Kommunalabgabengesetzes sowie des Gesetzes über die Kommunale Gemeinschaftsarbeit erlassen worden sind, aus denen sich die Aufgaben und Pflichten sowie die Kompetenzen der Verbände ergeben. Zusätzlich wird in den Satzungen deklaratorisch meist noch eine entsprechende Auskunftspflicht der Betroffenen vorgeschrieben. Ausdrücklich hinweisen möchte ich in diesem Zusammenhang auch noch darauf, daß personenbezogene Daten gem. § 12 BbgDSG direkt beim Betroffenen zu erheben und nicht durch die Befragung von Nachbarn oder sonstigen Dritten zu ermitteln sind. Auf die Verteilung der Rechte und Pflichten sollten die Betroffenen in einem Anschreiben zu dem Fragebogen oder auf diesem selbst, unter Nennung der entsprechenden

---

201 Brandenburgisches Wassergesetz vom 13. Juli 1994, GVBl. I S. 302

202 Gemeindeordnung für das Land Brandenburg vom 15. Oktober 1993, GVBl. I S. 398, geänd. d. Art. 3 d. 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

203 Gesetz über Kommunale Gemeinschaftsarbeit vom 19. Dezember 1991, GVBl. S. 685

204 s. 4. Tätigkeitsbericht unter 2.3

Vorschriften, ausführlich und in angemessener Form hingewiesen werden. Das gleiche gilt für eine möglicherweise vorgesehene Datenübermittlung an Dritte.

Im Zusammenhang mit den Eingaben zu den Selbstauskunftsbogen habe ich Kontrollbesuche bei den Verbänden durchgeführt. Dabei bot sich mir ein sehr unterschiedliches Bild. Während bei einem der besuchten Verbände die Datenerfassung mittels eines Selbstauskunftsbogens in rechtmäßiger Weise erfolgte und man sehr bemüht war, die Datenverarbeitung auch ansonsten datenschutzgerecht zu gestalten, hatte man bei einem anderen Verband sogar versucht, personenbezogene Daten mittels Postkarte zu ermitteln. In diesem Fall waren mit den zur eigenen Aufgabenerfüllung erforderlichen Daten gleichzeitig zusätzliche - nur zur Aufgabenerfüllung der Meldebehörden notwendige - Daten angefordert worden. Dabei bezog sich eine der zu beantwortenden Fragen nicht einmal auf die Betroffenen selbst, sondern auf deren Nachbarn und stellte damit eine unzulässige Fremddatenerhebung dar. Personenbezogene Daten dürfen keinesfalls mittels Postkarte, sondern nur in verschlossenen Umschlägen angefordert werden, da nur durch die Verwendung verschlossener Umschläge eine unerlaubte Datenoffenbarung an Dritte erreicht werden kann. Auf meine entsprechenden Hinweise hin ist dieses Verfahren eingestellt worden.

Des weiteren bin ich darauf gestoßen, daß die Verbände von der Möglichkeit Gebrauch machen, Teile ihrer Aufgaben, wie z. B. die Gebührenabrechnung, durch Dritte erledigen zu lassen oder auch Wartungsfirmen für die EDV-Pflege einzusetzen. Zur eigenen Aufgabenerfüllung und zur Wartung der DV-Anlage werden privatrechtliche Verträge abgeschlossen. Unberücksichtigt bleibt dabei in der Regel aber die Tatsache, daß auch personenbezogene Daten anfallen und daß entsprechend rechtliche und tatsächliche Vorsichtsmaßnahmen zu treffen sind.

Auch wenn die Möglichkeit einer solchen Datenverarbeitung im Auftrag nicht ausdrücklich aus der Satzung des jeweiligen Verbandes hervorgeht, so ist dies nach § 11 BbgDSG grundsätzlich zulässig. Allerdings müssen dabei die datenschutzrechtlichen Vorgaben eingehalten und entsprechende Regelungen mit in den privatrechtlichen Vertrag aufgenommen werden.

Die Nichtbeachtung der datenschutzrechtlichen Aspekte ist aber offenbar nicht Ausdruck einer Mißachtung gegenüber den Belangen des Datenschutzes, sondern resultiert vielmehr aus einer mangelnden Kenntnis der Bestimmungen bzw. aus einem fehlenden datenschutzrechtlichen Bewußtsein.

Mängel boten sich mir bei der Überprüfung auch bezüglich organisatorischer Sicherheitsaspekte bei der Datenverarbeitung. So habe ich festgestellt, daß die Daten durch Abspeichern zwar gesichert, aber nicht ausreichend vor einem unberechtigten Zugriff geschützt werden. Dieser Mangel sollte durch geeignete technisch-organisatorische Maßnahmen, wie Verschlüsselung und eine hinreichende Sicherung der Räumlichkeiten behoben werden.

12.6.5 Studie zur Wohnsituation älterer Bürger

Ein an einer Fachhochschule des Landes eingerichtetes Seniorenseminar hatte sich die Projektaufgabe gestellt, mit Befragungen in einer kreisangehörigen Stadt und zwei angrenzenden kleineren Gemeinden die Wohnsituation älterer Bürger und deren soziales Umfeld zu untersuchen. Die Kommunen selbst hatten daran Interesse signalisiert und insoweit

auch finanzielle Förderung in Aussicht gestellt. Die aus der Studie gewonnen Erkenntnisse sollten diesen zur Verfügung gestellt werden, damit die Bedürfnisse und Befindlichkeiten älterer Bürger besser als bisher in der Kommunalpolitik berücksichtigt werden. Das Projekt wurde mir von der Fachhochschule mit der Bitte angetragen, den umfänglichen Fragebogen - u. a. zu der Wohnung, dem Wohnpartner, der Bezahlbarkeit, der Kommunikation, der Betreuung, der Versorgung, der Mobilität, der Infrastruktur und zur befragten Person selbst - einer kritischen Bewertung zu unterziehen. Dieser sollte entweder als Grundlage für ein Interview-Verfahren dienen oder den älteren Bürgern (älter als 55 Jahre) durch Postversand zugestellt werden.

Das sicherlich begrüßenswerte Anliegen dieses Projektes war bei näherer Betrachtung in verschiedener Hinsicht nachbesserungsbedürftig. Den Initiatoren war offenbar weder bekannt, wie dafür die Gruppenauskunft gem. § 32 Abs. 3 Brandenburgisches Meldegesetz[205] zu beantragen ist, noch welche weiteren Rechtsgrundlagen bei der Datenverarbeitung im einzelnen zu beachten sind. Zweifel bestanden vor allem daran, ob die angedachte Studie nicht weit über die eigentlich erforderlichen Belange der Kommunalverwaltung hinausgingen und insoweit eine überperfektionierte Datenerfassung vorgesehen war. So sollte beispielswiese die Wohnungsgröße (qm) in Zehnerstufen, das Verhältnis zum Wohnungspartner, der Behinderungsgrad der Personen im Haushalt sowie Geschlecht und Berufsausbildung von Haushaltsmitgliedern abgefragt werden. Aufgrund meiner hierzu geäußerten Bedenken ist daraufhin ein pauschalerer Abfragemodus gewählt und aufgrund der Kleinräumigkeit zunächst von einer Befragung in den beiden Gemeinden Abstand genommen worden.

Darüber hinaus habe ich zu bedenken gegeben, daß dem Betroffenen die Möglichkeit eingeräumt werden muß, allein und in Ruhe den Fragebogen auszufüllen. Einer Eingabe zufolge war dies dann in der Praxis wohl nicht ausreichend gewährleistet worden. Es muß im Gegenteil der Eindruck entstanden sein, daß es dem Interviewer eher darum ging, wegen der damit verbundenen Anerkennung möglichst viele Interviews "durchzuziehen".

13 Personaldatenverarbeitung

13.1 Verwaltungsvorschriften zur Personalaktenführung

13.1.1 Rechtssituation

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

In meinem 4. Tätigkeitsbericht[206] hatte ich die Erwartung ausgedrückt, daß die in Vorbereitung befindliche Verwaltungsvorschrift über die Führung von Personalakten der Dienstkräfte des Landes Brandenburg (Personalaktenverwaltungsvorschrift - PersaktVV) "weiterführender" sein wird, als die zwischenzeitlich erlassenen "Allgemeine Hinweise zu datenschutzrechtlichen Vorgaben bei der Führung von Personalakten"[207]. Der jetzt vorliegende Entwurf zeigt, daß dies mit seiner Verabschiedung zumindest bzgl. des Regelungsinhalts gelingen könnte. Gleichwohl bleibt ungeachtet einiger Mängel im Detail auch weiterhin ein formal-rechtlicher Grundmangel festzustellen:

Zwar soll mit der Verwaltungsvorschrift wünschenswerterweise auch die Personalaktenführung für Arbeiter und Angestellte erfaßt werden, jedoch kann sich eine durchsetzbare und unmittelbare justitiable Anwendungsverpflichtung zum Wohle Betroffener nur für den Kreis der Beamten und der in einem öffentlich-rechtlichen Ausbildungsverhältnis stehenden Personen ergeben, da die Verwaltungsvorschrift - mangels entsprechender materiell-rechtlicher Regelungen in Tarifverträgen und allgemeinen Vorschriften des Arbeitsrechts - allein aufgrund von § 156 Landesbeamtengesetz (LBG)[208] erlassen werden soll.

Da z. B. die Tarifverträge (bis auf das Akteneinsichtsrecht) und die allgemeinen Vorschriften des Arbeitsrechts keine Regelungen für den Umgang mit den Personalakten von Arbeitern und Angestellten enthalten, sind die allgemeinen Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) anzuwenden. Dabei führt insbesondere § 29 BbgDSG, mit dem die Personaldatenverarbeitung geregelt wird, zu einigen anderen Ergebnissen als die § 56 bis 64 LBG (z. B. bei der Weitergabe von Personalaktendaten an Dritte). So ist auch die Aufbewahrungsfrist für Personalakten bei Beamten an die grundlegend anders gestaltete Beamtenversorgung geknüpft und kann nicht ohne weiteres auf die Personalakten der übrigen Beschäftigten des öffentlichen Dienstes übertragen werden. Zwar wird zu Beginn des Entwurfs darauf hingewiesen, daß die Verwaltungsvorschriften nur sinngemäß auch für die Führung von Personalakten der als Arbeitnehmer tätigen Dienstkräfte gelten können, jedoch wird damit zugleich auch deutlich, daß möglicherweise noch über die zuvor genannten Beispiele hinaus mangels Normenklarheit Interpretations- bzw. Anwendungszweifel entstehen könnten. Dem Gleichbehandlungsgebot könnte letztlich nur durch Einbettung vergleichbarer Regelungen in einem allgemein-verbindlichen Gesetz zum Arbeiternehmerdatenschutz Rechnung getragen werden. Hierauf werde ich - gemeinsam mit Kollegen in den anderen Bundesländern - immer wieder hinweisen. Ergänzend bleibt auch festzustellen, daß die wünschenswerte verbindliche Anwendbarkeit der für die Personalaktenführung bei Beamten unmittelbar geltenden Entwurfsregelungen nur in Form einer materiell-rechtlichen Regelung auch im Kommunalbereich zu erreichen wäre. Gleichwohl begrüße ich den Willen der Landesregierung, durch Selbstbindung zumindest für ihre unmittelbare und ihrer Aufsicht unterstehende mittelbare Landesverwaltung Regelungen zu finden, die geeignet sind, auf der Grundlage der weitreichenden Datenschutzbestimmungen im Landesbeamtengesetz aufbauend als Leitfaden für datenschutzgerechte Handhabung der Personalaktendaten im Sinne des informationellen Selbst-bestimmungsrechts der Beschäftigten zu dienen. Es bleibt zu hoffen, daß Gemeinden und Gemeindeverbände in ihrer Pflicht und in ihrem Willen zu gesetzmäßigem Handeln bereit sind, diesen Vorteil auch ohne Verpflichtung unmittelbarer Anwendung der Verwaltungsvorschrift zu nutzen. Immerhin werden sie sich z. B. bei datenschutzrechtlichen Überprüfungen in der Behandlung von Personalakten an den Bestimmungen der Verwaltungsvorschrift messen lassen müssen.

13.1.2 Sachstand

---

206 s. unter 13.2.1

207 Rundschreiben II/1 - 65 - 80 des MI vom 26. September 1995

208 vom 24. Dezember 1992, GVBl. I S. 506

Zum Regelungsinhalt des vorliegenden Entwurfs begrüße ich das Vorhaben, auch aktuellere Probleme der Personalaktenführung - wie die Behandlung von BStU-Unterlagen und noch vorhandenen "Vorakten" (Altpersonalakten/Kaderakten) - lösen zu wollen, die erst durch oder im Zusammenhang mit der Vereinigung entstanden sind. Erkennbar ist auch der Wille, die Regelungen im Detail nach datenschutzrechtlichen Erfordernissen - unter Berücksichtigung des bisherigen Meinungsaustausch mit meiner Behörde - auszurichten.

Gleichwohl bleibt eine Reihe von Kritikpunkten, zu denen ich weitgehende Empfehlungen oder konkrete Änderungsvorschläge formuliert habe. Dabei kam es mir insbesondere darauf an, daß erforderliche Begriffsdefinitionen so präzisiert werden, daß sie sowohl für die Betroffenen als auch für die mit der Personalaktenführung betrauten Mitarbeiter/-innen möglichst unmißverständlich sind. Dies halte ich vorrangig dann für erforderlich, wenn Rechte bzw. Verarbeitungsschritte von so unklaren Formulierungen wie "aus wichtigem Grund" oder "aus dienstlichen Gründen" abhängig gemacht werden sollen. Hier verlange ich durchgängig eine begriffliche Koppelung an unmittelbare dienst- oder arbeitsrechtliche Erfordernisse bzw. an unabdingbare Erfordernisse für eine ordnungsgemäße Bearbeitung der Personalakten.

Ausdrücklich begrüße ich es, daß das MI geneigt ist, meinen Empfehlungen weitgehend zu folgen, wenngleich bei einem gemeinsamen Gespräch mit Vertretern der obersten Landesbehörden im Januar 1997 deutlich wurde, daß eine einheitliche Sichtweise zum Regelungsumfang der Verwaltungsvorschrift zunächst noch nicht herstellbar ist. Während Vertreter einiger Ministerien von einer Überregulierung sprechen, die dem Bemühen entgegenstehe, überflüssige Normsetzungen und in der Sache nicht gerechtfertigten Verwaltungsaufwand zu vermeiden, vertrete ich auch aufgrund meiner Erfahrungen aus vielfältigen Anfragen aus allen Teilen der Landes- als auch der Kommunalverwaltung die Auffassung, daß die Verwaltungsvorschriften so klar und präzise sein müssen, daß sie für die Nutzer auch anwendbar sind. Dabei müssen die zu regelnden Formalaspekte so transparent sein, daß jedes Verwaltungshandeln sowohl für die zugriffsberechtigten Bearbeiter als auch für die Betroffenen selbst nachvollziehbar ist. Im übrigen müssen die Personalakten einheitlich von ihrem Aufbau so gestaltet sein, daß jederzeit eine Überprüfbarkeit ordnungsgemäßer Behandlung der Personalaktendaten gegeben ist. Dem müssen auch die Aktenvorblätter als besondere Arbeitshilfsmittel und Dokumentationen Rechnung tragen.

Schwerpunkt der bisherigen Diskussionen waren ganz allgemein Umfang und Sinn der beabsichtigten Regelungen, im speziellen die Festlegungen zu Zugriffsrechten von Geheimschutzbeauftragten sowie zur Behandlung der Vorakten und der sog. "Gauck-Unterlagen". Zumindest bezüglich der zuletzt genannten Unterlagen besteht weitestgehend Konsens auf der Grundlage der "Grundsätze der Landesregierung für die Überprüfung von Dienstkräften des Landes Brandenburg hinsichtlich einer Tätigkeit für das ehemalige Ministerium für Staatssicherheit/Amt für nationale Sicherheit (MfS/AfNS)[209]. Hierüber hatte ich bereits im 4. Tätigkeitsbericht näher ausgeführt[210].

13.1.3 Offene Einzelfragen

Von den wenigen Punkten, über die noch keine Einigung erzielt werden konnte, bzw. die noch kontrovers diskutiert werden, sollen nachstehend einige hervorgehoben werden:

---

[209] vom 10. Oktober 1995, ABl. S. 914

[210] s. unter 13.2.3

13.1.3.1 Zugriffsrechte des Geheimschutzbeauftragten

Dem Geheimschutzbeauftragten sollen originäre Zugriffsrechte eingeräumt werden. Das MI verweist dabei auf die Gesetzesbegründung zu Abs. 3 von § 90 Bundesbeamtengesetz (BBG), wo es heißt: "Eingeschlossen in diese Zugangsregel (Anmerkung: Zugang zur Personalakte) sind auch solche Bearbeiter von Personalangelegenheiten, die an bestimmten Aufgaben und Entscheidungen der Personalverwaltung zu beteiligen sind. Das gleiche gilt für Geheimschutzbeauftragte im Rahmen der Sicherheitsrichtlinien." Gleichwohl halte ich an meiner Auffassung fest, daß die Erweiterung des Berechtigtenkreises um diese Personengruppe unzulässig ist, da eine materiell-rechtliche Befugnisnorm, die eine Teilzuständigkeit von Geheimschutzbeauftragten für die Bearbeitung von Personalangelegenheiten begründen würde, bislang in Brandenburg nicht vorhanden ist. Es kann nicht angehen, daß mit einer Verwaltungsvorschrift der Versuch unternommen wird, dem Geheimschutzbeauftragten Rechte zuzubilligen, die z. B. Personalräten oder Gleichstellungsbeauftragten in aller Normenklarheit gemäß Personalvertretungsrecht bzw. Landesgleichstellungsgesetz materiell-rechtlich geregelt zustehen. Die für bestimmte Tätigkeitsbereiche wichtige Beteiligung von Geheimschutzbeauftragten könnte bis zur Schaffung einer materiell-rechtlichen Befugnisnorm, etwa in einem landeseigenen Sicherheitsüberprüfungsgesetz, dadurch sichergestellt werden, daß Geheimschutzbeauftragte zwar keinen eigenen Zugang zur Personalakte haben, Ihnen jedoch im Rahmen ihrer Aufgabenerfüllung von den zugangsberechtigten Dienstkräften Informationen aus der Personalakte im Rahmen der Erforderlichkeit zur Verfügung gestellt werden.

13.1.3.2 Kopierrechte Betroffener an Gauck-Berichten

Unter Verweis auf die vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) vertretene Rechtsauffassung zweifelt das MI weiterhin das Recht Betroffener auch auf Erhalt von Kopien der über sie erstellten BStU-Berichte an und stellt fest, daß lediglich zum Zweck der Rechtsverteidigung im Einzelfall Kopien herausgegeben werden dürften, im übrigen nur die Einsichtnahme Betroffener in die Bescheide gewährleistet sein müsse. Bereits im 4. Tätigkeitsbericht[211] hatte ich ausgeführt, daß die Rechtsauffassung des BStU jeder rechtlichen Grundlage entbehrt. Ich sehe keinen Ansatz, in diesem Punkt von meiner bisherigen rechtlichen Bewertung abzugehen.

13.1.3.3 Einsichtsrechte - vom Beschäftigungsverhältnis abhängig?

Zwar teilt das MI meine Auffassung, daß es nicht des Hinweises bedarf, daß Beamten aus der Fürsorgepflicht heraus Einsicht in die Personalakten nach Beendigung des Dienstverhältnisses zu gewähren ist, weil dieses Recht bereits unkommentiert in § 60 Abs. 1 LBG begründet ist. Allerdings will das MI einer Formulierung nicht ohne weiteres zustimmen, daß dieses Recht generell (auch für Arbeitnehmer) besteht. Es verweist dabei auf das Fehlen einer diesbezüglichen Regelung im BAT bzw. BAT-O. Daher sieht der Entwurf für Arbeitnehmer ein Recht auf Einsichtnahme in ihre Personalakte nach Beendigung des Beschäftigungsverhältnisses nur vor, wenn diese ein berechtigtes Interesse darlegen. Ich halte dies für nicht hinnehmbar, weil hierdurch eine nicht dem Gleichbehandlungsgrundsatz Rechnung tragende Unterscheidung der Beamten zu anderen Beschäftigten vorgenommen wird. Hinnehmbar wäre eine allgemeine Formulierung, daß die Einsichtnahme in die Personalakte auch nach Beendigung des Dienst- oder Beschäftigungsverhältnisses zugelassen ist.

Das Akteneinsichtsrecht während des laufenden Dienst- bzw. Beschäftigungsverhältnisses ist gemäß Protokollnotiz zu § 16 Abs. 1 BAT-O bei Angestellten weiter ausgeprägt als bei Beamten, bei denen es in § 60 Abs. 3 LBG einschränkend heißt: "... soweit dienstliche Gründe nicht entgegenstehen." Diese Formulierung auch auf Angestellte auszuweiten, wäre unzulässig.

---

[211] s. unter 13.2.4

Hieraus im Interesse des Gleichbehandlungsgrundsatzes nun auch ein uneingeschränktes Einsichtsrecht bei Beamten abzuleiten, hält das MI allerdings nicht für vertretbar. Wenn jedoch schon eine dem LBG folgende Einschränkung bei Beamten vorgenommen werden soll, müßte zumindest auch hier der zu allgemein gehaltene Begriff "dienstliche Gründe" im Sinne ordnungsgemäßer Aufgabenerfüllung bei der Personalaktenbearbeitung eingeschränkt und näher definiert sein. Als Kompromiß wäre denkbar, daß das allgemeine Akteneinsichtsrecht bei Beamten mit dem einschränkenden Zusatz versehen wird "... soweit zwingende dienstliche Gründe nicht entgegenstehen". Da die "zwingenden dienstlichen Gründe" - entsprechend meinen Forderungen - zuvor in der Verwaltungsvorschrift als allgemeine Bearbeitungsvoraussetzung eindeutig definiert sein werden, könnte dies eine dem Gleichbehandlungsgrundsatz angemessen entgegenkommende Formulierung darstellen.

13.1.3.4 Behandlung der Vorakten - eher ein Problem der Praxis

Ein besonderes Problem stellen sowohl hinsichtlich der rechtlichen Zuordnung als auch ihrer praktischen Behandlung die Vorakten (Altpersonalakten/Kaderakten) dar. Da von den Vertretern einiger Ministerien behauptet worden war, daß alle Teile der Vorakten auch heute noch erforderlicher Bestandteil der Personalakten sein müßten bzw. derart mit den laufenden Vorgängen in den Personalakten verknüpft seien, daß eine Abtrennung und besondere Behandlung nicht oder nur mit unverhältnismäßig hohem Aufwand ermöglicht werden könne, habe ich ein Polizeipräsidium, das bis dahin noch keine Aussonderung der Vorakten vorgenommen hatte, aufgesucht und anhand mehrerer willkürlich herausgegriffener Personalakten folgendes festgestellt:

- Alle Personalakten begannen mit den Vorakten.

- Die Voraktenteile waren nicht eingegrenzt, allerdings war von einem bestimmten Datum an erkennbar, wann die nach Übernahme der Mitarbeiter/-innen laufende Bearbeitung beginnt.

- Die Voraktenteile enthielten Beurteilungen und Hinweise auf Veranstaltungen, die heute völlig ohne Relevanz, möglicherweise sogar diskriminierend sind.

- Die Vorakten enthielten darüber hinaus eine Reihe von Fremddaten (z. B. Personalfragebögen mit detaillierten, in die Privatsphäre hineinreichenden Angaben zu Verwandten bis zum dritten Grad).

Ich teile die Auffassung des MI, daß für das neue Dienst- bzw. Arbeitsverhältnis relevante Unterlagen aus früheren Kaderakten Bestandteile der Personalakten sind. Dies kann aber nicht auch für die Teile zutreffen, die nicht unmittelbar in diesem Zusammenhang benötigt werden. Mangels einer materiell-rechtlichen Spezialregelung kann dies nur zu der Schlußfolgerung führen, daß alle für das neue Dienst- bzw. Arbeitsverhältnis benötigten Unterlagen aus den Vorakten herauszunehmen bzw. zu kopieren sind und entweder im Original oder als Kopie unmittelbarer Bestandteil der neuen Personal(Grund)akte werden.

Alle anderen hierfür nicht mehr erforderlichen Unterlagen können folglich nicht Bestandteil der Personal(Grund)- und somit auch nicht einer Teilakte sein. Dies bedeutet, daß solche Unterlagen gem. § 37 Abs. 1 Satz 1 BbgDSG als gesperrt gelten und entsprechend den gesetzlichen Vorgaben ordnungsgemäß behandelt und aufbewahrt werden müssen.

Da einerseits eine einheitliche Archivierung sämtlicher Vorakten nach dem Brandenburgischen Archivgesetz nicht gewährleistet werden kann, andererseits nicht ausgeschlossen werden kann, daß Teile später noch im Interesse der

Betroffenen (evtl. als Beleg für später entstehende Anspruchsmöglichkeiten oder zur Behebung einer Beweisnot) benötigt werden, kommt auch eine Löschung i. S. v. § 19 BbgDSG nicht in Frage. Daraus ist zu erkennen, daß - sofern sich keine zufriedenstellende verwaltungspragmatische Lösung über die öffentlichen Archive finden lassen sollte - nur eine eigenständige materiell-rechtliche Regelung zur Behandlung der Vorakten eine einheitliche Handhabung im Interesse der Betroffenen gewährleisten kann. Leider ist bis dato nicht bekannt, ob die Landesregierung eine solche Regelung anstrebt.

Gleichwohl halte ich es im Interesse der Betroffenen für vertretbar, daß mit der beabsichtigten Verwaltungsvorschrift bis zur Schaffung einer spezialgesetzlichen Regelung davon ausgegangen wird, daß auch die weitere Speicherung der nicht unmittelbar zur fortlaufenden Bearbeitung der Personalakte benötigten Teile der Vorakten im Interesse der Betroffenen geboten ist und diese insoweit bis auf weiteres als im datenschutzrechtlichen Sinne gesperrt im Zugriffsbereich der Personalstellen - wenn auch getrennt von der Personalakte - verschlossen aufzubewahren sind. Hierüber besteht zumindest mit dem MI Einvernehmen.

Vermutlich ist die bei Vertretern einiger oberster Landesbehörden zu beobachtende Ablehnung, die hierzu erforderliche Aktenbereinigung und Aussonderung vorzunehmen, darauf zurückzuführen, daß der damit verbundene Verwaltungsaufwand gefürchtet wird. In Einzelgesprächen wurde mir sowohl von den Personalsachbearbeitern als auch den weiteren Verantwortlichen zugestanden, daß es mit verhältnismäßig geringem Aufwand möglich sei, zumindest anlaßbedingt im Rahmen laufender Bearbeitung eine Bereinigung der Akten vorzunehmen. Es wird auch zugestanden, daß diese Form der Aktenbereinigung als ein im Interesse der Innenrevision laufendes Programm gesehen werden kann. Darüber hinaus wurde mir bestätigt, daß es aus arbeitsökonomischer Sicht durchaus möglich sei, in einem Zeitraum von ca. zwei Jahren parallel zur anlaßbedingten Bereinigung sukzessive auch eine retrograde Bereinigung aller übrigen Personalakten im obigen Sinne vorzunehmen.

13.2 Personalnachrichten in Ministerialblättern und in Hausmitteilungen

Aufgrund einer Verfügung des Ministers der Justiz[212] werden im Justizministerialblatt für das Land Brandenburg regelmäßig Personalnachrichten veröffentlicht. Dabei handelt es sich um Daten zu Ernennungen, Amtsübertragungen, Versetzungen, Ausscheiden aus dem Dienst, Ruhestand, Tod bei Beamten, um Daten zu Bestellungen, Verlegungen des Amtssitzes, Erreichen der Altersgrenze, Erlöschen des Amtes, Amtsenthebung bei Notaren und um Daten zu Eintragungen und Löschungen in der Anwaltsliste bei Rechtsanwälten.

Bezüglich der Verwaltungsbeamten stellt die Veröffentlichung eine Auskunft über Personalaktendaten i. S. v. §§ 57 LBG dar. Hiernach dürfen entsprechende Daten nur weitergegeben werden, wenn es die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Informationsempfängers zwingend erfordert.

Diese Voraussetzungen können schon deshalb nicht vorliegen, weil zum einen die Informationen an einen nicht bestimmbaren Empfängerkreis gelangen (können), ohne daß individuell eine Interessenabwägung stattfinden könnte, zum anderen das Gemeinwohl ohne die Publikationen wohl kaum beeinträchtigt würde. Ein eher allgemeines oder das gezielte Interesse allenfalls einer Interessentengruppe innerhalb des Empfängerkreises rechtfertigt jedenfalls eine uneingeschränkte Publikation aus dem Gesetz heraus nicht.

---

[212] Allgemeine Verfügung des Ministers der Justiz vom 21.April 1994 (1202-1.10) - JMBl. Bbg. S. 67

Das Ministerium der Justiz und für Bundes- und Europaangelegenheiten wird daher auf mein Betreiben hin entsprechend § 4 Abs. 1 Buchst. b BbgDSG i. V. m. § 61 Abs. 2 LBG zukünftig entsprechende Veröffentlichungen von der vorherigen schriftlichen Einwilligung der Betroffenen abhängig machen. Die näheren Verfahrensregelungen sollen in die genannte Rundverfügung eingearbeitet werden.

Zu einer anderen Bewertung komme ich hinsichtlich der Veröffentlichung von Personalnachrichten in den "Hausmitteilungen" der Ministerien, soweit es sich um Daten von Beamten, Angestellten und Arbeitern handelt, die den Dienstantritt, die Beendigung des Dienst- bzw. Arbeitsverhältnisses, Umsetzungen und Versetzungen betreffen. Ich folge der Argumentation des Ministeriums des Inneren, daß die Bekanntgabe dieser Daten für einen reibungslosen Geschäftsablauf im jeweiligen Ministerium von besonderer Bedeutung ist, die anderen Beschäftigten insoweit über diesbezügliche Informationen verfügen müssen. Dazu gehört auch die Mitteilung über Beförderungen von Beamten, da der Beamte gem. § 51 Abs. 3 LBG im Dienst die Dienstbezeichnung des ihm übertragenen Amtes führt und im Falle eines Übertritts in ein anderes Amt Anspruch, aber auch Verpflichtung hat, die neue Amtsbezeichnung zu führen bzw. unter dieser geführt zu werden.

Hier liegen bezüglich des Empfängerkreises dienstliche, also berechtigte Interessen an den Informationen vor, die den durch dienst- oder arbeitsrechtliche Verpflichtungen modifizierten Eigeninteressen Betroffener vorangehen. Insgesamt sind solche Veröffentlichungen aber nur zulässig, wenn die genannten Daten ohne weitere Informationen zu deren entscheidungsrelevanten Hintergründen bekanntgegeben werden und sichergestellt ist, daß im Verteiler nur der Empfängerkreis berücksichtigt wird, für den die Informationen von unmittelbarem dienstlichen Interesse sind bzw. zu sein haben.

13.3 Unzulässiger Offenbarungszwang bei Erklärungen zum Ortszuschlag

In Einzelfällen hält die Zentrale Bezügestelle des Landes Brandenburg bei der Oberfinanzdirektion Cottbus (ZBB) es für gerechtfertigt, einer/einem Bediensteten zum Ortszuschlag der Stufe 1 vom Unterschiedsbetrag zwischen Stufe 1 und Stufe 2 (sog. Verheiratetenzuschlag) nur noch die Hälfte zu zahlen, wenn sich dieser weigert, nähere Angaben zum Arbeitgeber des Ehepartners zu machen. Dies wäre aber nur gerechtfertigt, wenn die/der Bedienstete nähere Angaben zur Beschäftigungsstelle des Ehepartners verweigern würde, obwohl diese/-r im öffentlichen Dienst tätig ist, weil nur dann auch für diese/-n entsprechende Ansprüche bestehen.

Eine Verpflichtung für Beschäftigte im öffentlichen Dienst, Angaben über eine gleichzeitige Beschäftigung ihres Ehepartners im öffentlichen Dienst zu machen, ergibt sich aus § 40 Bundesbesoldungsgesetz (BBesG)[213] bzw. § 29 BAT-O zu dem Zweck, daß durch eine Vergleichsmitteilung an den anderen öffentlichen Arbeitgeber bzw. die andere Dienstbehörde ermöglicht wird, daß die dann vorgesehene jeweilige Kürzung des Unterschiedsbetrages zwischen Stufe 1 und Stufe 2 des Ortszuschlags auch an der anderen Stelle vorgenommen werden kann.

Die ZBB verweist zwar darauf, daß die Zuordnung zu einer Beschäftigung im öffentlichen Dienst nicht immer leicht sei und somit "erfahrungsgemäß" von vielen Bediensteten falsche Angaben gemacht würden, die in der Folge zu einer Überzahlung der Bezüge führten. Trotz allen Verständnisses, solche problematischen Situationen vermeiden zu wollen, muß ich darauf

[213] i. d. Fass. vom 22. Februar 1996, BGBl. I S. 262

hinweisen, daß mit den materiell-rechtlichen Vorschriften im Bundesbesoldungsgesetz und im BAT-O sich nur eine Verpflichtung zur Abgabe der Angaben rechtfertigen läßt, die für eine Anspruchsänderung tatsächlich von Relevanz sind. Jede darüber hinausgehende Datenerhebung könnte gem. § 4 BbgDSG nur auf freiwilliger Basis erfolgen, wobei zusätzlich zu berücksichtigen wäre, daß es sich bei den erwarteten Angaben um Fremddaten handelt, zu deren Offenbarung der jeweilige Ehepartner seine Einwilligung erteilen müßte.

Solange keine ausreichende materiell-rechtliche Erhebungsbefugnis gegeben ist, bleibt den Personalstellen bzw. der ZBB nur, der ausdrücklichen Versicherung, auch insoweit korrekte Angaben gemacht zu haben, zu vertrauen und vorbereitend in Merkblätter o. ä. zum Erklärungsvordruck die Definitionen für "Öffentlicher Dienst" in § 40 Abs. 6 BBesG bzw. § 29 BAT-O wiederzugeben mit dem Angebot, in Zweifelsfällen bei der korrekten Zuordnung behilflich zu sein.

13.4 "Freiwilligkeit" bei Stellenvergabe

In krasser Weise hatte der Hauptausschuß einer städtischen Gemeinde gegen den Datenschutz verstoßen. Im Zusammenhang mit einer Bewerberauswahl für eine von der Stadt ausgeschriebene Stelle einer Gleichstellungsbeauftragten waren die Bewerberinnen darum gebeten worden, sich damit einverstanden zu erklären, daß ihre Bewerbungsunterlagen an alle Vereine der Stadt weitergegeben werden.

Bei der Bewertung dieses Vorgehens habe ich die Stadt darauf hingewiesen, daß unter den gegebenen Umständen wohl jede sich bewerbende Person - formal - ihre Zustimmung erteilen würde (faktischer Zwang). Da aber das Ansinnen, die Bewerbungsunterlagen an alle Vereine der Stadt herauszugeben, zu der Interessenlage der betroffenen Personen in einem derart krassen Widerspruch steht, kann von einer Freiwilligkeit in keinem Fall mehr ausgegangen werden. Selbst wenn man unterstellt, daß es für die künftige Tätigkeit der einzustellenden Person hilfreich sein könnte, deren Kenntnisse möglichst genau zu kennen, so würden doch die umfassenden Persönlichkeitsdarstellungen auch aller anderen Bewerber den Vereinen bekannt werden. Bedenkt man außerdem, daß die Vereine einer Stadt die Bevölkerung ziemlich umfassend repräsentieren, da viele Menschen mehr als einem Verein angehören und so gut wie in jeder Familie Vereinsmitglieder leben, umfassen statistisch gesehen die Vereine die ganze Stadt. Die Weitergabe der Daten der Bewerberinnen kommt deshalb in etwa der Veröffentlichung dieser Daten in einer Zeitung gleich. Ich habe demzufolge erklärt, daß die Weitergabe der Bewerbungsunterlagen an die Vereine der Stadt aus Gründen des Persönlichkeitsrechts der Betroffenen nicht zulässig sein kann.

13.5 Datenschutz im Personalratsbüro

Der Personalrat, der organisatorisch Teil der Dienststelle ist, besitzt aufgrund seiner Funktion eine eigene Kompetenz, die ihn unabhängig und weisungsfrei macht. Daraus folgt nicht nur, daß er für seine Aufgabenerfüllung gem. §§ 44 und 45 Landespersonalgesetz (PersVGBbg)[214] Anspruch auf Kostenerstattung, räumliche und büromäßige Ausstattung sowie erforderliche zeitliche Befreiungen bzw. Freistellungen hat, sondern auch auf die räumliche und technisch-organisatorische Abschottung von der übrigen Verwaltung.

Da der Personalrat zudem nach § 94 Abs. 3 PersVGBbg im Rahmen der Erforderlichkeit das Recht auf eine eigene

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

Verarbeitung von personenbezogenen Daten hat und nach § 10 PersVG Bbg zur Vertraulichkeit verpflichtet ist, kann es beispielsweise nicht hingenommen werden, daß das Personalratsbüro nicht sicher verschließbar ist.

Bei einer von einem Personalrat selbst erbetenen Prüfung vor Ort, mußte ich feststellen, daß es diesem durch die Gesamtsituation nicht möglich war, seinen Verpflichtungen zur Vertraulichkeit gem. § 10 PersVGBbg im Rahmen seiner eigenständigen Datenverarbeitung nach § 94 Abs. 3 PersVG Bbg nachzukommen. Insbesondere war festzustellen, daß weder das Personalratsbüro verschließbar, noch der Einzel-PC so gesichert war, daß unbefugter Zugriff ausgeschlossen werden konnte. Beides ist nicht hinnehmbar. Ich habe auf Abstellung der Mängel gedrängt und die Anschaffung einer Sicherheitssoftware empfohlen. Abhilfe muß im vorliegenden Fall allerdings die betreffende Amtsverwaltung schaffen.

14 Aus der eigenen Behörde

Gegenstand von Bürgereingaben, die - ebenso wie Behördenanfragen sowie Stellungnahmen zu Regelungsvorhaben - gegenüber den Vorjahren weiterhin zugenommen haben, sind in immer geringerer Anzahl die kleinen Datenschutzprobleme im Zusammenhang mit Adressenhandel, Belästigung durch Werbesendungen, Indiskretionen usw. Im Vordergrund stehen dafür zunehmend eigentliche Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung bei Behörden. Dies läßt allerdings nicht unbedingt den Schluß zu, daß diesbezügliche Mängel zugenommen haben. Gespräche und Schriftwechsel mit Petenten lassen vielmehr darauf schließen, daß von den Bürgern die in einer neuen Rechtsordnung geforderte Selbstverantwortlichkeit und erwartete Eigeninitiative im Verhältnis zu Behörden zunächst eher als eine unliebsame Pflicht gesehen wurde und erst nach und nach auch erkannt wird, daß dies nicht bedeutet, der Willkür behördlichen Handelns ausgesetzt zu sein, sondern im Gegenteil gleichzeitig die Möglichkeit eröffnet ist, die Rechte ordnungsgemäßen behördlichen Handelns und Verhaltens einzufordern.

Möglicherweise konnte ich im Rahmen meiner Informations- und Aufklärungsarbeit zu dieser Entwicklung beitragen. Hier sei in der Wirksamkeit insbesondere die Broschüre "Datenscheckheft" genannt, deren Nachdruck[215] mir aufgrund der immensen Nachfrage so wichtig war, daß ich aus finanziellen Gründen zunächst auf die beabsichtigte Herausgabe anderer Informationsschriften mit Ausnahme der Broschüre "Technisch-organisatorische Aspekte des Datenschutzes"[216] verzichtete. Mit der zuletzt genannten Broschüre hoffe ich insbesondere den in der öffentlichen Verwaltung für die IT-Sicherheit Verantwortlichen und den mit der Verarbeitung personenbezogener Daten betrauten Mitarbeitern eine Orientierungshilfe zur Gewährleistung des Datenschutzes geben zu können.

Meinen Mitarbeiterinnen und Mitarbeitern bin ich dankbar, daß sie sich trotz einiger Umbaumaßnahmen im Dienstgebäude, mit denen unter Ausnutzung der letzten räumlichen Reserven ein weiterer Büroraum geschaffen werden konnte, kaum in ihrem Arbeitseinsatz beeinträchtigen ließen. Ein vorübergehender personeller Engpaß kann durch die befristete Einstellung einer Juristin und eines Juristen in Teilzeitbeschäftigung, die sich erfreulicherweise mit großem Engagement und Einfühlungsvermögen für meine Aufgaben einsetzen, ausgeglichen werden. Meinen Dank an beide verbinde ich mit dem Wunsch, daß sie alsbald eine angemessene dauerhafte Anstellung finden werden, wenn sie meine Behörde zu Beginn des nächsten Berichtszeitraums wieder verlassen müssen.

---

215 s. Broschüre "Datenscheckheft", 2., überarb. Aufl. November 1996 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz informiert"

216 s. Broschüre "Technisch-organisatorische Aspekte des Datenschutzes", 1. Aufl. Oktober 1996 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz informiert"

Trotz der vorübergehenden personellen Schwierigkeiten konnte ich mein Angebot, mich mit meinen Mitarbeiterinnen und Mitarbeitern an den Lehrveranstaltungen des Landesamts für Datenverarbeitung und Datensicherheit zum Thema "Datenschutz und Datensicherheit" zu beteiligen, auch im Berichtsjahr aufrechterhalten. Über die selbstverständlichen Aufklärungsgespräche und Vorträge gelegentlich der Überprüfungen vor Ort hinaus möchte ich beispielsweise zusätzliche Vorträge im Technologiezentrum Cottbus zum Thema "Datenschutz in Weitverkehrsnetzen/Neue Medien und Datensicherheit", bei der "Akademie der 2. Lebenshälfte" in Teltow zum Thema "Die Sicherheit Ihrer persönlichen Daten bei Behörden und Unternehmen", bei der Gesellschaft für Datenschutz und Datensicherung e. V. (ERFA-Kreis Brandenburg) zu aktuellen Fragen des Datenschutzes und auf einem Seminar der Konsil Consult für behördliche Datenschutzbeauftragte von Krankenhäusern im Land Brandenburg zu Problemen des Datenschutzes in Krankenhäusern, hervorheben.

Bedanken möchte ich mich abschließend beim Präsidenten des Landtags Brandenburg und seiner Verwaltung für die unterstützende Mithilfe bei der Lösung personeller und finanzieller Probleme, ohne die mir bei der derzeitigen rechtlichen Einbindung meiner Behörde eine auftragsgerechte Aufgabenerfüllung kaum möglich wäre.

Kleinmachnow, den 12. Mai 1997 Dr. sc. Dietmar Bleyl

Der Landesbeauftragte für den Datenschutz

Rede des Landesbeauftragten für den Datenschutz vor dem Plenum des Landtages Brandenburg am 20. Februar 1997

Sehr geehrter Herr Präsident! Sehr geehrte Damen und Herren Abgeordnete! Unzweifelhaft war das wichtigste Ereignis im Berichtszeitraum die Verabschiedung der EU-Datenschutzrichtlinien. Bis Ende 1998 sind nun die Mitgliedsländer in der Pflicht, diese in nationales Recht umzusetzen, so daß bis dahin europaweit ein Mindeststandard für die Verarbeitung personenbezogener Daten im öffentlichen sowie im nicht-öffentlichen Bereich erreicht sein könnte und verschiedene Länder damit überhaupt erst einmal Datenschutzgesetze schaffen müssen.

Im Ergebnis der Verhandlungen sind leider viele Kompromisse in Form sehr allgemein gehaltener Formulierungen beschlossen worden, weil die auf diesem Gebiet führenden Länder wie z. B. Großbritannien, Frankreich und auch die Bundesrepublik Deutschland selbst nicht bereit waren, neue Wege zu beschreiten, sondern strikt bemüht waren, ihre bisherige nationale Datenschutzphilosophie in der EU-Datenschutzrichtlinie zu verankern. Dadurch haben die Mitgliedsländer sich schließlich auf den kleinsten gemeinsamen Nenner geeinigt. Zum einen reicht dieser jedoch nicht für die dringend benötigte Weiterentwicklung des Datenschutzes unter den Bedingungen der modernen Informationsgesellschaft im Hinblick auf die Datenflüsse aus, die heute ungehindert über Landesgrenzen fließen. Zum anderen steht die Technik insgesamt, soweit sie diese Entwicklung ermöglicht hat, inzwischen zu dem im wesentlichen unverändert gebliebenen Datenschutzrecht in keinem ausgewogenen Verhältnis mehr zueinander. Deshalb haben sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch der Düsseldorfer Kreis als die Gemeinschaft der Aufsichtsbehörden für den Datenschutz im privaten Bereich einen umfangreichen Anforderungskatalog zur demnächst anstehenden Novellierung des Bundesdatenschutzgesetzes erstellt, in dem vor allem auf diese Diskrepanz abgehoben wird und Anforderungen an bestimmte, häufig verwendete Techniksysteme - wie z. B. Chipkarten, Datennetze - aufgezeigt werden. Bedauerlicherweise besteht beim Bundesministerium des Innern wenig Neigung, diesen Vorschlägen zu folgen.

Aber auch die Landesdatenschutzgesetze müssen an die EU- Datenschutzrichtlinie angepaßt werden. Sofern bei der Datenschutzaufsicht übertriebener Bürokratismus bei den Meldepflichten über automatisierte Datenverarbeitung vermieden werden soll, wird es beispielsweise gem. Art. 18 erforderlich sein, zumindest vom Grundsatz her bei allen öffentlichen Stellen die Berufung behördlicher Datenschutzbeauftragten gesetzlich vorzuschreiben. Ausgehend von den guten Erfahrungen in Brandenburg mit behördlichen Datenschutzbeauftragten dürfte letzterem der Vorzug zu geben sein.

In ihrer Stellungnahme zum Tätigkeitsbericht hat die Landesregierung zum Thema "Neue Technologien" irritierende Aussagen gemacht. Einerseits bedankt sie sich für Hinweise, die sie zu Datenschutzproblemen in den neuen Medien erhalten habe, andererseits sieht sie nur eine mittelbare Zuständigkeit meiner Behörde für neue Technologien. Dabei müßte doch Einvernehmen darüber bestehen, daß vorhandene Technologien, sofern sie für die Einführung eines bestimmten Zwecks für geeignet angesehen werden, heute oder morgen auch zur Wahrnehmung staatlicher Aufgaben eingesetzt werden.

Die Chipkartenproblematik belegt dies eindringlich. Zu dem bisher einzig gesetzlich geregelten Fall des Einsatzes von Chipkarten, nämlich der Krankenversichertenkarte, sind inzwischen neben der Wahrnehmung hoheitlicher Aufgaben auch Nutzungen im Bereich der Daseinvorsorge, also staatlichen Aufgaben, bekannt geworden. So gibt es nach meiner Information inzwischen die sog. Norderney-Card in Verbindung mit Kuraufenthalten und den Beschluß des

Abgeordnetenhauses von Berlin über eine Mobilitätskarte, genannt Chipticket, für den Verkehrsverbund Berlin-Brandenburg.

Die Datenschutzbeauftragten haben diese sowie andere Entwicklungen des Technikeinsatzes bei der Verarbeitung personenbezogener Daten seit längerem vorausgesehen und schätzen ein, daß sie in Zukunft nur ihre von Gesetzes wegen wahrzunehmenden Aufgaben nachkommen können, wenn sie zusätzlich zu ihren bisherigen Aufgaben auch auf die künftige Technikgestaltung Einfluß nehmen, soweit diese die Verarbeitung personenbezogener Daten betrifft. Dabei ist es die Zielvorstellung der Datenschutzbeauftragten, Grundanforderungen an den Einsatz von bestimmten Techniken aufzustellen. Damit soll verhindert werden, daß eine von jedem Freak leicht zu fälschende Chipkartentechnik, wie bei der Krankenversichertenkarte, künftig nicht mehr zum Einsatz gelangt. Dieser Paradigmenwechsel dürfte eine der entscheidenden, zukunftsträchtigen Herausforderungen an die Datenschutzbeauftragten darstellen.

Ich danke Ihnen für Ihre Aufmerksamkeit.

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 29. April 1996

Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. Anonyme bzw. datensparsame Nutzung: Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z.B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. Bestandsdaten: Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte

dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. Verbindungs- und Abrechnungsdaten: Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. Interaktionsdaten: Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z. B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. Einwilligung: Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten auf Grund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer: Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur auf Grund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z. B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. Rechte von Betroffenen: Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. Datenschutzkontrolle: Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. Geltungsbereich: Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. Internationale Datenschutzregelung: Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Mai 1996

Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z. B. § 78a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996 in Hamburg

Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996 in Hamburg

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Femsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996 in Hamburg

Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kasssenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch.
§ 295 SGB V fordert, daß Daten nur **im erforderlichen Umfang** und **nicht versichertenbezogen** übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in "Protokollnotizen" - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich für die Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung werden dadurch nicht berührt.

Kurzbericht
zum "Datenschutz durch Technik"
für die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 22./23. Oktober 1996 in Hamburg

Datensparsamkeit durch moderne Informationstechnik
- Datenvermeidung, Anonymisierung und Pseudonymisierung -

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip **"Datenschutz durch Technik"** umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen Datenschutzbeauftragten und des Datenschutzbeauftragten von Ontario/Kanada zum sogenannten **Identity Protector** beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto "Datenschutz durch Technik - Technik im Dienste der Grundrechte" Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte, sind bereits seit längerer Zeit allgemein akzeptiert. Erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind im Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag enthalten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Neben der Entwicklung entsprechender Hard- und Software werden Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um die technische Entwicklung berücksichtigen zu können. Auch Vertreter der Wirtschaft als Entwickler und Anwender werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Datenschutz und Telefax

I. Konventionelle Telefaxgeräte

Telefaxgeräte sind datenverarbeitende Geräte, mit denen auch personenbezogene Daten automatisiert übertragen werden können. Sie werden eingesetzt, um bei einfacher Handhabung schnell Informationen zu übermitteln. Das Telefax ist nach dem Telefon inzwischen zum wichtigsten Kommunikationsverfahren geworden. Nicht alle Nutzer von Telefaxgeräten sind sich darüber im klaren, welche Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen bestehen.

Die besonderen Gefahren sind:

- Die Informationen werden grundsätzlich "offen" (unverschlüsselt) übertragen, und der Empfänger erhält sie - vergleichbar mit einer Postkarte - in unverschlossener Form.

- Der Telefaxverkehr ist wie ein Telefongespräch abhörbar.

- Die Adressierung erfolgt durch eine Zahlenfolge (Telefaxnummer) und nicht durch eine mehrgliedrige Anschrift. Dadurch sind Adressierungsfehler wahrscheinlicher, und Übertragungen an den falschen Adressaten werden nicht oder erst nachträglich bemerkt.

- Bei Telefaxgeräten neueren Typs kann der Hersteller Fernwartungen durchführen, ohne daß der Besitzer diesen Zugriff wahrnimmt. Unter bestimmten Umständen kann er dabei auf die im Telefaxgerät gespeicherten Daten zugreifen (z. B. Lesen der Seitenspeicher sowie Lesen und Beschreiben der Rufnummern- und Parmeterspeicher).

Diese Gefahren werden von Anbietern der Telekommunikationsnetze und -dienste nicht abgefangen. Deshalb ist insbesondere die absendende Stelle für die ordnungsgemäße Übertragung und die richtige Einstellung der technischen Parameter am Telefaxgerät verantwortlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit den Risiken vertraulicher Kommunikation beim Einsatz von Telefaxgeräten befaßt. Sie geben die folgenden Empfehlungen, um den datenschutzgerechten Umgang mit Telefaxgeräten weitgehend zu gewährleisten:

1. Aufgrund der gegebenen Gefährdungen darf die Übertragung sensibler personenbezogener Daten per Telefax nicht zum Regelfall werden, sondern darf nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.

2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt wird, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z. B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für sensible, personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial,- Steuer-, Personal- und medizinische Daten).

3. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich zu hier genannten Maßnahmen mit dem Empfänger ein Sendezeitpunkt abzustimmen, damit Unbefugte keinen Einblick nehmen können. So kann auch eine Fehlleitung durch z. B. veraltete Anschlußnummern oder beim Empfänger aktivierte Anrufumleitungen

bzw. -weiterleitungen vermieden werden.

4. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

5. Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.

6. Alle vom Gerät angebotenen Sicherheitsmaßnehmen (z. B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Paßwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.

7. Die vom Gerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wahlfehlern die Übertragung unverzüglich abgebrochen werden kann.

8. Bei Telefaxgeräten, die an Nebenstellenanlagen angeschlossen sind, ist das Risiko einer Fehladressierung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten.

9. Die Dokumentationspflichten müssen eingehalten werden (z. B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren). Sende- und Empfangsprotokolle sind vertraulich anzulegen, da sie dem Fernmeldegeheimnis unterliegen.

10. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, daß alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

11. Die am Telefax eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

12. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer deaktiviert werden. Nur für notwendige Wartungsarbeiten ist diese Funktion freizugeben. Nach Abschluß der Wartungsarbeiten sollten die eingestellten Parameter und Speicherinhalte kontrolliert werden.

II. Telefax in Bürokommunikationslösungen

Rechner mit Standard- oder Bürokommunikationssoftware können um Hard- und Softwarekomponenten erweitert werden, mit deren Hilfe Telefaxe gesendet und empfangen werden können (integrierte Telefaxlösungen). Lösungen für den Faxbetrieb werden sowohl für Einzelplatzrechner als auch für Rechnernetze angeboten.

Der Betrieb (Installation, Konfiguration, Bedienung und Wartung) integrierter Telefaxlösungen birgt gegenüber dem konventionellen Telefaxgerät zusätzliche Gefahren, da beispielsweise die verwendeten Faxmodems bzw. -karten oft nicht nur für Telefaxsendung und -empfang geeignet sind, sondern auch andere Formen der Datenübertragung und des Zugriffs ermöglichen.

Daher sollten die folgenden Empfehlungen beim Umgang mit integrierten Telefaxlösungen zusätzlich zu den bereits genannten beachtet werden.

1. Das verwendete Rechnersystem muß sorgfältig konfiguriert und gesichert sein. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösung. Dazu gehört unter anderem, daß kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.

2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlußlisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu benutzen.

3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösungen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlußlisten und Protokolle.

4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen unkompliziert und kostengünstig möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sollten personenbezogene Daten immer verschlüsselt und digital signiert übertragen werden, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.

5. Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, daß ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzers zu gewährleisten.

Orientierungshilfe

Forderung an Wartung und Fernwartung

AK Technik, Stand: März 1993

Grundsätzliches

Die speichernde Stelle ist für alle Daten und Verfahren selbst verantwortlich. Sie hat dafür Sorge zu tragen, daß der einzelne davor geschützt wird, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Die speichernde Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, Datenschutz und Datensicherheit zu gewährleisten.

Hersteller von DV-Anlagen, externe Software-Ersteller und Wartungsfirmen dürfen daher nur auf konkrete Weisung der speichernden Stelle tätig werden. Art und Umfang dieser Service-Tätigkeit bestimmt stets die speichernde Stelle. Sie unterscheidet, ob und in welcher Weise Dritte auf dem DV-System tätig werden können. In einem solchen Falle legt die speichernde Stelle schriftlich fest, daß die Wartungsarbeiten möglichst ohne Kenntnisnahme personenbezogener Daten durchgeführt werden. Ist dies nicht möglich,

- ist die Kenntnisnahme personenbezogener Daten externen Dritten nach vorheriger Risikoabschätzung nur in dem Umfang erlaubt, wie dies für die konkreten Arbeiten im Einzelfall unerläßlich ist,

- kann das Zugänglichmachen personenbezogener Daten nur in besonderen Ausnahmefällen erfolgen, wobei die offenbarten Daten einer strengen Zweckbindung unterliegen und eine Weitergabe an Dritte untersagt ist.

Die speichernde Stelle hat technisch und organisatorisch sicherzustellen, daß eine Wartung oder Fernwartung (Fernbetreuung) nur mit ihrem Einverständnis und im Einzelfall erfolgen kann.

Die speichernde Stelle hat ferner sicherzustellen, daß sie kontrollieren kann, was bei einer Wartung oder Fernwartung im einzelnen geschieht, insbesondere, welche Zugriffe auf personenbezogene Daten erfolgen. Bei Systemen mit sensiblen personenbezogenen Daten hat sie diese Kontrolle in jedem Einzelfall durchzuführen. Das hat jedoch zur Folge, daß eigenes Personal vorhanden und entsprechend geschult ist, um diese Aufgabe zuverlässig erledigen zu können.

Schließlich muß die Fernwartungszentrale angemessene technische, organisatorische und personelle Sicherheitsanforderungen erfüllen.

Sicherheitsmaßnahmen für Wartung und Fernwartung:

Maßnahmen zur Zugangskontrolle

Die Personen, die die Wartungsarbeiten an der DV-Anlage durchführen, müssen sich den gleichen strengen Zugangskontrollprüfungen unterziehen wie das eigene Personal.

Bei der Fernwartung muß der Verbindungsaufbau stets durch den Kunden erfolgen, so daß Wartungsarbeiten nur mit Wissen und Willen des Kunden beginnen können.

Der Kreis des autorisierten Wartungspersonals ist festzulegen; ohne genaue Identifikation dürfen keine Wartungsarbeiten beginnen.

Der Kunde muß das Wartungspersonal als autorisiert identifizieren können.

Um zu verhindern, daß ein unbefugter Teilnehmer Zugriff auf das DV-System erhält, ist die Verbindung vom DV-System aus aufzubauen. Die Anschlußnummern der zulässigen Partner, einschließlich Fernwartungszentrale, sind einzuprogrammieren, so daß ein Anwählen einer anderen Nummer unmöglich wird.

Der Kunde muß die Fernwartungsarbeiten jederzeit abbrechen können.

Organisation der Datenträgerkontrolle

Bevor ein Datenträger mit Kundendaten den DV-Bereich zu Wartungszwecken oder zur Fehleranalyse verläßt, ist die Genehmigung einer vom Kunden dafür autorisierten Person einzuholen. Auf einem Begleitschein sind die Art der Daten und des Datenträgers zu vermerken. Für die Rücklaufkontrolle muß eine Kopie beim Kunden verbleiben.

Wenn personenbezogene Daten an die Fernwartungszentrale übertragen werden müssen, ist vorher die Erlaubnis durch eine vom Kunden autorisierte Person einzuholen.

Die Übertragung von Daten aus dem DV-System des Kunden an die Fernwartungszentrale ist nur bei gleichzeitiger Protokollierung der übertragenen Daten zuzulassen.

Die Kontrolle der protokollierten Daten ist DV-technisch durch geeignete Kommandos oder Dienstprogramme zu unterstützen.

Es ist sicherzustellen, daß das Wartungspersonal nicht mit den eigenen mitgebrachten Datenträgern die Wartung durchführt, sondern ausschließlich mit Duplikaten arbeitet, die an der DV-Anlage des Kunden zu erstellen und dort dann für Kontrollzwecke für einen bestimmten Zeitraum (in der Regel ein Jahr) aufzubewahren sind.

Es ist darauf zu achten, daß Wartungstechniker keine am DV-System benützten Datenträger ungelöscht mitnehmen.

Alle Wartungs- und Übertragungsaktivitäten müssen an der Kundenkonsole zum Mitlesen sichtbar gemacht werden.

Maßnahmen zur Speicherkontrolle

Der Betreiber der DV-Anlage muß alle Programme durch Paßworte schützen, soweit diese bei der Wartung physisch im Zugriff bleiben.

Das Wartungspersonal muß sich einer Anmeldeprozedur unterwerfen. Diese muß aus einer Identifikation

(Benutzerkennung) und einer Authentifikation (Paßwort) bestehen. Die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalterprivilegien einschließt.

Werden Test- und Service-Programme des Herstellers auf der DV-Anlage gespeichert, sind diese unter der Wartungskennung abzuspeichern.

Der Zugriffsschutz muß hinreichend differenziert sein.

Ist für Wartungszwecke ein Zugriff auf Kundendaten erforderlich, ist zu prüfen, ob sensible personenbezogene Kundendaten aus dem direkten Zugriff zu entfernen sind. Im Rahmen der Fernwartung ist der Zugriff auf Kundendaten grundsätzlich zu verhindern. Dabei ist denkbar, die Laufwerke, auf denen diese Daten gespeichert werden, vom DV-System physikalisch abzutrennen, soweit dies technisch möglich ist.

Ein Einspielen von Änderungen ins Betriebssystem, in systemnahe Software oder Anwendungsfremdsoftware im Rahmen der Fernwartung ist nicht zuzulassen. Die Änderungen sind ausschließlich vor Ort entweder vom Kunden selbst oder nach Freigabe durch eine vom Kunden dafür autorisierte Person vom Software-Hersteller in die entsprechende Software zu übernehmen. Dasselbe gilt für die Fehlerbehebung.

Wartungs- und Diagnosearbeiten im laufendem Betrieb, insbesondere, wenn sie die Software betreffen, sind unter ständiger Kontrolle eines sachkundigen Kundenmitarbeiters durchzuführen.

Es muß ausgeschlossen werden, daß vom Kunden erstellte Software und Kundendateien durch die Wartung verändert werden können.

Es ist auszuschließen, daß Anwendungsprogramme durch die Fernwartung aktiviert werden können, solange Kundendateien im direkten Zugriff stehen.

Maßnahmen zur Zugriffskontrolle

Für den Fall, daß in einem Wartungsvorgang ein Zugriff auf Dateien mit Kundendaten notwendig ist, sind nach Abschluß der Wartungsarbeiten die der Wartung offenbarten Paßworte unverzüglich zu ändern.

Alle Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festgehalten werden, sind zu überprüfen und zur Beweissicherung mindestens ein Jahr aufzubewahren. Die Verpflichtung des beim Kunden für das DV-System Verantwortlichen, den Wartungsvorgang am Bildschirm zu verfolgen und gegebenfalls zu unterbrechen, bleibt davon unberührt.

Maßnahmen zur Transportkontrolle

Beim Transport von Datenträgern sind der Transportweg und die am Transport beteiligten Personen festzulegen.

Es ist zu prüfen, ob beim Versand von Datenträgern für Wartungszwecke die Versandart angemessen und ausreichend ist.

Die Vollständigkeit der Unterlagen ist zu prüfen. Der Transport muß ausschließlich mit Begleitpapieren erfolgen.

Maßnahmen zur Organisationskontrolle

Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Kundenpersonal zu treffen. Art und Umfang der Wartung (Hard- und Software) sind schriftlich festzulegen.

Das Wartungspersonal ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten.

Eine Weitergabe von Daten, die dem Wartungspersonal übergeben oder bei der Fernwartung übertragen wurden, an Dritte ist vertraglich zu untersagen. Diese Daten sind ausschließlich für Zwecke der Wartung zu verwenden und nach Abschluß der Wartungsarbeiten oder der Fehlersuche unverzüglich zu löschen. Für eventuell weitergegebene Listen mit personenbezogenen Daten ist eine Rückgabe nach Abschluß der Wartungsarbeiten zu vereinbaren.

Hinsichtlich der Fernwartung wird empfohlen, einen separaten Vertrag abzuschließen, in dem Sicherheitsmaßnahmen festgelegt werden und die Kontrolle der Einhaltung aller Maßnahmen geregelt wird.

Zur DV-Revision ist der Betreiber der DV-Anlage gehalten, das Wartungs- bzw. Fernwartungskonzept schriftlich zu dokumentieren.

Die Systemverantwortlichen beim Kunden sind regelmäßig bezüglich der Möglichkeiten der Fernwartung zu schulen.

Die Einhaltung der getroffenen Sicherheitsmaßnahmen ist regelmäßig zu überprüfen.

Datenschutz und Privatsphäre im Internet
(Budapest - Berlin Memorandum)

(verabschiedet bei der 20. Sitzung der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation in Berlin am 19. November 1996 auf der Basis der Diskussionen der Arbeitsgruppe in Budapest am 15. und 16. April 1996)

- Übersetzung -

Zusammenfassung

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz von Benutzern des Internet gegenwärtig unzureichend ist.

In diesem Dokument werden zehn Prinzipien zur Verbesserung des Datenschutzes im Internet beschrieben:

1. Die Diensteanbieter sollten jeden Benutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationales Datenschutzrecht geregelt. Dies bedeutet z.B. daß personenbezogene Daten nur auf eine nachvollziehbare Art und Weise gespeichert werden dürfen. Medizinische und andere besonders sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den an das Internet angeschlossenen Computern gespeichert werden. Polizeiliche Steckbriefe und Fahndungsaufrufe sollten nicht im Internet veröffentlicht werden.

3. Initiativen für eine engere internationale Zusammenarbeit, ja sogar für eine internationale Konvention, die den Datenschutz im Zusammenhang mit grenzüberschreitenden Computernetzen und Diensten regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen.

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden. Insbesondere die Nutzung

sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von "Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten "Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

Bericht

Das Internet ist gegenwärtig das größte internationale Computernetz der Welt. In mehr als 140 Ländern gibt es "Auffahrten" zu dieser "Datenautobahn". Das Internet besteht aus mehr als vier Millionen angeschlossenen Rechnern ("hosts"); mehr als 40 Millionen Benutzer aus aller Welt können wenigstens einen der verschiedenen Internet-Dienste nutzen und haben die Möglichkeit, miteinander durch elektronische Post zu kommunizieren. Die Benutzer haben Zugriff auf einen immensen Informationsbestand, der an verschiedenen Orten in aller Welt gespeichert wird. Das Internet kann als erste Stufe der sich entwickelnden Globalen Informationsinfrastruktur (GII) bezeichnet werden. Das World Wide Web bildet als die modernste Benutzeroberfläche im Internet eine Basis für neue interaktive Multimedia-Dienste. Die Internet-Protokolle werden zunehmend auch für die Kommunikation innerhalb großer Unternehmen genutzt ("Intranet").

Die Teilnehmer am Internet haben unterschiedliche Aufgaben, Interessen und Möglichkeiten:

- Die Software-, Computer- und Telekommunikationsindustrien erstellen die Kommunikationsnetze und die angebotenen Dienste.

- Telekommunikationsorganisationen wie die nationalen Telekommunikationsunternehmen stellen die Basisnetze für die Datenübertragung zur Verfügung (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen).

- Dienstleistungsunternehmen stellen Basisdienste für die Speicherung, Übertragung und Darstellung von Daten zur Verfügung. Sie sind für den Datentransport im Internet verantwortlich (routing, delivery) und verarbeiten Verbindungsdaten.

- Informationsanbieter stellen den Benutzern in Dateien und Datenbanken gespeicherte Informationen zur Verfügung.

- Die Benutzer greifen auf die verschiedenen Internet-Dienste (elektronische Post, news, Informationsdienste) zu und

nutzen das Netz sowohl zur Unterhaltung als auch für Teleshopping, Telearbeit, Fernunterricht und Telemedizin.

I. Probleme und Risiken

Anders als bei der traditionellen Verarbeitung personenbezogener Daten, bei der normalerweise eine einzelne Behörde oder ein Unternehmen für den Schutz der personenbezogenen Daten ihrer Kunden verantwortlich ist, ist im Internet eine solche Gesamtverantwortung keiner bestimmten Einrichtung zugewiesen. Darüber hinaus gibt es keinen internationalen Kontrollmechanismus zur Erzwingung der Einhaltung gesetzlicher Verpflichtungen, soweit diese existieren. Der Benutzer muß daher Vertrauen in die Sicherheit des gesamten Netzes setzen, das bedeutet in jeden einzelnen Bestandteil des Netzes, unabhängig davon, wo dieser angesiedelt ist oder von wem er verwaltet wird. Die Vertrauenswürdigkeit des Netzes wird durch die Einführung neuer Software, bei deren Nutzung Programme aus dem Netz geladen werden und die mit einer Verschlechterung der Kontrolle der auf dem Rechner des Benutzers gespeicherten personenbezogenen Daten verbunden ist, sogar noch wichtiger werden.

Die schnelle Ausbreitung des Internet und seine zunehmende Nutzung für kommerzielle und private Zwecke führen zur Entstehung schwerwiegender Datenschutzprobleme:

- Das Internet ermöglicht die schnelle Übertragung großer Informationsmengen auf beliebige andere an das Netzwerk angeschlossene Computersysteme. Sensible personenbezogene Daten können in Länder übertragen werden, die nicht über ein angemessenes Datenschutzniveau verfügen. Informationsanbieter könnten personenbezogene Daten auf Rechnern in Ländern ohne jegliche Datenschutzgesetzgebung anbieten, auf die aus aller Welt durch einen einfachen Mausklick zugegriffen werden kann.

- Personenbezogene Daten können über Länder ohne jegliche oder ohne hinreichende Datenschutzgesetzgebung geleitet werden. Im Internet, das ursprünglich für akademische Zwecke eingerichtet wurde, ist die Vertraulichkeit der Kommunikation nicht sichergestellt.

  Es gibt keine zentrale Vermittlungsstelle oder sonstige verantwortliche Einrichtung, die das gesamte Netz kontrolliert. Damit ist die Verantwortung für Datenschutz und Datensicherheit auf Millionen von Anbietern verteilt. Eine übertragene Nachricht könnte an jedem Computersystem, das sie passiert, abgehört und zurückverfolgt, verändert, gefälscht, unterdrückt oder verzögert werden. Trotzdem nimmt die Nutzung des Internet für Geschäftszwecke exponentiell zu, und personenbezogene und andere sensible Daten (Kreditkarten-Informationen und Gesundheitsdaten) werden über das Internet übertragen.

- Bei der Nutzung von Internet-Diensten wird weder eine angemessene Anonymität noch eine angemessene Authentifizierung sichergestellt. Computernetzwerk-Protokolle und viele Internet-Dienste arbeiten in der Regel mit dedizierten (Punkt-zu-Punkt-)Verbindungen. Zusätzlich zu den Inhaltsdaten wird dabei die Identität (ID) von Sender und Empfänger übertragen. Jeder elektronische Brief enthält einen "header" mit Informationen über Sender und Empfänger (Name und IP-Nummer, Name des Rechners, Zeitpunkt der Übertragung). Der "header" enthält weitere Informationen über den Übertragungsweg und den Inhalt der Nachricht. Er kann auch Hinweise auf Publikationen anderer Autoren enthalten. Die Benutzer sind gezwungen, eine elektronische Spur zu hinterlassen, die zur Erstellung eines Benutzerprofils über persönliche Interessen und Vorlieben verwendet werden kann. Obwohl es keinen zentralen Abrechnungsmechanismus für Zugriffe auf news oder das World Wide Web gibt, kann das Informationsgebaren von Sendern und Empfängern zumindest von dem Dienstleistungsunternehmen, an das der

Benutzer angeschlossen ist, verfolgt und überwacht werden.

- Andererseits sind die unzureichenden Identifizierungs- und Authentifizierungsprozeduren im Internet bereits dazu benutzt worden, in unzureichend geschützte Computersysteme einzudringen, auf dort gespeicherte Informationen zuzugreifen und diese zu verändern oder zu löschen. Das Fehlen einer sicheren Authentifikation könnte auch genutzt werden, um auf kommerzielle Dienste auf Kosten eines anderen Benutzers zuzugreifen.

- Es gibt im Internet Tausende von speziellen news-groups, von denen die meisten jedem Nutzer offenstehen. Die Artikel können personenbezogene Daten von Dritten enthalten, die gleichzeitig auf vielen tausend Computersystemen gespeichert werden, ohne daß der Einzelne eine Möglichkeit hat, dagegen vorzugehen.

Die Teilnehmer am Internet haben ein gemeinsames Interesse an der Integrität und Vertraulichkeit der übertragenen Information: Die Benutzer sind an verläßlichen Diensten interessiert und erwarten, daß ihre personenbezogenen Daten geschützt werden. In bestimmten Fällen können sie ein Interesse daran haben, Dienste ohne Identifizierung benutzen zu können. Den Benutzern ist es normalerweise nicht bewußt, daß sie beim "Surfen" im Netz einen globalen Marktplatz betreten und daß jeder einzelne Schritt dort überwacht werden kann.

Andererseits sind viele Diensteanbieter an der Identifizierung und Authentifizierung von Benutzern interessiert: Sie benötigen personenbezogene Daten für die Abrechnung, könnten diese Daten aber auch für andere Zwecke nutzen. Je mehr das Internet für kommerzielle Zwecke genutzt wird, desto interessanter wird es für Diensteanbieter und andere Einrichtungen sein, so viele Verbindungsdaten über das Nutzerverhalten im Netz wie möglich zu speichern und damit das Risiko für den Datenschutz der Kunden zu verstärken. Unternehmen bieten in zunehmendem Maße freien Zugang zum Internet an, um sicherzustellen, daß die Kunden ihre Werbeanzeigen lesen, die zu einer der hauptsächlichen Finanzierungsquellen des gesamten Internets werden. Die Unternehmen wollen nachvollziehen können, in welchem Ausmaß, von wem und wie oft ihre Werbeanzeigen gelesen werden.

Im Hinblick auf die erwähnten Risiken kommt den Einrichtungen, die das Netz auf internationaler, regionaler und nationaler Ebene verwalten, insbesondere bei der Entwicklung der Protokolle und Standards für das Internet, bei der Festlegung der Regeln für die Identifikation der angeschlossenen Server und schließlich bei der Identifikation der Benutzer eine wichtige Funktion zu.

II. Vorhandene Regelungen und Empfehlungen

Obwohl verschiedene nationale Regierungen und internationale Organisationen (z. B. die Europäische Union) Programme gestartet haben, um die Entwicklung von Computernetzen und -diensten zu erleichtern und zu intensivieren, sind dabei nur sehr geringe Anstrengungen unternommen worden, um für ausreichende Datenschutz- und Datensicherheitsregelungen zu sorgen. Einige nationale Datenschutzbehörden haben bereits Empfehlungen für die technische Sicherheit von an das Internet angeschlossenen Computernetzen und über Datenschutzrisiken für die einzelnen Benutzer von Internet-Diensten herausgegeben. Solche Empfehlungen sind z. B. in Frankreich, Großbritannien (vgl. den 11. Jahresbericht des Data Protection Registrar, Anhang 6) und in Deutschland erarbeitet worden. Die wesentlichen Punkte können wie folgt zusammengefaßt werden:

- Das Anbieten von Informationen auf dem Internet fällt in den Regelungsbereich der nationalen Datenschutzgesetze und -regelungen. In dieser Hinsicht ist das Internet nicht so ungeregelt, wie oft behauptet wird. Es ist, um nur ein

Beispiel zu nennen, einem deutschen Anbieter eines WorldWideWebServers verboten, ohne Wissen des Benutzers die vollständigen Angaben über den auf ihr Angebot zugreifenden Rechner, die abgerufenen Seiten und heruntergeladene Dateien zu speichern (wie es im Netz allgemein praktiziert wird). Nationale Regelungen können eine Verpflichtung für Informationsanbieter enthalten, sich bei einer nationalen Datenschutzbehörde anzumelden. Nationale Gesetze enthalten darüber hinaus spezielle Regelungen im Hinblick auf internationales Straf-, Privat- und Verwaltungsrecht (Kollisionsrecht), die unter bestimmten Umständen Lösungen bereitstellen können.

- Bevor ein lokales Computernetz - z. B. das einer Behörde - an das Internet angeschlossen wird, müssen die Risiken für das lokale Netzwerk und die darauf gespeicherten Daten im Einklang mit dem nationalen Recht abgeschätzt werden. Dazu kann die Erarbeitung eines Sicherheitskonzepts und einer Abschätzung, ob es erforderlich ist, das gesamte Netz oder nur Teile davon an das Internet anzuschließen, gehören. Abhängig von dem verfolgten Zweck kann es sogar ausreichend sein, nur ein Einzelplatzsystem an das Netz anzuschließen. Es sollten technische Maßnahmen getroffen werden, um sicherzustellen, daß auf dem Internet nur auf Daten, die veröffentlicht werden könnten, zugegriffen werden kann, z. B. durch Einrichtung eines Firewall-Systems, das das lokale Netzwerk vom Internet trennt. Es muß jedoch festgestellt werden, daß der Anschluß eines Computernetzwerks an das Internet eine Erhöhung des Sicherheitsrisikos auch dann bedeutet, wenn solche technischen Maßnahmen getroffen worden sind.

- Falls personenbezogene Daten von Nutzern eines bestimmten Dienstes gespeichert werden, muß für die Benutzer klar sein, wer diese Daten nutzen wird und zu welchen Zwecken die Daten genutzt oder übermittelt werden sollen. Dies bedeutet eine Information am Bildschirm vor der Übermittlung und die Schaffung einer Möglichkeit, die Übermittlung zu unterbinden. Der Benutzer sollte in der Lage sein, diese Unterrichtung und aller übrigen Bedingungen, die durch den Diensteanbieter gestellt werden, auszudrucken.

- Wenn der Zugang zu personenbezogenen Daten auf einem Computersystem bereitgestellt wird - z. B. durch die Veröffentlichung biographischer Angaben über Mitarbeiter in einem Verzeichnis - muß der Informationsanbieter sicherstellen, daß diese Personen sich der globalen Natur des Zugriffs bewußt sind. Am sichersten ist es, die Daten nur mit der informierten Einwilligung der betroffenen Person zu veröffentlichen.

Darüber hinaus gibt es eine Reihe von internationalen gesetzlichen Bestimmungen und Konventionen, die u. a. auch auf das Internet anwendbar sind:

- Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, verabschiedet vom Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) am 23. September 1980

- Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981

- Richtlinien betreffend personenbezogene Daten in automatisierten Dateien, von der Generalversammlung der Vereinten Nationen verabschiedet am 4. Dezember 1990

- Richtlinie des Rates der Europäischen Gemeinschaften 90/387/EWG vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network

Provision - ONP) (in der Datenschutz als "grundlegende Anforderung" definiert wird)

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie)

- Allgemeines Abkommen über Handel und Dienstleistungen (GATS) (das in Artikel XIV regelt, daß die Mitgliedstaaten durch das weltweite Abkommen nicht daran gehindert werden, Regelungen über den Datenschutz von Einzelpersonen im Zusammenhang mit der Verarbeitung und Verbreitung von personenbezogenen Daten und dem Schutz der Vertraulichkeit von Akten und Aufzeichnungen über Einzelpersonen zu erlassen oder durchzusetzen).

Die Richtlinie der Europäischen Union enthält als erstes supra-nationales Gesetzeswerk eine wichtige Neudefinition des Begriffs "für die Verarbeitung Verantwortlicher", die im Zusammenhang mit dem Internet von Bedeutung ist. Artikel 2 Buchstabe c) definiert den "für die Verarbeitung Verantwortlichen" als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Wenn man diese Definition auf die Nutzung des Internet für die Zwecke der Übermittlung elektronischer Post anwendet, muß der Absender einer elektronischen Nachricht als "für die Verarbeitung Verantwortlicher" dieser Nachricht angesehen werden, wenn er eine Datei mit personenbezogenen Daten absendet, da er die Zwecke und Mittel der Verarbeitung und Übermittlung dieser Daten bestimmt. Andererseits bestimmt der Anbieter eines Mailbox-Dienstes selbst die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Betrieb des Mailbox-Dienstes und hat damit wenigstens eine Mitverantwortung für die Einhaltung der anwendbaren Regelungen über den Datenschutz.

Kürzlich hat die Europäische Kommission zwei Dokumente veröffentlicht, die zu einer europäischen Gesetzgebung führen könnten und in diesem Fall beträchtliche Auswirkungen auf den Datenschutz im Internet haben werden:

- Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über illegale und schädigende Inhalte im Internet (KOM(96) 487)

und

- Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten (KOM(96) 483).

Obwohl auch diese nicht rechtlich bindend und eher auf einer nationalen denn auf einer internationalen Ebene verabschiedet worden sind, sollten die

- Grundsätze für die Bereitstellung und Nutzung personenbezogener Daten
  "Privacy und die nationale Informations-Infrastruktur"
  verabschiedet von der Privacy Working Group des Information Policy Committee innerhalb der Information Infrastructure Task Force (IITF) am 6. Juni 1995

genannt werden, da sie einen Einfluß auf die internationalen Datenflüsse haben werden. Sie sind intensiv und fruchtbar mit der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation bei einem gemeinsamen Treffen in Washington D. C. am 28. April 1995 diskutiert worden.

In der Praxis werden einige wichtige und effektive Regeln zur Selbstregulierung von der Netzgemeinde selbst aufgestellt (z. B. "Netiquette"). Solche Maßnahmen dürfen im Hinblick auf die Rolle, die sie gegenwärtig und zukünftig für den Datenschutz des einzelnen Benutzers spielen können, nicht unterschätzt werden. Sie tragen mindestens dazu bei, die nötige Aufmerksamkeit unter den Benutzern dafür zu schaffen, daß Vertraulichkeit als eine Grundanforderung auf dem Netz nicht existiert ("Sende oder speichere niemals etwas in Deiner Mailbox, das Du nicht in den Abendnachrichten sehen möchtest"). Die EU-Datenschutzrichtlinie wiederum fordert Verhaltensregeln (Artikel 27), die von den Mitgliedstaaten und der Kommission gefördert werden sollen.

III. Empfehlungen

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz im Internet im Augenblick unzureichend ist.

Das Recht jedes Einzelnen, die Datenautobahn zu benutzen, ohne überwacht und identifiziert zu werden, sollte garantiert werden. Andererseits muß es im Hinblick auf die Nutzung personenbezogener Daten auf der Datenautobahn (z. B. von Dritten) Grenzen geben ("Leitplanken").

Eine Lösung für dieses Grunddilemma muß auf folgenden Ebenen gefunden werden:

1. Die Diensteanbieter sollten jeden potentiellen Nutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. Da "sowohl die einzelnen Teile der Netzwerk-Infrastruktur als auch die Benutzer jeder einen physikalischen Standort haben, können Staaten einen bestimmten Grad von Verläßlichkeit in bezug auf die Netze und ihre Teilnehmer verhängen und durchsetzen" (Joel Reidenberg). In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationale Datenschutzgesetze geregelt.

   Personenbezogene Daten dürfen nur in einer nachvollziehbaren Art und Weise gespeichert werden. Medizinische und andere sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den am Internet angeschlossenen Computern gespeichert werden.

   Es spricht viel dafür, die Nutzung des Internet für die Veröffentlichung von Steckbriefen und Fahndungsaufrufen durch die Polizei zu verbieten (das amerikanische Federal Bureau of Investigations veröffentlicht seit einiger Zeit eine Liste von gesuchten Verdächtigen im Internet). Die beschriebenen Defizite der Authentifizierungsprozeduren und die leichte Manipulierbarkeit von Bildern im Cyberspace scheinen die Nutzung des Internet für diesen Zweck auszuschließen.

3. Verschiedene nationale Regierungen haben internationale übereinkommen über die globale Informations-Infrastruktur angeregt. Initiativen für eine engere internationale Zusammenarbeit, ja sogar eine internationale Konvention, die den Datenschutz im Hinblick auf grenzüberschreitende Netze und Dienste regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz

personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen. Konzepte für solche Maßnahmen sind bereits entwickelt und veröffentlicht worden. Beispiele sind das "Identity-Protector"-Konzept, das in "Privacy-enhancing technologies: The path to anonymity" von der niederländischen Registratiekamer und dem Datenschutzbeauftragten von Ontario/Kanada enthalten ist (vorgestellt auf der 17. Internationalen Konferenz der Datenschutzbeauftragten in Kopenhagen (1995)) und das "User Agent-Konzept", das auf der gemeinsamen Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation und der Privacy Working Group der Information Infrastructure Task Force vorgestellt wurde (April 1995).

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden.

   Die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

   Die Arbeitsgruppe unterstützt neue Entwicklungen im Internet-Protokoll (z. B. IP v6), die die Vertraulichkeit durch Verschlüsselung, Klassifizierung von Nachrichten und bessere Authentifizierungsprozeduren verbessern. Die Hersteller von Software sollten den Sicherheitsstandard des neuen Internet-Protokolls in ihre Produkte aufnehmen und Diensteanbieter sollten die Nutzung dieser Produkte so schnell wie möglich unterstützen.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von "Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten "Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

    Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die weitere Entwicklung in

diesem Bereich genau beobachten, Anregungen aus der Netzgemeinde berücksichtigen und weitere, detailliertere Vorschläge entwickeln.

Grenzen und Möglichkeiten der staatlichen Reglementierung des Einsatzes von Verschlüsselungsverfahren

Arbeitspapier der AG Kryptographie des AK Technik; Stand: September 1996

Ergebnis der Betrachtungen

Jede staatliche Reglementierung des Einsatzes kryptographischer Verfahren bei der Übertragung und Speicherung von Daten stößt ins Leere, weil:

- sie leicht umgangen werden kann, insbesondere dann, wenn die notwendigen Fachkenntnisse und finanziellen Mittel zur Verfügung stehen (z. B. in Kreisen des organisierten Verbrechens),

- sie kaum kontrollierbar ist, weder aus technischer noch aus finanzieller Sicht,

- sie anderen staatlichen und wirtschaftlichen Interessen an der Sicherung von Daten gegen Risiken der Vertraulichkeit, Integrität (Unversehrtheit) und Zurechenbarkeit (Authentizität) bei der Übertragung und Speicherung zuwiderläuft,

- sich bei den dann eventuell realisierten Stichprobenkontrollen die unbefugte Kenntnisnahme übermittelter oder gespeicherter Daten nicht verhindern läßt.

Unter technischen Aspekten sollte die staatliche Reglementierung des Einsatzes kryptographischer Verfahren unterlassen werden, da sich der erhoffte Nutzen bei der Bekämpfung der organisierten Kriminalität und der Verhinderung von Straftaten aus diesem Bereich nicht einstellen wird.

Dagegen stehen sowohl erhebliche Kosten bei der Überwachung der Regelungen und dem Aufbau einer Kontrollinfrastruktur als auch die Tatsache, daß Daten durch mangelhaft geschützte Übertragung und Speicherung in zunehmendem Maße der organisierten Computerkriminalität ausgesetzt werden.

Zusammenfassung

In den letzten Jahren hat sich die in breiten Bevölkerungskreisen prinzipiell verfügbare DV-Technik und Kommunikationstechnik so entwickelt, daß Verschlüsselungsverfahren praktisch eingesetzt werden können. Sie sind - je nach Algorithmus und Implementierung - sowohl geeignet, Daten auf Rechnern als auch eine Telekommunikation zu verschlüsseln. Damit kann es insbesondere Außenstehenden unmöglich gemacht werden, Kommunikationsinhalte zur Kenntnis zu nehmen. Der Bürger hat also die Möglichkeit, das Fernmeldegeheimnis mit eigenen Mitteln zu schützen. Im Fall einer staatlichen Überwachungsmaßnahme bedeutet das:

> Die Überwachungsbehörden können den Nachrichteninhalt eventuell nicht entziffern oder nicht einmal feststellen, daß eine - versteckte - Nachricht vorliegt.

Überlegungen, wie das Problem einer Überwachung der Telekommunikation unter diesen Voraussetzungen gehandhabt werden kann, führen zu vier denkbaren Handlungsalternativen.

a) Der Einsatz von Verschlüsselungsverfahren wird verboten; ggf. besteht ein Genehmigungsvorbehalt.

b) Es werden Algorithmen und Verfahren zugelassen, die Schwachstellen besitzen, die den Überwachungsbehörden bekannt sind.

c) Es werden Schlüssel(-teile) hinterlegt, die es im Fall einer Strafverfolgungsmaßnahme erlauben, die Daten zu entschlüsseln (Key-Escrow).

d) Es erfolgt keine Reglementierung.

Die Alternativen a) und b) geben Dritten - neben Bedarfsträgern können z. B. ausländische Geheimdienstes oder kriminelle Kreise die Kenntnisse erlangen - die Möglichkeit, mit vergleichsweise geringem Aufwand eine Kommunikation zu überwachen. Diese Lösungen widersprechen auch in wesentlichen Punkten Entschließungen der Datenschutzbeauftragten.

Die Alternative c) bietet dem Bürger einen hohen Schutz gegen das Abhören durch unberechtigte Stellen. Sie erfordert aber eine Infrastruktur, deren verläßliche Funktion unumgänglich ist. Dazu müssen Personal, Organisation und Technik sehr hohe Anforderungen erfüllen.

Die Lösung d) läßt dem Bürger in seiner Kommunikation alle Möglichkeiten offen. Eine Überwachung der Telekommunikation durch Bedarfsträger dürfte aber in vielen Fällen nicht zum Ziel führen.

Eine Überwachung kann in jedem Fall unterlaufen werden, indem man

- einen mit dem Partner vorher abgesprochenen Code benutzt (Codierung),

- mit einem zugelassenen Verschlüsselungsverfahren einen Text überträgt, der vorher mit einem nicht reglementierten Verfahren verschlüsselt wurde; entsprechende Verfahren sind zu geringen Kosten allgemein verfügbar (Überschlüsselung),

- Informationen in digitalen Signalen so versteckt, daß diese bei der Überwachung nicht erkannt werden (Steganografie),

- Lücken im Übertragungsprotokoll nutzt.

Wenn der Einsatz von Verschlüsselungsverfahren nicht nur für die Telekommunikation, sondern auch bei der Speicherung von Informationen reglementiert würde, wären "Grundfesten" des Datenschutzes betroffen, weil in vielen Bereichen die verschlüsselte Speicherung personenbezogener Daten gefordert und realisiert wurde. Insbesondere bei den Alternativen a) und b) kann eine ausreichende Datensicherheit vielfach nicht mehr gewährleistet werden.

Weitere Probleme sind neben Normenklarheit und Beweislast auch die Trennung zwischen digitaler Signatur - deren geheime Schlüssel nicht hinterlegt oder für Fremde nutzbar werden dürfen - einerseits und verschlüsselter Kommunikation andererseits.

Darüber hinaus stellt sich die Frage nach Sinn und Auswirkung nationaler Regelungen bei zunehmend supranationaler Kommunikation: wie wird mit dem Ersuchen ausländischer Strafverfolgungsbehörden nach einer Preisgabe geheimer Schlüssel von Bundesbürgern oder Firmen verfahren?

1. Beschreibung der Situation

1.1 Bundesrepublik Deutschland

Seit einiger Zeit wird von der Bundesregierung geprüft, ob das Erfordernis einer rechtlichen Regelung des Einsatzes von Verschlüsselungsverfahren besteht (vgl. Bundestagsdrucksache 13/1889). Durch die Empfehlung des Europarates No. R(95) 13 vom 11.09.1995 hat die Fragestellung an Aktualität gewonnen. Dies wird auch in der Presse aufgegriffen. So berichtet der Spiegel (2/96, Seite 106; 13/96, Seite 141 f.), daß über staatliche Reglementierungen der Nutzung von Verschlüsselungsverfahren bei e-mail nachgedacht wird.

Interessant ist zu diesem Zusammenhang auch die Antwort der Bundesregierung zur Kleinen Anfrage "Sicherheit der Informationstechnik und Kryptierung" (Bundestagsdrucksache 13/4105 vom 14.03.1996)

Die Gesellschaft für Informatik (GI) hat am 28. Februar 1996 ihre Bedenken gegen staatliche Einschränkung der Kryptographie in einer Presseerklärung veröffentlicht (vgl. auch DuD 5/96). Der Vorstand des TeleTrusT Deutschland e. V. hat am 26. März 1996 gegenüber sechs Bundesministern und dem Bundeskanzleramt zu gesetzlichen Anforderungen an den Einsatz von Verschlüsselungsverfahren Stellung genommen und Position zur Gewährleistung der Vertraulichkeit bei der Übermittlung von Nachrichten bezogen (vgl. auch DuD 5/96).

Wenn der Entwurf zu einem Kryptogesetz von der Bundesregierung eingebracht werden sollte, dürfte innerhalb kürzester Zeit eine breite öffentliche Diskussion stattfinden. Zu diesem Zeitpunkt sollten sich die Datenschutzbeauftragten bereits mit dem Problem beschäftigt haben.

Die folgende Darstellung versucht Rahmenbedingungen aus technischer Perspektive zu verdeutlichen.

1.2 Gesetzliche Reglementierungen des Einsatzes von Verschlüsselungsverfahren

Australien, Dänemark, Finnland, Großbritannien, Irland, Island, Japan, Kanada, Litauen, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Schweiz, Spanien, Türkei, Ungarn, USA In diesen Ländern ist der *Einsatz* von Verschlüsselungsverfahren nicht reglementiert. In den **Niederlanden** wurde ein erster Gesetzentwurf zur Reglementierung starker Verschlüsselungsverfahren aufgrund massiver öffentlicher Kritik zurückgezogen. Das Thema ist dort jedoch weiterhin in der Diskussion. Die Regierung der **USA** versucht mit der sog. "Clipper-Initiative" seit 1993 ein Verschlüsselungsverfahren zu standardisieren, das die Belange der Strafverfolgungsbehörden berücksichtigt. Es basiert auf der zentralen Hinterlegung von Teilschlüsseln bei zwei Regierungsstellen. Die Initiative ist aufgrund öffentlicher Kritik ins Stocken geraten.

Frankreich
Die Herstellung, der Einsatz und der Export von Verschlüsselungsprogrammen ist seit Dezember 1990

genehmigungspflichtig (Gesetz Nr. 90-1170). Die Genehmigung erteilt der Premierminister. Nicht genehmigungspflichtig, jedoch anzeigepflichtig, sind Verfahren, die ausschließlich zur Authentifizierung einer Verbindung oder der Integritätskontrolle einer Nachricht dienen. Die Verwendung nicht genehmigter Verschlüsselungsverfahren wird mit Geldstrafen bis 500.000 FF und drei Monaten Haft geahndet. Zielrichtung des Gesetzes ist die Wahrung der nationalen Verteidigungsinteressen und der inneren und äußeren Sicherheit des Landes.

Belgien

Im Dezember 1994 wurde ein Gesetz verabschiedet, das die Möglichkeit einer Konfiszierung von Telekommunikationsgerät vorsieht, mit dessen Hilfe ein staatliches Abhören verhindert wird. Das Gesetz wird z. Z. offenbar nicht in dieser Weise angewendet.

Rußland

Die Entwicklung und Herstellung, der Vertrieb und die Benutzung von Verfahren zur sicheren Speicherung oder Übertragung von Nachrichten sind genehmigungspflichtig (Dekret Nr. 334 des Präsidenten vom April 95). Die nicht genehmigte Verwendung solcher Verfahren ist verboten. Zielrichtung des Dekrets sind die Interessen der Informationssicherheit der Russischen Föderation sowie die Bekämpfung der organisierten Kriminalität.

Weißrußland

Für die Herstellung und den Betrieb von Verschlüsselungsgerät ist eine Genehmigung erforderlich.

Europarat

Im September 1995 wurde beschlossen, den Mitgliedsstaaten zu empfehlen, Maßnahmen zu erwägen, die die negativen Auswirkungen des Einsatzes von Verschlüsselungsverfahren bei der Strafverfolgung minimieren. Die legitime Verschlüsselung solle dabei jedoch nicht stärker als erforderlich eingeschränkt werden (Recommendation No. R(95) 13).

1.3 Verschlüsselungsverfahren in der Telekommunikation

1.3.1 Technische und organisatorische Rahmenbedingungen

Die Verfügbarkeit von Algorithmen in einer Softwareimplementation ist spätestens seit der Verbreitung des Internet für interessierte Bürger kein Problem mehr. So ist speziell das Programm PGP zu diesem Zweck konzipiert und verbreitet worden. Aber auch Implementationen anderer Algorithmen wie des DES liegen auf Servern für jedermann abrufbar vor. Dabei handelt es sich teilweise um Algorithmen, die als sicher angesehen werden müssen, d. h. sie sind nicht mit vertretbarem Aufwand zu brechen. Die Sicherheit der heutigen Verfahren ist allerdings nur durch empirische Erkenntnisse einschätzbar.

Den Bemühungen, Wege zu finden, um die Verfahren zu knacken, wird durch Fortschritte bei den Algorithmen und Entwicklung neuer Verfahren begegnet.

Beispielsweise wird an Quantencomputern gearbeitet. Das sind Computer, die insbesondere auch nach den Gesetzen der Quantenmechanik arbeiten. Wenn ein funktionierender Quantencomputer überhaupt gebaut werden kann, ist Faktorisieren von Zahlen und Durchprobieren von Schlüsseln für ihn eine Kleinigkeit; damit wären die heutigen Kryptoverfahren, wie z. B. RSA und DES, zu brechen.

Andererseits wird versucht, Verfahren zu entwickeln, die nicht gebrochen werden können: die Quantenkryptographie versucht dies über den Einsatz quantenmechanischer Methoden. Sie setzen einen quantenkohärenten Zustand zwischen Sender und Empfänger voraus, der bei jedem Meß- bzw. Abhörvorgang zerstört würde. Damit wäre die Ursprungsinformation zerstört, also nicht abhörbar, und das Abhören könnte nachgewiesen werden.

Die Erfahrungen aus verschiedenen Projekten mit den klassischen Kryptographieverfahren zeigen, daß die größten Probleme in der Realisierung der Schlüsselverwaltung liegen. Kleine, geschlossene Benutzergruppen können untereinander mit ziemlich geringem Aufwand Schlüssel austauschen, während sich für große Benutzerkreise oder offene Systeme Lösungen noch bewähren müssen.

Ein weiteres Verfahren - die Steganografie - soll hier genannt werden, obwohl es kein Verschlüsselungsalgorithmus im hergebrachten Sinn ist. Sie erlaubt es, in Audio- oder Bildinformationen Nachrichten zu verstecken. Entsprechende Programme sind im Internet verfügbar (vgl. Datenschutzberater 1/96; dort wird auf weitere Quellen verwiesen). An die Software kann jedermann gelangen, so auch Personen, die das Verfahren zu kriminellen Zwecken nutzen wollen.

1.3.2 Denkbare Handlungsalternativen

Es gibt prinzipiell vier Handlungsalternativen zu dem Themenkreis "Überwachung der Telekommunikation", wenn die Kommunikationsteilnehmer Verschlüsselungsverfahren einsetzen.
- Auf die Durchsetzbarkeit soll an dieser Stelle noch nicht eingegangen werden. -.

a) Der Einsatz von Verschlüsselungsverfahren wird verboten; ggfs. besteht ein Genehmigungsvorbehalt.

b) Es werden Algorithmen und Verfahren zugelassen, die Schwachstellen besitzen, die den Überwachungsbehörden bekannt sind. Dies können z. B. Schwächen des Algorithmus oder kurze Schlüssellängen sein.

c) Es werden Schlüssel(-teile) hinterlegt, die es im Fall einer Strafverfolgungsmaßnahme erlauben, die Daten zu entschlüsseln (Key-Escrow).

d) Es erfolgt keine Reglementierung.

Alle vier Ansätze werfen Probleme auf, auch unter der Annahme, daß sich die Kommunikationspartner gesetzeskonform verhalten.

1.3.3 Konsequenzen aus den Handlungsalternativen

Mit einer Kryptoreglementierung ist untrennbar die Frage nach der Durchsetzung verbunden. Bei den Alternativen a), b) und c) müßte eine Kontrollinfrastruktur geschaffen werden, die überwacht, ob sich die Kommunikationsteilnehmer an die Gesetze halten. Diese Überwachung, die zumindest in Form einer Stichprobe stattfinden muß, kann jeden Bürger ohne Vorliegen eines Anhaltspunktes für einen Verstoß treffen. Dabei werden Kommunikationsbeziehungen und in vielen Fällen Kommunikationsinhalte im Zuge der Kontrolle bekannt; sie bedingen einen Eingriff in das Fernmeldegeheimnis.

zu a)

Konsequenzen für den Bürger

Es wird dem Bürger die Möglichkeit genommen, sich selbst gegen einfachste Abhöraktionen oder zufällige Kenntnisnahme durch Dritte zu schützen. Dies gilt beispielsweise für den Versand elektronischer Post (e-mail) im Internet, bei Compuserve oder anderen Anbietern, bei dem die Nachricht über diverse, dem Teilnehmer nicht bekannte Server läuft. Die Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Mitteilungssystemen empfiehlt zur Wahrung der Vertraulichkeit von übertragenen personenbezogenen Daten eine Verschlüsselung. Darüber hinaus fordern die Datenschutzbeauftragten in ihrer Entschließung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten bei deren Transport geeignete, sichere kryptographische Verfahren zu verwenden.

In vielen Fällen, so bei der Kommunikation von Banken oder in Wirtschaftsunternehmen, müßten Ausnahmen erforderlich sein, da z. B. ausländische Nachrichtendienste Wirtschaftsspionage betreiben und sich die Unternehmen schützen können müssen.

Konsequenzen für Bedarfsträger

Die Bedarfsträger können die Kommunikation mit vergleichsweise geringem Aufwand überwachen. Die Kontrolle der Behörden dürfte analog dem jetzigen Verfahren geregelt werden können.

zu b)

Falls Verschlüsselungsverfahren mit Schwachstellen eingesetzt werden, können potentielle Angreifer - wie auch ausländische Nachrichtendienste (Wirtschaftsspionage) oder kriminelle Organisationen - das Verfahren brechen und anschließend die Kommunikation überwachen. Diese unerwünschte Dechiffrierung würde nicht auffallen und wäre nicht kontrollierbar. Auch dies wäre mit den Forderungen der beiden o. g. Entschließungen unvereinbar.

Anm.:

In Exportversionen von US-amerikanischer Software sind ausschließlich schwächere Algorithmen oder kürzere Schlüssellängen implementiert, u. a. zu dem Zweck, daß amerikanische Geheimdienste die Möglichkeit zur Überwachung haben. Beispiele sind:

- de Software Netscape besitzt in der Exportversion 40-Bit Schlüssel statt 128-Bit Schlüssel wie in der amerikanischen Version.

- Lotus Notes 4.0 besitzt 64-Bit Schlüssel, von denen 24 Bit aber der NSA (amerikanischer Geheimdienst) bekannt sind.

In beiden Fällen kann mit einem relativ geringen Aufwand eine Entschlüsselung durch Ausprobieren der möglichen Schlüssel erfolgen.

Konsequenz für den Bürger

Gegen einfache Abhöraktionen oder zufällige Kenntnisnahme besteht ein Schutz. Der Bürger kann aber nie sicher sein, wer seine Kommunikation abhört.

Konsequenz für die Bedarfsträger

Die Behörden können mit einem überschaubaren Aufwand die Kommunikation überwachen. Die Kontrolle dürfte analog der bisherigen Vorgehensweise durchgeführt werden. Wie bei Alternative a) kann einer Verdächtigung, daß ohne die rechtlich erforderlichen Genehmigungen eine Überwachung durchgeführt wurde, nur unvollkommen begegnet werden.

Verschlüsselungssoftware muß zugelassen werden.

zu c)

Eine derartige Reglementierung erfordert eine Infrastruktur mit Institutionen, die Schlüssel speichern. Die Schlüsselerzeugung muß nicht notwendig, kann aber durch die gleichen Institutionen erfolgen.

Anm.:
Es gibt den Ansatz der fairen Systeme, bei dem der Teilnehmer seine Schlüssel selbst generiert und an Institutionen verteilen kann.

Sollten diese Institutionen fehlerhaft arbeiten, ist damit die Gesamtsicherheit nicht mehr gewährleistet. Um an geheime Informationen zu gelangen, wären sie die besten Ansatzpunkte. Bei einer Gefährdungsanalyse reicht es nicht aus, ausschließlich Organisation und Technik zu betrachten. Einen wesentlichen Schwachpunkt stellt das Personal dar, das vielfältigen Gefahren ausgesetzt ist. Um an die geheimen Schlüssel zu gelangen, gibt es vielfältige Einwirkungsmöglichkeiten wie Erpressung des Personals, Spionage, Erpressung durch das Personal, Bestechung usw.

Es müssen Regularien getroffen werden, die gewährleisten, daß nur im Rahmen zulässiger Überwachungsmaßnahmen auf die geheimen Schlüssel zugegriffen werden kann. Dazu gehören auch eine Reihe von Detailfragen, die in diesem Zusammenhang geklärt werden müssen.

- Für wen gelten die Vorschriften (Diensteanbieter, alle Bürger ...)?

- Wie wird gewährleistet, daß die schlüsselverwaltende Stelle nicht ungerechtfertigt Schlüssel herausgibt?

- Was geschieht nach Abschluß einer Überwachungsmaßnahme? Den Überwachungsbehörden bekannte Schlüssel müssen ungültig werden. Der Teilnehmer muß darüber informiert werden.

Konsequenzen für den Bürger
Es besteht ein hoher Schutz gegen das Abhören durch unberechtigte Stellen. Es darf allerdings nur Software eingesetzt werden, die den Erfordernissen genügt.

Konsequenzen für Bedarfsträger
Die Überwachungsmaßnahmen sind mit einem relativ hohen Aufwand verbunden. Die Software, die von den Bürgern eingesetzt werden darf, muß geprüft und freigegeben werden.

zu d)

Konsequenzen für den Bürger
Es besteht ein sehr hoher Schutz der Kommunikation gegen Abhörung durch Dritte.

Konsequenzen für Bedarfsträger
Eine Überwachung der Telekommunikation wird in vielen Fällen nicht zum Ziel führen. Es muß nach Alternativen gesucht werden.

1.3.4 Möglichkeiten, eine Überwachung zu unterlaufen

Wird mit einer Überwachung gerechnet, so kann diese auf verschiedene Weise unterlaufen werden:

- Codierte Informationen:
  (kann unter jeder der drei Optionen a) - c) benutzt werden)

  Es werden Codes genutzt, die für den eigentlichen Nachrichteninhalt stehen. Beispiel: Zu Zeitangaben muß immer eine Stunde addiert werden. Auf diese Weise fällt es nicht auf, wenn Informationen ausgetauscht werden.

  Hierzu muß vorher eine Absprache der Kommunikationsteilnehmer erfolgt sein. Das Vorgehen funktioniert nur in einer geschlossenen Benutzergruppe. Je nach gewählter Codierung ist es kaum noch möglich, die Information zu entziffern.

- Überschlüsselung
  (Optionen b) und c))

  Es wird mit einem zugelassenen Verschlüsselungsverfahren ein Text übertragen, der vorher mit einem nicht reglementierten Verfahren verschlüsselt wurde.

  Es muß nicht notwendig eine geschlossene Benutzergruppe existieren, z. B. ist es möglich, mit einem reglementierten Verfahren dem Kommunikationspartner zu einem beliebigen Zeitpunkt den öffentlichen PGP-Schlüssel und die PGP-Version mitzuteilen. Nachrichteninhalte könnten mit PGP verschlüsselt werden und anschließend mit dem reglementierten Verfahren zusätzlich verschlüsselt werden.

  Bei einer Überwachungsmaßnahme würde die übertragene Nachricht entschlüsselt. Erst zu diesem Zeitpunkt fällt auf, daß ein nicht reglementiertes Verfahren genutzt wurde. Die Nachrichteninhalte bleiben geheim.

- Steganografie
  (Optionen a) - c))

  Es werden Informationen in digitalen Signalen so versteckt, daß diese bei einer Überwachung nicht erkannt werden (siehe Datenschutzberater 1/96). - Die Steganografie hinterläßt in den jetzt verfügbaren Programmversionen möglicherweise Spuren, die auf ihren Einsatz hindeuten. Es müßte aber speziell danach gesucht werden. - Als weitere Hürde können die Informationen zusätzlich verschlüsselt werden.

  Auch hier muß im Vorfeld eine Einigung zwischen den Kommunikationspartnern über das Verfahren erfolgen. Anschließend dürfte eine Überwachung erfolglos sein.

- Lücken im Übertragungsprotokoll

  Es ist beim Clipper-Ansatz gelungen, das Übertragungsprotokoll so zu ändern, daß auf den ersten Blick alles korrekt war. Erst bei einer Überwachungsmaßnahme wäre dann festgestellt worden, daß den Behörden kein gültiger Schlüssel vorliegt.

Aufwand

Die Software für eine Überschlüsselung oder die Steganografie ist allgemein verfügbar. Sie kann mit geringen Kosten beschafft werden. In einer kleinen geschlossenen Benutzergruppe - dazu gehören auch Straftäter - ist der Schlüsselaustausch mit geringem Aufwand möglich.

Fazit

Wenn mit gruppenspezifisch codierten Informationen gearbeitet wird, fallen die gesuchten Informationen bei einer Überwachung in vielen Fällen nicht auf. Für die Steganografie gilt universell entsprechendes. Es wäre folglich kein Verstoß gegen Gesetze feststellbar. Im Fall einer Überschlüsselung können die Überwachungsbehörden erst zum Zeitpunkt der Überwachung den Verstoß feststellen.

Die Zielsetzung der Bedarfsträger kann mit geringem Aufwand unterlaufen werden. In Anbetracht der Straftaten, bei denen eine Überwachung zulässig ist, dürften die Täter gerade in diesen Fällen von den Möglichkeiten Gebrauch machen.

2. Verschlüsselte Speicherung

Ein Einsatz von Verschlüsselungstechniken erfolgt nicht nur zur Sicherung der Datenübertragung, sondern auch zur gesicherten Speicherung von Daten auf Datenträgern wie Festplatten, Bändern oder Disketten. Hier gelten zum Teil andere Rahmenbedingungen:

- Die verschlüsselte Speicherung wird vielerorts bereits gefordert und eingesetzt, u. a. um Datensicherheit bei einem Diebstahl von Computern (z. B. Laptops) oder Datenträgern zu gewährleisten. Ein Verschlüsselungsverbot würde in solchen Fällen dazu führen, daß eine ausreichende Sicherheit vielfach nicht mehr gewährleistet ist.

- Eine verschlüsselte Speicherung erfolgt im allgemeinen unabhängig von zentralen Schlüsselverwaltungsinstanzen und nicht zwischen Kommunikationspartnern. Die betroffenen Rechner haben in vielen Fällen keinerlei DFÜ-Technik. Eine individuelle Verschlüsselung mit beliebigen Verschlüsselungsverfahren wird hier durch erleichtert und bleibt unbemerkt. Eine Überwachung der Einhaltung eines Kryptogesetzes wäre nur mit Hilfe von Hausdurchsuchungen und Beschlagnahme von Datenträgern möglich.

- Im Gegensatz zum Abhören bei Übertragungen erfolgt das Lesen beschlagnahmter Datenträger fast ausschließlich mit Wissen des Betroffenen. Es besteht somit für Überwachungsbehörden nicht die Notwendigkeit, in den Besitz der Schlüssel zu gelangen, bevor der Betroffene von der Überwachungsmaßnahme Kenntnis erhält. Vielmehr reicht es aus, den Schlüssel bei Beschlagnahme der Datenträger vom Betroffenen zu fordern. In den Fällen, in denen sich der weigert, den Schlüssel herauszugeben, ist anzunehmen, daß er auch nach Einführung eines gesetzlich

vorgeschriebenen Key-Escrow-Verfahrens ein nicht genehmigtes Verschlüsselungsverfahren einsetzen würde, um die Preisgabe der Daten bei einer Beschlagnahme der Datenträger zu verhindern.

Diese Punkte sprechen gegen ein Verschlüsselungsverbot bzw. gegen ein Key-Escrow-Verfahren. Bei einer Regelung, die zwischen Übertragung und Speicherung differenziert, gäbe es das Problem einer klaren Trennung beider Bereiche. So ist fraglich, ob eine Übertragung zwischen PC und Server bereits als Übertragung anzusehen ist oder ob aus einer Speicherung eine Übertragung wird, wenn ein Datenträger transportiert wird.

3. Weitere Probleme

- Internationale Kommunikation

  Wie sinnvoll sind nationale Regelungen bei supranationaler Kommunikation? Beim freien Binnenmarkt bereitet eine Kryptoreglementierung auch wegen der damit verbundenen Handelsbeschränkungen Probleme. Wie sind staatliche Genehmigungsvorbehalte und ihre Auswirkungen zu sehen? Kann sich der Bürger angesichts der Vielfalt unterschiedlicher nationaler Handels- und Nutzungsbeschränkungen überhaupt noch gesetzeskonform verhalten?

  Es stellt sich zudem die Frage, wie mit dem Ersuchen ausländischer Strafverfolgungsbehörden nach einer Preisgabe von geheimen Schlüsseln von Bundesbürgern oder von Firmen zu verfahren ist.

- Trennung digitale Signatur/verschlüsselte Kommunikation

  Die zu einer digitalen Signatur gebrauchten Algorithmen und Schlüssel sind zumindest im Fall von DES und RSA prinzipiell geeignet, Daten zu verschlüsseln. Es ist aber undenkbar, daß die bei der digitalen Signatur eingesetzten geheimen Schlüssel als Kopien gespeichert werden, da dann Dokumente gefälscht werden könnten.

  Eine Reglementierung der Verschlüsselung darf in keinem Fall den Zugriff auf Schlüssel vorsehen, die zur digitalen Signatur vorgesehen sind.

- Technische Rahmenbedingungen

  Bei einer Kontrolle auf Verstöße gegen ein Kryptogesetz könnte bereits ein exotisches Protokoll als nicht interpretierbar und damit als Verstoß angesehen werden.

- Normenklarheit

  Es muß eine Abgrenzung zwischen verschlüsselten Daten, codierten Informationen und Protokollen getroffen werden, um deren Zulässigkeit regeln zu können.

- Beweislast

  Was geschieht, wenn durch technisches Versagen Daten übertragen werden, die nicht interpretiert werden können? Wie soll ein Beschuldigter beweisen, daß es das Ergebnis eines technischen Versagens ist? Wie kann die

Staatsanwaltschaft das Gegenteil beweisen?

4. Fragestellungen

Ist es gerechtfertigt, Reglementierungen vorzunehmen?

Beschnitten werden die Möglichkeiten, das Fernmeldegeheimnis oder die Vertraulichkeit von Daten mit eigenen Mitteln zu schützen. So kann ein Bürger die Vertraulichkeit elektronischer Mitteilungen gegenüber Diensteanbietern, Betreibern und auch Behörden mit einer Verschlüsselung erreichen.

Andererseits zielt eine Reglementierung darauf ab, dem Staat Eingriffsmöglichkeiten zu geben, die den Bürger schützen.

- Handelt es sich bei der Reglementierung des Einsatzes von Verschlüsselungsverfahren um ein geeignetes Mittel der Strafverfolgung?

- Hält eine Kryptoreglementierung einer Wirtschaftlichkeitsbetrachtung stand?
  Die zur Umsetzung einer Kryptoreglementierung nötige Infrastruktur dürfte mit erheblichen Kosten verbunden sein, sowohl beim Aufbau als auch im Betrieb. Es stellt sich die Frage, ob das mit dem zu erwartenden Erfolg zu rechtfertigen ist.

- Soll eine Reglementierung für alle Kryptosysteme gelten?
  Telekommunikation
  Rechnersysteme

- Gibt es Lösungen, die in einem Kryptogesetz nicht gewählt werden dürfen?
  Verbot der Kryptographie
  schwache Algorithmen
  Escrow Agencies

- Gibt es Forderungen, die je nach gewählter Lösung eingehalten werden müssen?
  Einschränkung des Gesetzes auf Diensteanbieter

- Wie soll ein Verstoß geahndet werden?
  OWI, Straftat, Geldbuße, Haft ...

Quellenangaben

- Antwort auf die Kleine Anfrage "Überlegungen der Bundesregierung zur Verschlüsselung von Daten in der Telekommunikation", BT-Drs. 13/1889 vom 29.06.1995

- Antwort auf die Kleine Anfrage "Sicherheit der Informationstechnik und Kryptierung", BT-Drs. 13/4105 vom 14.03.1996

- Europaratsbeschluß Recommendation No. R(95) 13 vom 11.9.95

- Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Mitteilungssystemen.

- Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

- Workshop Kryptographie vom 31.8.94; Protokoll verschickt am 15.12.94

- Datenschutzberater 1/96

- DuD 1/96 mit dem Schwerpunktthema Kryptographie

- Spiegelartikel aus 2/96, Seite 106, 11/96, Seite 102 ff., 13/96, Seite 142 f.

- Hammer, V. (1995), Sicherungsinfrastrukturen, ISBN 3-540-60081-7

- Kuner, Rechtliche Aspekte der Datenverschlüsselung im Internet, CoR 6/95, S. 413 ff.

- Lloyd, S., Quanten-Computer, Spektrum der Wissenschaft, Dez. 1995

- Pressemitteilung der GI vom 28.02.1996, Bedenken der Gesellschaft für Informatik gegen staatliche Einschränkung der Kryptographie, vgl. DuD 5/96

- TeleTrusT Deutschland e. V. zu gesetzlichen Anforderungen an den Einsatz von Verschlüsselungsverfahren, Stellungnahme vom 26.03.1996, vgl. DuD 5/96

- http://cwis.kub.ml/~frw/people/koops/lawsurvy.html

- http://web.cnam.fr/Network/Crypto/survey.html

Erarbeitet von Helmut Eiermann (LfD Rheinland-Pfalz), Walter Ernestus (BfD), Dr. Martin Hube (LfD Niedersachsen), Ulrich Kühn (HambDSB), Werner Moritz (LfD Bremen), Dr. Gisela Quiring-Kock (LfD Hessen), Rüdiger Wehrmann (LfD Hessen), Dr. Thilo Weichert (LfD Niedersachsen). Als Sachverständiger hat Dr. Michael Hortmann, Universität Bremen, mitgewirkt.

Arbeitsgruppe Chipkarten [1]

des Arbeitskreises "Technische und organisatorische Datenschutzfragen"
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Anforderungen zur informationstechnischen Sicherheit bei Chipkarten

Stand 02.12.1996 [2]

I. Einleitung

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Sie haben Eingang ins tägliche Leben gefunden, gewinnen zunehmend an gesellschaftlicher Bedeutung und bedürfen aus der Sicht des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Ebenfalls allgemein bekannt ist die Krankenversichertenkarte (KVK), die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent.

Weitere neue Anwendungsbereiche von Chipkarten sind derzeit in der Diskussion bzw. in der Erprobung, z. B.:

- die Chipkarte im bargeldlosen Zahlungsverkehr,
- Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Von der Technik her sind reine Speicherchipkarten zur Aufnahme von Daten (meist in Halbleiter-Technologie oder optischer Speichertechnik) von solchen Karten zu unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Solche Prozessorchipkarten sind als Kleinstcomputer ohne Mensch-Maschine-Schnittstelle anzusehen. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher.

Systeme zur Erschließung der Funktionen von Chipkarten werden im folgenden Chipkartenbasierte Dienstleistungssysteme (CDLS) genannt. Beispiele für solche Systeme sind:

- Öffentliches Telefon-Kartenterminal
- Funktelefon (Handy)
- PC mit externem Kartenterminal oder integriertem Kartenleser
- Laptop mit PCMCIA-Kartenleser

- Geldausgabeautomat
- Point-of-Sale-Kartenterminal (POS-Kartenterminal)
- Versicherten-Kartenterminal in seiner Stand-alone-Ausführung (ohne PC-Anschluß)
- Kontoauzugsdrucker
- Airline-Checkin-Terminal
- Customer-Service-Terminal
- Fahrschein-/Parkticket-Terminal

Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Wichtige Funktionalitäten der Chipkarten sind:

- Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische Individualdaten, Personalausweisdaten, Führerscheindaten);

- Chipkarten als Mittel zur Authentisierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten);

- Chipkarten als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.);

- Chipkarten als Träger elektronischer Geldbörsen.

Die weiteren Ausführungen dieses Papiers beschränken sich auf die für die Sicherheit der Informationstechnik relevanten Merkmale und Anforderungen an Chipkarten, sowohl in ihrer Funktion als Instrumente zur Herstellung von Sicherheit als auch als sicherheitsbedürftige IT-Komponenten.

Obwohl - wie die Krankenversichertenkarte zeigt - auch Speicherchipkarten datenschutzrechtlich relevant sind, beschränken sich die weiteren Ausführungen auf Prozessorchipkarten. Diese haben in Zukunft sowohl hinsichtlich ihrer Verbreitung und Anwendung als auch in Hinblick auf datenschutzrechtliche Chancen und Risiken eine größere datenschutzrechtliche Bedeutung.

II. Empfehlungen zum Einsatz von Chipkarten

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Dabei ist von folgenden Gefahren auszugehen:

- unbefugte Preisgabe von Informationen (Verlust der **Vertraulichkeit**);
- unbefugte Veränderung von Informationen (Verlust der **Integrität**);

- unbefugte Vorenthaltung von Informationen oder Betriebsmitteln (Verlust der **Verfügbarkeit**);

- unbefugte Änderung identifizierender Angaben (Verlust der **Authentität**).

Diese Gefahren sind sowohl dann zu betrachten, wenn die Daten auf der Chipkarte gespeichert werden, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die durch Chipkarten erschlossen wird.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte eine projektbezogene Technikfolgenabschätzung durchgeführt werden, so wie dies Art. 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht und das Recht auf kommunikative Selbstbestimmung vorzunehmen und sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen "Chipkarte" zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chipkarte selbst. Genausowenig wie es "die" Chipkarte gibt, genausowenig kann man von "der" Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die geplanten Gesundheits- und Patientenchipkartensysteme sind insoweit geeignete Beispiele.

Notwendig erscheint auch eine dauernde Bereitschaft, die schnell fortschreitende technologische Weiterentwicklung aufmerksam zu begleiten und bei Bedarf steuernd einzugreifen, denn die datenschutztechnischen Fragestellungen werden um so komplexer, je weiter sich die Chipkartentechnologie entwickelt.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Diese werden über CDLS realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den CDLS auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung von Chipkarten in Fällen des Verlustes oder der Zerstörung einschließlich des "Ungültigkeitsmanagements". Die Hersteller bieten Chipkarten an, deren Leistungsfähigkeit und Funktionsweise diesbezüglich zum Teil sehr unterschiedlich ist. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen, wenn Schutzbedarf besteht:

1. Grundschutzmaßnahmen

- Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmerkmalen, wie z. B. Unterschrift, Foto, Hologramme.

- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst

- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen.

- Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.

- Sicherung der Kommunikation zwischen der Chipkarte, dem CDLS und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen.

- Sicherung unterschiedlicher Chipkartenanwendungen auf einer Chipkarte durch gegenseitige Abschottung.

- Durchführung einer gegenseitigen Authentisierung von Chipkarte und CDLS mit dem Challenge-Response-Verfahren.

2. Erweiterte Sicherungsmaßnahmen

- Realisierung weiterer "aktiver" Sicherheitsfunktionen des Betriebssystems, wie "Secure Messaging", I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen und dergleichen. Zur Sicherung von Transaktionen oder zur Rekonstruktion nicht korrekt abgelaufener Transaktionen kann ein Logging vorhanden sein.

- Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein "Gesamtwissen" verfügt.

3. Grundsätzlich sollte zunächst die Möglichkeit in Betracht gezogen werden, daß bei der Chipkartenbenutzung Anonymität gewahrt bleiben kann. Ist dies nicht möglich, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.

4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit erhalten, auf neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren und die Produktion, die Initialisierung und der Versand der Chipkarten zu überwachen.

6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, das bei unbefugten Handlungen das Strafrecht anwendbar macht.
7. Alle Systemkomponenten datenschutzrelevanter Chipkartenanwendungen sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.

8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z. B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.

9. Sicherheitsrelevante Karten (z. B. Bankkarten) sollten über den gesamten Lebenszyklus der Karte kryptographisch gesichert sein.

III. Technische Grundlagen

III.1 Hardware der Chipkarten

Chipkarten gibt es in vielfältigen Bauformen, Funktionsweisen und Funktionsspektren. Man unterscheidet Chipkarten hinsichtlich der

- Art der Datenübertragung bei der Interaktion mit der Außenwelt:
    - kontaktbehaftet oder
    - kontaktlos über elektromagnetische Felder (bestimmte kontaktlose Karten können auch über eine Entfernung von mehreren Metern von einem CDLS gelesen werden);
- Art der in der Karte bereitgestellten IT-Ressourcen:
    - reine Speicherchipkarten mit nicht flüchtigem Speicher (z. B. Identifikationskarten)
    - intelligente Speicherchipkarten mit EPROM (z. B. Telefonkarte) oder EEPROM (z. B. Krankenversichertenkarten)
    - Prozessorchipkarten mit EEPROM, RAM, ROM und CPU
    - Prozessorchipkarten mit Coprozessor für die Abwicklung kryptografischer Verfahren (Krypto-Coprozessor).
- Art der Anwendung:
    - elektronischer Zahlungsverkehr (Elektronische Geldbörse),
    - Wegwerfkarten (Telefonkarte),
    - wiederaufladbare Karten (z. B. Chipkarten im öffentlichen Personennahverkehr),
    - multifunktionale wiederaufladbare Chipkarten (z. B. unterschiedliche "Geldbörsen auf einer Chipkarte)
    - Berechtigungskarten (z. B. Mobiltelefone, Betriebsausweise)

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 512 Byte, Festwertspeicher (ROM) für das Betriebssystem erreichen derzeit eine Kapazität von 16 KB, der elektrisch löschbare, programmierbare Festwertspeicher (EEPROM) mit der Kapazität von 16 KB erlaubt die Installation einer kleinen Datenbank. Im Vergleich dazu leisten Mikroprozessoren heute üblicherweise eingesetzter PC ca. 100 - 150 Millionen Befehle pro Sekunde und arbeiten mit RAM-Speichern von 8 - 32 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch

keine Manipulationen ermöglicht.

In diesem "Read-Only-Memory" (ROM) befindet sich das Betriebssystem einer Chipkarte. Für Chipkarten-Betriebssysteme existieren u. a. die Normen aus der Serie ISO/IEC 7816, in der die Befehle solcher Systeme beschrieben werden. Die Chipkarten-Betriebssysteme nutzen diese Befehle in unterschiedlicher Weise, d. h., nicht jedes Betriebssystem unterstützt jedes Kommando oder jede Option eines Kommandos. Auch weisen fast alle Chipkarten-Betriebssysteme zusätzliche herstellerspezifische Kommandos auf. Die Chipkarten-Betriebssysteme ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird an den internationalen Standard angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF). Auf der MF-Ebene können Daten vorhanden sein, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden (z. B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Sie sind in der Regel in Elementary Files (EF) abgelegt.

Daneben gibt es auch sog. Dedicated Files (DF), die mit ihren untergeordneten EFs und ihren Funktionen die Anwendungen in einer Karte repräsentieren. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten auf der MF-Ebene zugreifen.

EFs können dem Betriebssystem zugeordnet sein und damit Daten enthalten, die das Betriebssystem nutzt, z. B. anwendungsbezogene Paßwörter, Schlüssel und andere Zugriffsattribute zu Nutzdaten. Ein direkter Zugriff mittels des CDLS ist nicht möglich.

Sie können aber auch die Nutzdaten einer Anwendung enthalten, die ggfs. erst nach einer Authentisierung unter Berücksichtigung von Sicherheitsattributen gelesen und/oder verändert werden. Es gibt unterschiedliche Dateistrukturen für EFs: Sie können Records mit fester (linear fixed) oder variabler (linear variable) Länge enthalten, können eine Ringstruktur mit fester Länge (cyclic) haben, können jedoch auch eine amorphe, d. h. vom Benutzer frei wählbare Struktur (transparent) aufweisen, auf denen auf Daten byte- oder blockweise zugegriffen werden kann.

III.2.2 Authentisierung

Die Authentisierungstechniken zwischen Chipkarte und einer externen Einheit werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentisierung, bei der sich die Chipkarte gegenüber der externen Einheit authentisiert und externer Authentisierung, bei der sich die externe Einheit gegenüber der Chipkarte authentisiert unterschieden. Die gegenseitige Authentisierung ist in Vorbereitung.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentisierung) von Files sowie zur Auswahl von zu bearbeitenden Files definiert ISO 7816-4 einige Kommandos, die für die Implementation von Sicherheitsfunktionalitäten bedeutsam sind:

- VERIFY zur Benutzerauthentisierung mit einer PIN. Dies kann eine auf MF-Ebene gespeicherte globale PIN oder eine DF-spezifische anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und - falls erforderlich - die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit dem gespeicherten Referenzwert. Ein Erfolg wird durch Senden des Status "OK" angezeigt, ansonsten ein interner Fehlversuchszähler dekrementiert und als Status "nicht OK" übertragen. Bei Zählerstand 0 wird die Anwendung der Applikation, die die PIN benutzt, blockiert. Bei einigen Betriebssystemen kann die Blockierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt ist.

- INTERNAL AUTHENTICATE löst eine interne Authentisierung aus. Dazu erhält die Chipkarte den Schlüsselbezeichner des ausgewählten EF und Authentisierungsdaten (Zufallszahl). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten EF und sendet das Chiffrat zurück. Die prüfende Einheit (z. B. das CDLS oder eine Patientenkarte) entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.

- EXTERNAL AUTHENTICATE löst die externe Authentisierung aus. Dazu wird mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte gefordert, die an die zu authentisierende Instanz übergeben wird. Diese verschlüsselt sie und sendet das Ergebnis zusammen mit der Nummer des zu verwendenden Schlüssels an die Karte zurück. Dann entschlüsselt die Karte die Zufallszahl mit dem Schlüssel der angegebenen Schlüsselnummer. Bei Übereinstimmung wird die zu authentisierende Instanz als authentisch anerkannt.

Weitere Sicherheitsfunktionen werden derzeit in ISO 7816-8 spezifiziert. Von besonderer Bedeutung ist hierbei das Kommando PERFORM SECURITY OPERATION, mit dem folgende Sicherheitsoperationen ausgeführt werden können:

- COMPUTE DIGITAL SIGNATURE,
- VERIFY DIGITAL SIGNATURE,
- VERIFY CERTIFICATE,
- HASH,
- COMPUTE CRYPTOGRAPHIC CHECKSUM,
- VERIFY CRYPTOGRAPHIC CHECKSUM,
- ENCIPHER,
- DECIPHER.

In ISO 7816-7 sind außerdem spezielle Sicherheitsfunktionen beschrieben, die sich auf Chipkarten mit einer sog. SCQL-Datenbank (Structured Card Query Language) beziehen.

III.3 Chipkartenbasierte Dienstleistungssysteme (CDLS)

Wie in der Einleitung kurz dargestellt, sind Chipkarten nicht als isolierte Träger von Risiken zu betrachten, wenn es um Fragen ihrer IT-Sicherheit geht. Aufwendige sicherheitstechnische Maßnahmen an und in der Chipkarte können durch unsichere Systemumgebungen bei der weiteren Verwendung der Daten konterkariert werden.

Wenn zum Beispiel das System eines zugriffsberechtigten Arztes nicht den erforderlichen Schutz bietet, können die Schutzmaßnahmen der Karte umgangen werden. Der Schutz der Chipkarte gegen unbefugte Manipulationen ist

weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das POS-Terminal leicht manipuliert werden kann. Jedoch sieht ISO/IEC 7816 Schutzmechanismen vor, die bei richtiger Anwendung mit vertretbarem Aufwand nicht umgangen werden können.

Hier sollen jedoch nur für solche Komponenten Sicherheitsbetrachtungen angestellt werden, die chipkartenspezifisch sind. Solange die Chipkarten keine eigenen Mensch-Maschine-Schnittstellen enthalten, sind für die Erschließung der Chipkarteninhalte und -funktionen Systeme notwendig, mit denen die Chipkarten gelesen und beschrieben werden können. Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z. B. über Sensorfelder, werden CDLS kaum entbehrlich sein, denn sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. CDLS können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversichertenkarten, Sicherungskarten für Mobiltelefone usw.) spezielle CDLS entwickelt und eingesetzt worden. Soweit erkennbar, werden universell einsetzbare CDLS bisher nicht auf dem Markt angeboten. Im Gesundheitswesen werden derzeit CDLS eingesetzt, deren Verwendung auf die Kommunikation mit der Krankenversicherungskarte eingeschränkt wurde. Da sich weitergehende Anwendungen abzeichnen, wurde eine Spezifikation für multifunktionale CDLS angefertigt, die von einem Arbeitskreis der Arbeitsgemeinschaft "Karten im Gesundheitswesen" und der Gesellschaft für Mathematik und Datenverarbeitung (GMD) herausgegeben worden ist.

Dieser Spezifikation liegt folgende Konzeption zugrunde:

- Die CDLS sind transparent für jeden Dialog zwischen einem Anwendungsprogramm und einer Chipkarte, sofern dieser Dialog über eine genormte Schnittstelle geführt wird. Damit ist ihre Anwendung auch außerhalb des Gesundheitswesens möglich.

- Allerdings ist die Option, ein universell einsetzbares CDLS zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil als obligatorisch gefordert. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Der Spezifikation entsprechende CDLS können sowohl mit synchronen Chipkarten wie die Krankenversicherungskarte als auch mit Prozessor-Chipkarten kommunizieren, die ein standardisiertes Übertragungsprotokoll unterstützen.

- Es können anwendungsspezifische Funktionen im CDLS realisiert werden, die dann nicht dem Anwendungsprogramm überlassen werden, solange nicht andere Vorkehrungen zum Schutz der Karte vor unbefugten oder durch Fehlfunktionen ausgelösten schreibenden Zugriffen getroffen sind. So ist z. B. ein Modul zur Verarbeitung der Versichertenkarte gem. § 291 SGB V für Gesundheitskarten-Terminal spezifiziert worden.

- Es können je nach Anwendung weitere anwendungsspezifische Module definiert werden, die periphere Geräte steuern. So wurde für die Gesundheitschipkarten ein Modul definiert, das einen Drucker steuert, damit Ärzte ohne IT-Einsatz die Kartensysteme zumindest für die Übertragung des Inhalts der Versichertenkarte auf die Belege der vertragsärztlichen Versorgung nutzen können. Das Druckmodul mit der parallelen Schnittstelle ist optional zu realisieren.

- Eine Download-Funktion erlaubt die Behebung von Softwarefehlern und ggf. im gewissen Umfang einen Upgrade von Leistungen.

- Die Spezifikation gilt für kontaktbehaftete Chipkarten nach ISO 7816 in 5-Volt-Technologie. Kontaktlose Chipkarten und kontaktbehaftete Chipkarten in 3-Volt-Technologie sollen einbezogen werden, wenn die Normung Klarheit geschaffen hat. Das gleiche gilt für eine Erweiterung von Standards für die Nutzung der Kontakte und für höhere als derzeit spezifizierte Übertragungsraten.

- Das Anwendungssystem in einem PC wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik aufgesetzt.

- CDLS als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:

    - Display und/oder Tastatur,
    - mehrere Kontaktiereinheiten für eine Chipkarte im Normalformat gem. ISO-IEC 7816-2 oder
    - im Plug-in-Format.

IV. Sicherheitstechnische Gestaltungsspielräume

Für die Entwicklung sicherer Chipkartenanwendungen gibt es eine Vielzahl von Ansatzpunkten, die je nach den in einer anwendungsspezifischen Sicherheitspolitik definierten Anforderungen zur Verbesserung der Sicherheit mit gewissen Spielräumen ausgenutzt werden können. In diesem abschließenden Kapitel geht es einerseits darum, diese sicherheitstechnischen Gestaltungsspielräume darzustellen und andererseits die Empfehlungen der Datenschutzbeauftragten zur Ausschöpfung dieser Spielräume hervorzuheben.

IV.1 Allgemeine Anforderungen

Wie bereits einleitend dargestellt sind Chipkarten als miniaturisierte Computer anzusehen, die (noch) nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Daraus ergeben sich folgende Konsequenzen:

- Chipkarten sind leicht transportable Rechner. Die besonderen Bedrohungen der IT-Sicherheit, die z. B. bei anderen transportablen Rechnern (Laptops, Notebooks,...) berücksichtigten werden müssen, existieren in ähnlicher Weise auch für Chipkarten.

- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter technischer Systeme (CDLS), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem CDLS ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.

- Speicher- und Prozessorkapazitäten bilden Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen. Heutige Betrachtungen müssen sie jedoch noch berücksichtigen.

Allgemein sind an die Sicherheitsfunktionen folgende Anforderungen zu stellen:

- Zugriffs- und Nutzungsberechtigungen sollten soweit möglich von der Chipkarte selbst geprüft und gesteuert werden.

- In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies in sicherer Umgebung oder ohne zwischengeschaltete Systeme erfolgen kann. Dies würde eine autonome Stromversorgung der Chipkarte und geeignete Mensch-Maschine-Schnittstellen voraussetzen (z. B. Sensorfelder für biometrische Merkmale).

- Es muß grundsätzlich ein Mindestschutz vorhanden sein, mit dem die in § 202a Abs. 1 StGB geforderte "besondere Sicherung gegen unberechtigten Zugang" realisiert wird, um bei unbefugter Nutzung einer Chipkarte das Strafrecht anwendbar zu machen.

IV.2 Hardwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.2.1 Herstellung, Initialisierung und Versand von Chipkarten

Sicherheitserwägungen greifen bereits bei der Herstellung, Initialisierung und dem Versand von Chipkarten. Dabei müssen

- die Produktion der Prozessoren und Chipkarten,
- die Produktion und das Laden von Software,
- das Erzeugen der Schlüssel,
- das Laden der Schlüssel in die Sicherheitsmodule (Internal Elemetary Files),
- das Laden von Hersteller- und Transportschlüssel für die spätere Initialisierung und
- der Versand der Chipkarten und Transportschlüssel an den Empfänger

durch entsprechende technische und organisatorische Maßnahmen abgesichert werden.

IV.2.2 Sicherheitsmerkmale des Kartenkörpers

Zur Unterstützung der Authentifizierung des Karteninhabers gegenüber der Chipkarte und damit des Nachweises, daß die Chipkarte

- zur jeweiligen Anwendung gehört und
- die die Karte vorlegende Person die Karte rechtmäßig nutzt,

sollte der Kartenkörper mit Sicherheitsmerkmalen ausgestattet sein, die der Sensibilität angemessen sind:

- Aufdruck,
- Hologramm,
- Unterschrift des Besitzers (nur bei nicht anonymen Anwendungen),

- Foto des Besitzers (nur bei nicht anonymen Anwendungen),
- aufgebrachtes Echtheitsmerkmal,
- Multiple Laser Image (durch Lasergravur auf der Chipkarte aufgebrachte hologrammähnliches Kippbild mit kartenindividuellen Informationen).

Dabei ist allerdings zu berücksichtigen, daß es Sicherheitsmerkmale gibt, die z. B. bei anonymen Chipkartenanwendungen (z. B. anonyme Zahlungsverfahren) die Anonymität aufheben würden und daher dabei nicht verwendet werden können.

IV.2.3 Sicherheitsmechanismen der Chip-Hardware

Sicherheitsmechanismen der Chip-Hardware richten sich vor allem gegen die Analyse der Chip-Inhalte und -Sicherheitssysteme mit Hilfe von Spezialgeräten, z. B. durch Abtragen dünner Chipschichten. Dabei kann unterschieden werden zwischen passiven Mechanismen, bei denen eine bestimmte Bauweise des Chips die Schutzfunktionen ergibt, und aktiven Mechanismen, die auf äußere Eingriffe passend reagieren und ggfs. den Chip zerstören.

Passive Mechanismen:

- Es gibt von außen keine direkte Verbindung zu den Funktionseinheiten. Ein Testmodus, der eventuell später nicht mehr erlaubte Zugriffe auf den Speicher ermöglicht, muß irreversibel auf den Benutzermodus geschaltet werden können.

- Interne Busse werden nicht nach außen geführt.

- Der Datenfluß auf den Bussen wird mit Scrambling geschützt.

- Der ROM befindet sich in den unteren Halbleiterschichten, um eine optische Analyse zu verhindern.

- Gegen das Abtasten von Ladungspotentialen erfolgt eine Metallisierung des gesamten Chips.

- Die Chipnummern werden eindeutig vergeben (werden u. U. von den Anwendungen benötigt).

Aktive Mechanismen:

- Es wird eine Passivierungsschicht aufgebracht, deren Entfernen einen Interrupt auslöst, der die Ausführung der Software unterbindet, sowie Schlüssel und andere sicherheitsrelevante Daten löscht.

- Es erfolgt eine Spannungsüberwachung. Wenn der Spannungswert den zulässigen Bereich über- oder unterschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden.

- Den gleichen Zweck verfolgt die Taktüberwachung. Es werden damit Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.

- Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

IV.3 Softwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.3.1 Basisalgorithmen für Schutzfunktionen der Software

Die Schutzfunktionen der Chipkarten-Software basieren auf den bekannten und teilweise standardisierten Algorithmen zur Verschlüsselung, Signatur und Generierung von Zufallszahlen.

Dazu gehören symmetrische Verschlüsselungsalgorithmen wie DES, Triple-DES, IDEA und SC85 und asymmetrische Verfahren wie RSA, Signieralgorithmen wie DSS und RSA mit RipeMD160, Einwegfunktionen zur Berechnung des MAC und für das Hashing wie SHA und RipeMD160 sowie Zufallszahlengeneratoren.

IV.3.2 Schutzfunktionalitäten und -mechanismen des Betriebssystems

Zunächst sollte sichergestellt sein, daß sich nicht alle Teile des Betriebssystems im ROM befinden, damit der Chiphersteller nicht über das ganze Wissen über die Sicherung der Chipkarte verfügt. Wesentliche Teile des Betriebssystems können bei der späteren Initialisierung über entsprechend authentisierte CDLS dynamisch aus Tabellen geladen werden.

Darüber hinaus sollte das Betriebssystem in folgender Weise Sicherheit "erzeugen":

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN oder mit biometrischen Verfahren.

   Üblicherweise erfolgt die Prüfung einer PIN. Zwar können die normale Forderungen zur Paßwortverwaltung bei Rechnern nicht voll auf Chipkarten übertragen werden, jedoch sollte die PIN-Länge je nach Sensibilität mindestens 4 oder mehr Stellen betragen, die Anzahl der Fehlversuche begrenzt sein, die Möglichkeit bestehen, die PIN zu ändern und eine Freischaltung der Karte auch mittels Personal Unblocking Key (PUK) in Abhängigkeit von der Anwendung ermöglicht werden.

   Biometrische Verfahren erfassen Fingerabdrücke, Augenhintergründe, Handgeometrien, Sprachmerkmale oder Unterschriftsdynamiken, verformeln sie und übertragen das Ergebnis zur Überprüfung auf die Chipkarte.

b) Es erfolgt eine Zugriffskontrolle mit einer Rechteverwaltung, wobei die Zugriffsrechte an die einzelnen Dateien geknüpft werden. Den Dateien sind Sicherheitsattribute zugeordnet, mit denen festgelegt wird, ob die Dateien (Daten) gelesen, kopiert, beschrieben, gelöscht, gesperrt oder freigegeben werden dürfen.

c) Wenn anderen Personen als dem Karteninhaber Zugriffsmöglichkeiten auf die Chipkarte gewährt werden sollen, erfolgt dies im Rahmen einer Programm-Programm-Kommunikation mit einem anderen Rechner oder einer anderen Karte (z. B. mit einer Professional Card). Der Rechner bzw. die andere Karte muß authentifiziert werden.

   Die Rechnerauthentifizierung wird meist nach einem auf DES basierenden Challenge-Response-Verfahren vorgenommen.

   Nach dem gleichen Schema verläuft die gegenseitige Authentifizierung von Chipkarte und Professional Card. Beide

Benutzer müssen ihre Chipkarte aktivieren. Dann erfolgt die Authentifizierung zwischen den beiden Karten, wobei das CDLS die Daten transparent weiterleitet.

d) Zum Schutz gegen Ausforschung und Manipulation erfolgt eine sichere Datenübertragung zwischen Chipkarte und CDLS ("Secure Messaging").

e) Auf Opto-Hybridkarten können die Daten auf der optischen Fläche verschlüsselt abgelegt werden. Die Entschlüsselung kann mit Hilfe des Prozessors erfolgen, der die Schlüssel verwaltet.

f) Das Betriebssystem führt eine I/O-Kontrolle aller Schnittstellen gegen unerlaubte Zugriffe durch.

g) Die Interferenzfreiheit der einzelnen Anwendungen wird gewährleistet, d. h., eine gegenseitige unerwünschte Beeinflussung der Anwendungen wird ausgeschlossen.

h) Trace- und Debugfunktionen sind nicht verfügbar.

i) Beim Initialisieren des Betriebssystems werden RAM und EEPROM geprüft.

j) Fehleingaben werden abgefangen.

k) Der Befehlsumfang wird auf die notwendigen Befehle reduziert. Funktionalitäten, die nicht zugelassen werden sollen, werden vom Betriebssystem unterbunden.

l) Die Dateiorganisation, Header und Speicherbereiche im EEPROM werden durch Prüfsummen abgesichert.

m) Das Betriebssystem sieht die Möglichkeit vor, die Chipkarte durch Löschung zu deaktivieren (etwa nach Ablauf einer Gültigkeitsdauer), jedoch verhindert es die mißbräuchliche Deaktivierung.

IV.3.3 Die Sicherheit der Anwendung

Die Betrachtung der Sicherheit bei der Anwendung von Chipkarten setzt die ganzheitliche Betrachtung der Kommunikation zwischen Chipkarten, CDLS und im Hintergrund wirkenden Systemen voraus. Die Kommunikation zwischen den einzelnen Systemen und Systembestandteilen ist ebenfalls mit kryptographischen Methoden zu sichern:

- Zur Unterstützung der Sicherheit der Kommunikation dienen Funktionen des Chipkarten-Betriebssystems zur gegenseitigen Authentifizierung von Chipkarten und Rechnern, zur sicheren Datenübertragung und zum Signieren und Verschlüsseln (siehe IV.3.2 c), d)).

- Gegen die unberechtigte Nutzung der Daten auf der Chipkarte muß eine Zugriffskontrolle erfolgen, die auf einer sicheren Identifikation und Authentifizierung der Benutzer beruht (siehe IV.3.2 a), b)).

Darüber hinaus sind die folgenden für die Sicherheit der Anwendung bedeutsamen Maßnahmen zu berücksichtigen:

- Den Dateien auf der Chipkarte sind Befehle zuzuordnen, die mit ihnen ausgeführt werden können. Die Ausführung

anderer Befehle ist zu unterbinden.

- Zugriffe auf geschützte Datenbereiche und Veränderungen der Daten sollten protokolliert werden - vorzugsweise auf der Chipkarte. Die Anwendung muß die Auswertung der Protokolldaten unterstützen.

- Bedarfsweise sollten Überprüfungen durch Abgleich mit Hintergrundsystemen erfolgen, z. B. die Erkennung gesperrter Karten durch Abgleich mit Sperrdateien, Feststellung von Betragslimits im chipkartengestützten Zahlungsverkehr.
- Die eindeutige Nummer des Chips schützt vor der Erstellung von Dubletten.

Bei den letzten beiden Spiegelstrichen muß allerdings berücksichtigt werden, daß mit solchen Maßnahmen bei anonymen Systemen unter Umständen die Anonymität gefährdet sein kann. Es kann nicht immer ausgeschlossen werden, daß anonyme Chipkarten einzelnen Nutzern zugeordnet werden, wenn die Identifizierung der Karte möglich ist.

IV.4 Risiken und Anforderungen bei chipkartenbasierten Dienstleistungssystemen (CDLS)

Zwar bilden - wie oben festgestellt - Chipkarten und CDLS erst zusammen ein vollwertiges Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das CDLS in der von Anwendern. Denkbar ist auch, daß bei Inhabern und Anwendern unterschiedliche Vorstellungen und Interessen mit der Nutzung verbunden werden. Wesentliche Teile der unabdingbaren Sicherheitsmechanismen der Karte können daher konterkariert werden, indem die Steuerungssoftware des CDLS verändert oder die Hardware des CDLS manipuliert wird. Eine Zertifizierung von CDLS kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein CDLS eingeführt wird, gibt der Inhaber die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände auf. Eine unbefugte Veränderung der Software muß daher technisch verhindert werden.

Allerdings sind die Datenbestände grundsätzlich variabel. Sie können daher benutzt werden, über das CDLS Daten abzulegen, die für den Karteninhaber verdeckt sind und nur mit bestimmten Codes gelesen werden können (verdeckte Kanäle). Dies eröffnet Möglichkeiten für unbefugtes oder gar kriminelles Handeln.

Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern die tatsächlichen Funktionen z. B. auf neutralen CDLS testen zu können. Wegen der u. U. unterschiedlichen Interessenlagen (z. B. in wirtschaftlichen Beziehungen) ist die Prüfung der korrekten Funktion der Software sowie umgekehrt des Ausschlusses ungewollter Funktionen im realisierbaren Rahmen zu ermöglichen.

Manipulationen an der Hardware und der Eingabesteuerungssoftware der CDLS können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale) bei der Authentifizierung des Kartenbesitzers in das CDLS übertragen und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an CDLS zu stellen:

- Die CDLS müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert

oder erschwert bzw. erkennbar wird.

- Sicherheitsmodule, die die für die vertrauliche Kommunikation mit Chipkarten und die gegenseitigen Authentifizierungen erforderlichen Hauptschlüssel enthalten, sind mechanisch (zum Beispiel durch Vergießung in Epoxidharz) und elektrisch gegen vielfältige Angriffsformen besonders abzusichern. Jeder Angriff auf das Sicherheitsmodul muß zum Löschen aller Schlüssel im Sicherheitsmodul führen. Dies setzt auch voraus, daß das Sicherheitsmodul weitgehend von der Stromversorgung des CDLS autark sein muß.

- Die CDLS müssen alle automatisch prüfbaren Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über die entsprechenden Sensoren verfügen (siehe IV.2.2).

- Sofern die Kommunikation zwischen Chipkarte und CDLS nicht durch kryptographische Verfahren gegen Abhören und Manipulation gesichert wird, ist das Abhören der Kommunikation durch mechanische Maßnahmen (sog. Shutter zum Abschneiden aller manipulativ mit der Karte in das CDLS eingebrachten Drähte) zu verhindern.

Als besonders angriffsgefährdet sind CDLS vom Typ "PC mit Kartenterminal" anzusehen, sofern sie nicht in manipulationsgeschützten Umgebungen eingesetzt werden. Erhöhte Schutzfunktionen werden hier als notwendig angesehen. Die bisherigen Spezifikationen für die CDLS lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im CDLS ergriffen werden können. Es fehlt daher an einem schlüssigen Sicherheitskonzept für das Zusammenspiel zwischen dem Betriebssystem und den Applikationen der (übergeordneten) IT-Umgebung und dem Betriebssystem und den Applikationen des Systems Chipkarte/CDLS.

Abkürzungsverzeichnis

CDLS	Chipkartenbasiertes-Dienstleistungssystem
CPU	Central Processing Unit (Zentraleinheit)
DES	Symmetrischer Verschlüsselungsalgorithmus (Data Encryption Standard)
DF	Dedicated File
DSS	Signieralgorithmus (Digital Signature Standard)
EEPROM	Electrically Erasable.Programmable Read Only Memory (elektrisch löschbarer, programmierbarer Festwertspeicher)
EF	Elementary File
EPROM	Erasable Programmable Read Only Memory (löschbarer, programmierbarer Festwertspeicher)
IDEA	Symmetrischer Verschlüsselungsalgorithmus
IEC	International Electrotechnical Commission
ISO	International Standardisation Organisation
IT	Informationstechnik
KB	Kilobyte
KT	Kartenterminal
KVK	Krankenversichertenkarte
MAC	Message Authentication Code
MB	Megabyte
MF	Masterfile

PC	Personal Computer
PIN	Persönliche Identifikations-Nummer
PUK	Personal Unblocking Key
RAM	Random Access Memory (Direktzugriffsspeicher)
RipeMD160	Hash-Algorithmus
ROM	Read Only Memory (Festwertspeicher)
RSA	Asymmetrischer Verschlüsselungsalgorithmus (Rivest-Shamir-Adleman)
SC 85	Symmetrischer Verschlüsselungsalgorithmus
SGB V	Sozialgesetzbuch V (Gesetzliche Krankenversicherung)
SHA	Secure Hash-Algorithmus

Literaturangaben:

Das Papier basiert in wesentlichen Teilen auf dem Buch

Rankl, W.; Effing, W.: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz, München, Wien: Carl Hanser-Verlag, 1995

Ferner wurden verwendet:

Giesecke & Devirent GmbH (Hrsg.): Referenz-Handbuch STARCOS S 1.1, Jan. 1995

Krummeck, G.; König, R.: Chipkarten im Gesundheitswesen - Technikfolgen-Abschätzung zur Sicherheit in der Informationstechnik, BSI-Schriftenreihe zur Informationstechnik, 1994

Zur ergänzenden Lektüre wird empfohlen:

Aberer, Karl: ISO/IEC 7816-8 SCQL-Database: Technik- und Nutzungsmöglichkeiten, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

Bachmeier, Roland: Chipkarten und Datenschutz, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Ferreira, Malzahn, Quisquater, Wille: A High Performance Third Generation Crypto Card, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Fumy: Authentifizierung und Schlüsselmanagement, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Hamann, Hirsch: Chipkarten-IC´s - die richtige Lösung für sicherheitssensitive Anwendungen, in: Glade, Reimer, Struif: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Horster, Lender: Hybride Opto-Chip-Karten, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, 1995

Kruse, Peuckert: Chipkarte und Sicherheit; DuD 3/95, S. 142 ff

Kruse: Sicherheitszertifikate für Chipkarten; DuD 9/95, S. 537 ff
Normann, Ute: Telefonkarten-Chip und Sicherheit, in Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

SmartsCards - eine neue Dimension in der Informationstechnik, Der GMD-Spiegel 1/92, GMD, 1992

Struif, B.: Chipkarten - State of the Art, Tutorium "Verläßliche Informationssysteme", anläßlich der Fachtagung VIS 1991

Struif, B.: Neue Smart Card-Features aus Normensicht, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, 1996

Weikmann: Die neue Generation von Chipkarten-Mikrocontrollern, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

---

Arbeitsgruppe Chipkarten

[1] In der Arbeitsgruppe haben mitgewirkt: Walter Ernestus (Der Bundesbeauftragte für den Datenschutz), Hanns-Wilhelm Heibey (Federführung) (Berliner Datenschutzbeauftragter), Uwe Jürgens (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Veikko Müller (Der Landesbeauftragte für den Datenschutz Brandenburg), Wolfgang Polacek (Der Landesbeauftragte für den Datenschutz Niedersachsen), Dr. Uwe Schläger (Der Hamburgische Datenschutzbeauftragte), Wilfried Seiffert (Der Landesbeauftragte für den Datenschutz Niedersachsen), Rüdiger Wehrmann (Der Hessische Datenschutzbeauftragte).

Wir danken den Mitgliedern des DIN-Arbeitskreises NI-17.4 (Austauschprotokolle bei Chipkarten), vor allem aber dessen Sprecher Herrn Bruno Struif (GMD-Darmstadt, Forschungszentrum Informationstechnik) für eine kritische Durchsicht und viele wertvolle Hinweise und Anregungen zu dem vorliegenden Papier.

[2] Die hiermit vorgelegte Ausarbeitung ist in der Version vom 2. Dezember 1996. Der schnelle Fortschritt bei der Entwicklung der Chipkartentechnologien macht im Prinzip eine ständige Anpassung oder Fortschreibung erforderlich. Die Arbeitsgruppe hat jedoch beschlossen, zunächst ein fertiges Papier mit festgelegtem Aktualitätsstand vorzulegen, da sonst die Gefahr besteht, nie zu einem Abschluß zu kommen. Jedoch ist es geeignet, in weiteren Arbeitsschritten fortgeschrieben zu werden.

Zur besseren Lesbarkeit der Ausarbeitung wird sie durch ein Abkürzungsverzeichnis ergänzt.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997 in München

Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z.B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.

- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages "berechtigtes" statt eines rechtlichen Interesses gefordert.

- Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.
Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.

- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.

- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.

- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.

- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.

- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.

- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997 in München

Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz -DNA-Analyse ("Genetischer Fingerabdruck")- die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z.B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81

e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   - Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung auf Grund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

   - Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

   - Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z.B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997 in München

Geplante Verpflichtung von Teledienstеanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 (§ 5 Absatz 3) des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z.B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z.B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997 in München

Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen."

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. April 1997 in München

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

   Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), - z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Stichwortverzeichnis

(Berichtszeitraum der Jahresberichte: I = März bis Dezember 1992; II = bis März 1994; III = bis März 1995; IV = bis März 1996; V = bis März 1997 /Seitenangabe)

Abkürzungsverzeichnis

1. SKWPG	=	Erstes Gesetz zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms
1. SRG	=	Erstes Schulreformgesetz für das Land Brandenburg
2. MeldDÜÄV	=	Zweite Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
2. SGBÄndG	=	2. Gesetz zur Änderung des Sozialgesetzbuches
a. F.	=	alte Fassung
ABl.	=	Amtsblatt
Abs.	=	Absatz
Abschn.	=	Abschnitt
ADV	=	Automatische Datenverarbeitung
AFIS	=	Automatisierte Fingerabdruck-Identfizierungssystem
AfNS	=	Amt für Nationale Sicherheit
AG	=	Ausführungsgesetz
AGE	=	Autobahngebührenerfassungssystem
AgrStaG-DVO	=	Verordnung über die Durchführung des Agrarstatistikgesetzes
AGTierSGBbg	=	Gesetz zur Ausführung des Tierseuchengesetzes
ALK	=	Automatisierte Liegenschaftskarte
AMG	=	Arzneimittelgesetz
Änd.	=	Änderung
Anl.	=	Anlage
AO	=	Abgabenordnung
AO-GS	=	Ausbildungsordnung der Grundschule im Land Brandenburg
AOK	=	Allgemeine Ortskrankenkasse
APOmJD	=	Ausbildungs- und Prüfungsordnung mittlerer Justizdienst
Art.	=	Artikel
Ärzte-ZV	=	Zulassungsordnung für Vertragsärzte
ATKIS	=	Amtliches topographisch-kartographisches Informationssystem
Aufl.	=	Auflage
AufnV	=	Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg
AuslG	=	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet
AV	=	Allgemeine Verfügung
AVA	=	Automatisierten Vorgangstagebuchs
AWMF	=	Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften
AZV	=	Abfallzweckverband
BAFI	=	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	=	Bundesausbildungsförderungsgesetz
BauGB	=	Baugesetzbuch
BbgDSG	=	Brandenburgisches Datenschutzgesetz
Bbg.	=	Brandenburgisch(es)
BbgAbfG	=	Brandenburgisches Abfallgesetz

BbgArchG	=	Brandenburgisches Architektengesetz
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgBO	=	Brandenburgische Bauordnung
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPAuswG	=	Brandenburgischen Personalausweisgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgRAVG	=	Brandenburgisches Rechtsanwaltsversorgungsgesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgVerf	=	Brandenburgische Verfassung
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BBiG	=	Berufsbildungsgesetz
BDSG	=	Bundesdatenschutzgesetz
BdVP	=	Bezirksdirektionen der Volkspolizei
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BKAG-E	=	Bundeskriminalamtgesetz-Entwurf
BKA-Gesetz	=	Bundeskriminalamtgesetzes
BKGG	=	Bundeskindergeldgesetz
BlnDSG	=	Berliner Datenschutzgesetz
BLVS	=	Landesamt für Verkehr und Straßenbau Brandenburg
BLZpB	=	Brandenburgischen Zentralstelle für politische Bildung
BML	=	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BND	=	Bundesnachrichtendienst
BR-Drs.	=	Bundesrats-Drucksache
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BSS	=	Basisstationen
BSeuchenG	=	Bundesseuchengesetz
BSHG	=	Bundessozialhilfegesetz
BbgSozBerG	=	Brandenburgische Sozialberufsgesetz
BStatG	=	Bundesstatistikgesetz
BStU	=	Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs	=	Bundestags-Drucksache
Buchst.	=	Buchstabe
Bundes-SISY	=	bundesweites staatanwaltschaftliches Informationssystem
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BZR	=	Bundeszentralregister
BZRG	=	Bundeszentralregistergesetz
bzw.	=	beziehungsweise

ca.	=	circa
CD-ROM	=	Compact Disc Read Only Memory
CERT	=	Computer Emergency Response Team
CSIS	=	Centrales Schengener Informationssystem
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DBeschrV	=	Verordnung zur Dateibeschreibung
DDR-GBl.	=	DDR-Gesetzblatt
DES	=	Data Encryption Standard
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DORA	=	Dialogorientertes Recherche- und Auskunftssystem
DSVS	=	Datenschutzverordnung Schulwesen
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
e. V.	=	eingetragener Verein
ed-Behandlung	=	erkennungsdienstliche Behandlung
EDU	=	European Drug Unit
EG	=	Europäische Gemeinschaft
EGBGB	=	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EuGH	=	Europäischen Gerichtshof
EPV	=	Verordnung über die Ergänzungsstudien und Ergänzungsprüfungen für Lehrämter an Schulen (Ergänzungsprüfungsverordnung)
EUROPOL	=	Europäisches Polizeiamt
EuWG	=	Europawahlgesetz
FDGB	=	Freier Deutscher Gewerkschaftsbund
ff.	=	folgende
FrauFöV	=	Frauenförderungsverordnung
GastVO	=	Verordnung zur Ausführung des Gaststättengesetzes
geänd.	=	geändert
GEK	=	Kohortenstudie "Gesundheit, Ernährung, Krebs"
gem.	=	gemäß
GewAnzVwV	=	Allgemeine Verwaltungsvorschrift zur Durchführung der Gewerbeordnung
GewO	=	Gewerbeordnung
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
GGG	=	Gesetz über die gesellschaftlichen Gerichte der DDR
GIS	=	Geographische Informationssysteme
GKG	=	Gesetz über kommunale Gemeinschaftsarbeit im Land Brandenburg
GKR	=	Gemeinsames Krebsregister
GMBl.	=	Gemeinsames Ministerialblatt
GO	=	Gemeindeordnung
GUZ	=	Gesetzes über Unschädlichkeitszeugnisse im Grundstücksverkehr
GVBl.	=	Gesetz- und Verordnungsblatt

GWG	=	Geldwäschegesetz
G 10	=	Gesetz zu Artikel 10 Grundgesetz
G 10 AG Bbg	=	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg
HebBOBbg	=	Berufsordnung für Hebammen und Entbindungspfleger im Land Brandenburg
HeilBerG	=	Heilberufsgesetz
hrsg.	=	herausgegeben
i. d. Fassung	=	in der Fassung
IHK	=	Industrie- und Handelskammern
IHK-G	=	IHK-Gesetz
ILB	=	Investitionsbank des Landes Brandenburg
INPOL	=	Informationssytem der Polizei
InVeKoS	=	Integriertes Verwaltungs- und Kontrollsystem
ISO	=	International Organization for Standardization
i. S. v.	=	im Sinne von
ISVB	=	Informationssystem für Verbrechensbekämpfung Berlin
i. V. m.	=	in Verbindung mit
ISDN	=	Integrated Services Digital Network (dienste-integrierendes Digitalnetz)
JMBl.	=	Justizministerialblatt
JVA	=	Justizvollzugsanstalt
KA	=	Kriminalakte
KAG	=	Kommunalabgabengesetz
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
Kap.	=	Kapitel
KBA	=	Kraftfahrt-Bundesamt
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
KHIS	=	Krankenhausinformationssystems
KitaBKV	=	Kindertagesstätten-Betriebskostenverordnung
Kita-Gesetz	=	Zweites Gesetz zur Ausführung des Achten Buches des Sozialgesetzbuches - Kinder- und Jugendhilfe - Kindertagesstättengesetz
KJGDV	=	Verordnung über die Aufgaben des Kinder- und Jugend-Gesundheitsdienstes der Gesundheitsämter im Land Brandenburg
KJHG	=	Kinder- und Jugendhilfegesetz
KKO	=	Konfliktkommissionsordnung
KOVVfG	=	Gesetz über das Verwaltungsverfahren der Kriegsopferversorgung
KRG	=	Krebsregistergesetz
LAG	=	Landesarbeitsgruppe
LAN	=	Local Area Network
LBG	=	Landesbeamtengesetz
LDS	=	Landesamt für Datenverarbeitung und Statistik
LELF	=	Landesamt für Ernährung, Landwirtschaft und Flurneuordnung
LfD	=	Landesbeauftragter für den Datenschutz
LfV	=	Landesamt für Verfassungsschutz
LGG	=	Landesgleichstellungsgesetz

LHO	=	Landeshaushaltsordnung
LiKaDÜV	=	Verordnung über die Einrichtung automatisierter Abrufverfahren und regelmäßiger Datenübermittlungen im Liegenschaftskataster
LImschG	=	Vorschaltgesetz zum Immissionsschutz
LKA	=	Landeskriminalamt
LKGBbg	=	Krankenhausgesetz des Landes Brandenburg
LSPV	=	Lehrerstellen- und Personalverwaltung
LT-Drs.	=	Landtags-Drucksache
LVK	=	Lichtbildvorzeigekartei
MAC	=	Medium Access Control
MASGF	=	Ministerium für Arbeit, Soziales, Gesundheit und Frauen
MBJS	=	Ministerium für Bildung, Jugend und Sport
MdF	=	Ministerium der Finanzen
MdJBE	=	Ministerium der Justiz und für Bundes- und Europaangelegenheiten
MDK	=	Medizinischen Dienst der Krankenkassen
MDS	=	Spitzenverband der medizinischen Dienste der Krankenversicherungen
MeldDÜÄV	=	Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MeldDÜV	=	Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MELF	=	Ministerium für Ernährung, Landwirtschaft und Forsten
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
MfS	=	Ministerium für Staatssicherheit
MI	=	Ministerium des Innern
MiStra	=	Anordnung über Mitteilungen in Strafsachen
MOD	=	Magneto-optische Datenträger
MSWV	=	Ministerium für Stadtentwicklung, Wohnen und Verkehr
MUNR	=	Ministerium für Umwelt, Naturschutz und Raumordnung
MWFK	=	Ministerium für Wissenschaft, Forschung und Verkehr
MW	=	Ministerium für Wirtschaft, Mittelstand und Technologie
NASISTE	=	Nachrichtensammelstelle
n. F.	=	neue Fassung
Nr.	=	Nummer
NSIS	=	Nationales Schengener Informationssystem
OEG	=	Opferentschädigungsgesetz
ORB	=	Ostdeutscher Rundfunk Brandenburg
OWiG	=	Gesetz über Ordnungswidrigkeiten
PAK	=	Personenarbeitskartei
PaßG	=	Paßgesetz
PAuswG	=	Personalausweisgesetz
pB	=	Polizeiliche Beobachtung
PC	=	Personalcomputer
PersVG	=	Landespersonalvertretungsgesetz
PflRi	=	Pflegebedürftigkeits-Richtlinien
PHW	=	personenbezogener Hinweis
PolG	=	Polizeigesetz

POLIKS BB/BR	=	Polizeiliches Informations- und Kommunikationssystem Brandenburg/Berlin
PO-Nsch	=	Nichtschülerprüfungsordnung
PrüfBerV	=	Prüferberufungsverordnung
PStG	=	Personenstandsgesetz
PTRegG	=	Gesetz über die Regulierung der Telekommunikation und des Postwesens
RAK	=	Referatsarbeitskartei
RSA-Algorithmus	=	nach den Entwicklern Rivest, Shamir und Adleman
RTK	=	Rasterdaten topographischer Karten
RVO	=	Reichsversicherungsordnung
S.	=	Seite
s.	=	siehe
Sachgeb.	=	Sachgebiet
SchG	=	Schiedsstellengesetz
SCHUFA	=	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SchuVVO	=	Verordnung über das Schuldnerverzeichnis
SchwbG	=	Schwerbehindertengesetz
SDÜ	=	Schengener Durchführungsübereinkommen
SGB	=	Sozialgesetzbuch
SIS	=	Schengener Informationssystem
SopEPV	=	Verordnung über das Ergänzungsstudium und die Ergänzungsprüfung in Sonderpädagogik (Sonderpädagogik-Ergänzungsprüfungsordnung)
SopV	=	Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf
StA	=	Staatsanwaltschaft
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StUG	=	Stasi-Unterlagen-Gesetz
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
StVZO	=	Straßenverkehrszulassungsordnung
TB	=	Tätigkeitsbericht
TDSV	=	Telekom-Datenschutzverordnung
TFH	=	Technische Fachhochschule Wildau
TierSchG	=	Tierschutzgesetz
TierSchTrV	=	Tierschutztransportverordnung
TK	=	Telekommunikation
TSK	=	Tierseuchenkasse
TÜ-Maßnahmen	=	Telefonüberwachungsmaßnahmen
u. a.	=	unter anderem
UAG	=	Untersuchungsausschußgesetz
UIG	=	Umweltinformationsgesetz
u. U.	=	unter Umständen
UVEG	=	Unfallversicherungseinordnungsgesetz
UVollzG	=	Untersuchungshaftvollzugsgesetz

UWG	=	Gesetz gegen den unlauteren Wettbewerb
VDMA	=	Verband Deutscher Maschinen- und Anlagenbau e.V.
VermLiegG	=	Vermessungs- und Liegenschaftsgesetz
VersammlG	=	Versammlungsgesetz
VGH	=	Verfassungsgerichtshof
vgl.	=	vergleiche
VGO	=	Vollzugsgeschäftsordnung
VGPolGBbg	=	Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg
VPKÄ	=	Volkspolizeikreisämter
VV	=	Verwaltungsvorschrift
VV-Betriebspraktika	=	Verwaltungsvorschriften über die Durchführung von Schülerbetriebspraktika
VV-Datenschutz/ Statistik	=	Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen
VV-Hauunt	=	Verwaltungsvorschriften über die Durchführung von Hausunterricht
VV-Schulakten	=	Verwaltungsvorschriften über Akten an Schulen in öffentlicher Trägerschaft
VV-WissU	=	Verwaltungsvorschrift über wissenschaftliche Untersuchungen an Schulen
VwGO	=	Verwaltungsgerichtsordnung
VwVfGBbg	=	Verwaltungsverfahrensgesetz
VZR	=	Verkehrszentralregister
WildÜV	=	Wildhandelsüberwachungsverordnung
WoBelegG	=	Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen
WoBindG	=	Wohnungsbindungsgesetz
WoGG	=	Wohngeldgesetz
WoGSoG	=	Wohngeldsondergesetz
WORM	=	Write Once Read Many
WoStatG	=	Wohnungsstatistikgesetz
WWW	=	World Wide Web
ZBB	=	Zentrale Bezügestelle des Landes Brandenburg
Ziff.	=	Ziffer
ZPO	=	Zivilprozeßordnung
zul.	=	zuletzt
z. Z.	=	zur Zeit